Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

www.rijksoverheid.nl
www.facebook.com/minbzk
www.twitter.com/minbzk

Kenmerk
2019-0000016942

Uw kenmerk

Bijlage(n)
4

Datum 12 APR 2019

Betreft Beslissing op uw Wob-verzoek inzake Malware ICS

Bij brief van 20 december 2018 heeft u bij mijn ministerie een verzoek ingediend als bedoeld in artikel 3, eerste lid, van de Wet openbaarheid van bestuur (hierna: Wob). Uw verzoek heeft betrekking op Malware ICS in het tijdvak 2014 tot en met 2018, in het bijzonder op:

1. documenten betreffende het beleid ten aanzien van malware in Industrial Control Systems (ICS). Dit omvat informatie over preventiemaatregelen, risicoanalyses over de weerbaarheid van partijen en systemen, nota's over het beleid en documenten over veranderingen in dit beleid. Ook wordt hier gevraagd om informatie over de samenwerkingsverbanden die bestaan tussen mijn ministerie en verschillende partijen, en de rolverdeling binnen die samenwerkingsverbanden, om de (cyber)veiligheid van bedrijven en ICS te waarborgen.

   Dit omvat ook documenten die specifiek de malware 'Black Energy' betreffen.

2. een overzicht van de gevallen waar malware in ICS werd vastgesteld. Indien een dergelijk overzicht niet bestaat, dan zou u graag kopieën van brondocumenten, waaronder communicatie, ontvangen waarvan op basis van die documenten zelf een overzicht gemaakt kan worden waaruit blijkt bij welke partij, op welke plaats(en), wat voor soort malware is aangetroffen en, hoe, wanneer en door wie dit verwijderd is en met welke kosten.

   Dit omvat ook documenten die specifiek de malware 'Black Energy' betreffen.

Proces
U heeft Wob-verzoeken van vergelijkbare strekking bij een aantal andere bestuursorganen ingediend, met name de Nationaal Coördinator Terrorisme en Veiligheid (NCTV), Rijkswaterstaat (RWS) en de Algemene Inlichtingen- en Veiligheidsdienst (AIVD).

Bij brief van 10 januari 2019 heb ik de ontvangst van uw verzoek aan u bevestigd.

Bij brief van 28 januari 2019 is de termijn om op uw verzoek te beslissen met vier weken verlengd.

U heeft op 19 februari 2019 uw Wob-verzoek toegelicht aan de NCTV. In dit overleg zijn nadere afspraken gemaakt over de wijze waarop invulling wordt gegeven aan uw verzoek, nl.:

- van het verzoek om de onder 2. van het Wob-verzoek genoemde kopie van de incidentenregistratie wordt afgezien;
- documenten bevattende analyses over malware in ICS met meer contextuele informatie en duiding worden, voor zover mogelijk, wel met u gedeeld.

Op 8 maart 2019 is telefonisch verzocht om instemming dat ik deze afspraken kon meewegen bij de beoordeling welke informatie binnen de reikwijdte van uw verzoek valt. U heeft in reactie hierop aangegeven ook geïnteresseerd te zijn "in de communicatie tussen de BZK en de andere ministeries, ook omdat we geïnteresseerd zijn in de coördinerende rol van BZK over dit onderwerp."
Uit uw reactie maak ik op dat de afspraken die gemaakt zijn met de NCTV, niet van toepassing zijn op uw Wob-verzoek zoals ingediend bij mijn ministerie.

Wettelijk kader
Uw verzoeken vallen onder de reikwijdte van de Wob. Voor de relevante Wob-artikelen verwijs ik u naar de bijlage 1.

Inventarisatie documenten
Op basis van uw verzoek zijn in totaal 7 documenten aangetroffen. Deze documenten zijn opgenomen in een inventarislijst, die als bijlage 2 bij dit besluit is gevoegd.

Beoordeling van uw verzoek
U heeft uw verzoek ook ingediend bij de AIVD. De DG AIVD zal een besluit nemen op uw verzoek onder de inzagebepalingen van de Wet op de inlichtingen- en veiligheidsdiensten 2017.

De documenten met nummers 1-4 uit de inventarislijst zijn documenten die door de NCTV zijn opgesteld. Hiervoor verwijs ik u naar het besluit van de NCTV op uw Wob-verzoek inzake Malware ICS. Document nummer 6 uit de inventarislijst is een document dat door RWS is opgesteld. Voor dit document verwijs ik u naar het besluit van RWS op uw verzoek inzake spionage ICS.

Tot slot zijn twee documenten geïnventariseerd die reeds openbaar zijn. De Wob is niet van toepassing op al openbare documenten. Om u ten dienste te zijn stuur ik de twee documenten met nummers 5 en 7 naar u op (bijlagen 3 en 4). Voor de overige documenten verwijs ik u, zoals hierboven beschreven, naar het besluit van de NCTV en RWS.

<u>Algemeen</u>
In uw verzoek merkt u op dat de Volkskrant graag meer inzicht zou willen krijgen in daadwerkelijke registraties van malware in ICS, het beleid ten aanzien van

dergelijke malware en maatregelen die zijn genomen om aanvallen te voorkomen. Voor informatiebeveiliging gelden Rijksbrede kaders, die ook van toepassing zijn op de vitale infrastructuur bij de Rijksdienst.

Voor uw informatie geef ik hier een korte beschrijving van het geldende beleidskader. Dit kader valt buiten uw verzoek, maar neem ik ter informatie in dit besluit op.

Rijksbeleid
Hieronder schets ik het algemene beleidskader.

In het Besluit voorschrift Informatiebeveiliging rijksdienst 2007 (https://wetten.overheid.nl/BWBR0022141/2007-07-01 VIR) is vastgelegd hoe de Rijksoverheid omgaat met de beveiliging van haar informatie, waaronder gerubriceerde of geclassificeerde informatie. Deze regeling stelt minimumeisen aan het te ontwikkelen beveiligingsbeleid binnen een ministerie.

Het Besluit Voorschrift Informatiebeveiliging Rijksdienst-Bijzondere Informatie 2013 https://wetten.overheid.nl/BWBR0033507/2013-06-01 (VIRBI 2013) geeft regels voor de beveiliging van gerubriceerde informatie bij de rijksdienst.

Het VIR en VIRBI beschrijven aan welke eisen het beveiligingsbeleid moet voldoen, gegeven de gevoeligheid van de informatie. Ter uitvoering hiervan is de Baseline Informatiebeveiliging Rijksdienst (BIR) vastgesteld. Hierin worden specifieke maatregelen benoemd om invulling te geven aan de VIR en VIRBI. De onderdelen van de Rijksoverheid, waaronder Rijkswaterstaat, hebben de BIR geïmplementeerd voor informatievoorzieningen of vertalen de eisen van de BIR in contracteisen voor aan te schaffen IT voorzieningen en te leveren diensten.

In 2018 is een nieuwe versie van de BIR vastgesteld binnen het Rijk; de BIR 2017. https://www.cip-overheid.nl/wp-content/uploads/2018/05/20180210-BIR2017-definitief.pdf. De BIR 2017 schrijft detectie van spionage/sabotage door statelijke actoren voor vanaf basisbeveiligingsniveau 2 (BBN2).

Andere overheidslagen beschikten tot voor kort ieder over eigen baselines die vergelijkbaar waren met BIR2012. Thans geldt voor de gehele overheid de Baseline Informatiebeveiliging Overheid (BIO 1.0) die in december jl. in de ministerraad is bekrachtigd. De BIO bevat weliswaar geen specifieke bepalingen ten aanzien van ICS, maar geldt voor alle informatiesystemen en -processen en daarmee impliciet ook voor ICS.

Samenwerkingsverbanden Rijksdienst
Bovengenoemd beleid en initiatieven vloeien voort uit mijn verantwoordelijkheid voor de coördinatie op het gebied van de informatievoorziening in de openbare sector als geheel (artikel 5, Besluit informatievoorziening in de rijksdienst 1990). (https://wetten.overheid.nl/BWBR0004976/1990-12-01) Voor de Rijksdienst heb ik de bevoegdheid om na overleg met de ministers kaders vast te stellen ter bevordering van de eenheid, de kwaliteit of de efficiëntie van de bedrijfsvoering door de ministeries (artikel 2 lid 1, Coördinatiebesluit organisatie en

bedrijfsvoering rijksdienst, https://wetten.overheid.nl/BWBR0029514/2018-10-13). Hiertoe behoren ook de kaders ten aanzien van de informatiebeveiliging bij de rijksdienst.

Rijksbrede beleidskaders worden in interdepartementaal overleg vastgesteld. Dergelijk overleg staat ook ten dienste van het monitoren van de effectiviteit van beleid. Ook wordt interdepartementaal op diverse manieren veelvuldig kennis gedeeld over informatiebeveiliging. Onder voorzitterschap van de directeur-generaal Overheidsorganisatie (BZK) vindt overleg plaats in de Interdepartementale Commissie Bedrijfsvoering Rijk (ICBR). Voor onderwerpen op het gebied van informatievoorziening en ICT adviseert het beraad van de departementale CIO's, het CIO Beraad onder voorzitterschap van de CIO Rijk, aan de ICBR. Op zijn beurt adviseert het rijksbrede CISO overleg, waaraan de CISO's van alle ministeries deelnemen, aan het CIO-beraad over rijksbrede onderwerpen op het gebied van informatiebeveiliging. Het gaat daarbij om bijvoorbeeld het vaststellen (en de herziening) van rijksbrede kaders, beleid en tools voor informatiebeveiliging (IB).

Onder voorzitterschap van de CIO Rijk worden strategische informatiebeveiligingsonderwerpen besproken in het Strategische Informatiebeveiligingsberaad van de Rijksdienst (SIB). In de SIB heeft een aantal departementen plaats samen met Nationaal Cyber Security Centrum (NCSC, onderdeel van het ministerie van Justitie en Veiligheid) alsmede het Nationaal Bureau Verbindingsbeveiliging (NBV, onderdeel van de Algemene Inlichtingen en Veiligheidsdienst) en de Rijks-BVA.

De uitvoering van de kaders hoort bij de betreffende ministers omdat zij zelf verantwoordelijk voor de informatiebeveiliging bij hun ministerie.

Informatiebeveiliging bij medeoverheden
Ook medeoverheden zijn in beginsel zelf verantwoordelijk voor de eigen informatiebeveiliging.

Om uitwerking te geven aan het treffen van adequate beveiligingsmaatregelen binnen de overheid is de eerder genoemde BIO vastgesteld als normenkader voor informatiebeveiliging bij de overheid. De overheidsbrede maatregelen, gericht op het verhogen van de informatieveiligheid bij de overheid, zijn in oktober vorig jaar aan de Tweede Kamer aangeboden.
https://zoek.officielebekendmakingen.nl/kst-26643-574.html

Wijze van openbaarmaking
Dit Wob-besluit wordt enkele werkdagen na toezending gepubliceerd op de website www.rijksoverheid.nl.

Ik vertrouw erop u hiermee voldoende te hebben geïnformeerd.

Hoogachtend,
De minister van Binnenlandse Zaken en Koninkrijksrelaties,
namens deze,

drs. M.R. Schurink
Secretaris-generaal

Belanghebbenden kunnen binnen zes weken na bekendmaking van dit besluit daartegen per brief bezwaar maken bij de minister van Binnenlandse Zaken en Koninkrijksrelaties, DGOO, Postbus 20011, 2500 EA Den Haag. Het bezwaarschrift moet zijn ondertekend, voorzien zijn van een datum alsmede de naam en het adres van de indiener en dient vergezeld te gaan van de gronden waarop het bezwaar berust en, zo mogelijk, een afschrift van het besluit waartegen het bezwaar is gericht.

Bijlage 1 – Relevante artikelen uit de Wob

Artikel 1

In deze wet en de daarop berustende bepalingen wordt verstaan onder:

a. document: een bij een bestuursorgaan berustend schriftelijk stuk of ander materiaal dat gegevens bevat;
b. bestuurlijke aangelegenheid: een aangelegenheid die betrekking heeft op beleid van een bestuursorgaan, daaronder begrepen de voorbereiding en de uitvoering ervan;
c. intern beraad: het beraad over een bestuurlijke aangelegenheid binnen een bestuursorgaan, dan wel binnen een kring van bestuursorganen in het kader van de gezamenlijke verantwoordelijkheid voor een bestuurlijke aangelegenheid;
d. niet-ambtelijke adviescommissie: een van overheidswege ingestelde instantie, met als taak het adviseren van een of meer bestuursorganen en waarvan geen ambtenaren lid zijn, die het bestuursorgaan waaronder zij ressorteren adviseren over de onderwerpen die aan de instantie zijn voorgelegd. Ambtenaren, die secretaris of adviserend lid zijn van een adviesinstantie, worden voor de toepassing van deze bepaling niet als leden daarvan beschouwd;
e. ambtelijke of gemengd samengestelde adviescommissie: een instantie, met als taak het adviseren van één of meer bestuursorganen, die geheel of gedeeltelijk is samengesteld uit ambtenaren, tot wier functie behoort het adviseren van het bestuursorgaan waaronder zij ressorteren over de onderwerpen die aan de instantie zijn voorgelegd;
f. persoonlijke beleidsopvatting: een opvatting, voorstel, aanbeveling of conclusie van een of meer personen over een bestuurlijke aangelegenheid en de daartoe door hen aangevoerde argumenten;
g. milieu-informatie: hetgeen daaronder wordt verstaan in artikel 19.1a van de Wet milieubeheer;
h. hergebruik: het gebruik van informatie die openbaar is op grond van deze of een andere wet en die is neergelegd in documenten berustend bij een overheidsorgaan, voor andere doeleinden dan het oorspronkelijke doel binnen de publieke taak waarvoor de informatie is geproduceerd;
i. overheidsorgaan:
   1°. een orgaan van een rechtspersoon die krachtens publiekrecht is ingesteld,
   2°. een ander persoon of college, met enig openbaar gezag bekleed.

Artikel 3

1. Een ieder kan een verzoek om informatie neergelegd in documenten over een bestuurlijke aangelegenheid richten tot een bestuursorgaan of een onder verantwoordelijkheid van een bestuursorgaan werkzame instelling, dienst of bedrijf.
2. De verzoeker vermeldt bij zijn verzoek de bestuurlijke aangelegenheid of het daarop betrekking hebbend document, waarover hij informatie wenst te ontvangen.
3. De verzoeker behoeft bij zijn verzoek geen belang te stellen.

4. Indien een verzoek te algemeen geformuleerd is, verzoekt het bestuursorgaan de verzoeker zo spoedig mogelijk om zijn verzoek te preciseren en is het hem daarbij behulpzaam.
5. Een verzoek om informatie wordt ingewilligd met inachtneming van het bepaalde in de artikelen 10 en 11.

Artikel 6

1. Het bestuursorgaan beslist op het verzoek om informatie zo spoedig mogelijk, doch uiterlijk binnen vier weken gerekend vanaf de dag na die waarop het verzoek is ontvangen.
2. Het bestuursorgaan kan de beslissing voor ten hoogste vier weken verdagen. Van de verdaging wordt voor de afloop van de eerste termijn schriftelijk gemotiveerd mededeling gedaan aan de verzoeker.
3. Onverminderd artikel 4:15 van de Algemene wet bestuursrecht wordt de termijn voor het geven van een beschikking opgeschort gerekend vanaf de dag na die waarop het bestuursorgaan de verzoeker meedeelt dat toepassing is gegeven aan artikel 4:8 van de Algemene wet bestuursrecht, tot de dag waarop door de belanghebbende of belanghebbenden een zienswijze naar voren is gebracht of de daarvoor gestelde termijn ongebruikt is verstreken.
4. Indien de opschorting, bedoeld in het derde lid, eindigt, doet het bestuursorgaan daarvan zo spoedig mogelijk mededeling aan de verzoeker, onder vermelding van de termijn binnen welke de beschikking alsnog moet worden gegeven.
5. Indien het bestuursorgaan heeft besloten informatie te verstrekken, wordt de informatie verstrekt tegelijk met de bekendmaking van het besluit, tenzij naar verwachting een belanghebbende bezwaar daar tegen heeft, in welk geval de informatie niet eerder wordt verstrekt dan twee weken nadat de beslissing is bekendgemaakt.
6. Voor zover het verzoek betrekking heeft op het verstrekken van milieu-informatie:

a. bedraagt de uiterste beslistermijn in afwijking van het eerste lid twee weken indien het bestuursorgaan voornemens is de milieu-informatie te verstrekken terwijl naar verwachting een belanghebbende daar bezwaar tegen heeft;
b. kan de beslissing slechts worden verdaagd op grond van het tweede lid, indien de omvang of de gecompliceerdheid van de milieu-informatie een verlenging rechtvaardigt;
c. zijn het derde en vierde lid niet van toepassing.

Artikel 7

1. Het bestuursorgaan verstrekt de informatie met betrekking tot de documenten die de verlangde informatie bevatten door:
   a. kopie ervan te geven of de letterlijke inhoud ervan in andere vorm te verstrekken,
   b. kennisneming van de inhoud toe te staan,
   c. een uittreksel of een samenvatting van de inhoud te geven, of
   d. inlichtingen daaruit te verschaffen.

2. Het bestuursorgaan verstrekt de informatie in de door de verzoeker verzochte vorm, tenzij:
   a. het verstrekken van de informatie in die vorm redelijkerwijs niet gevergd kan worden;
   b. de informatie reeds in een andere, voor de verzoeker gemakkelijk toegankelijke vorm voor het publiek beschikbaar is.

3. Indien het verzoek betrekking heeft op milieu-informatie als bedoeld in artikel 19.1a, eerste lid, onder b, van de Wet milieubeheer, verstrekt het bestuursorgaan, zo nodig, en indien deze informatie voorhanden is, tevens informatie over de methoden die zijn gebruikt bij het samenstellen van eerstbedoelde informatie.

Artikel 10

1. Het verstrekken van informatie ingevolge deze wet blijft achterwege voor zover dit:
   a. de eenheid van de Kroon in gevaar zou kunnen brengen;
   b. de veiligheid van de Staat zou kunnen schaden;
   c. bedrijfs- en fabricagegegevens betreft, die door natuurlijke personen of rechtspersonen vertrouwelijk aan de overheid zijn meegedeeld;
   d. persoonsgegevens betreft als bedoeld in paragraaf 2 van hoofdstuk 2 van de Wet bescherming persoonsgegevens, tenzij de verstrekking kennelijk geen inbreuk op de persoonlijke levenssfeer maakt.

2. Het verstrekken van informatie ingevolge deze wet blijft eveneens achterwege voor zover het belang daarvan niet opweegt tegen de volgende belangen:
   a. de betrekkingen van Nederland met andere staten en met internationale organisaties;
   b. de economische of financiële belangen van de Staat, de andere publiekrechtelijke lichamen of de in artikel 1a, onder c en d, bedoelde bestuursorganen;
   c. de opsporing en vervolging van strafbare feiten;
   d. inspectie, controle en toezicht door bestuursorganen;
   e. de eerbiediging van de persoonlijke levenssfeer;
   f. het belang, dat de geadresseerde erbij heeft als eerste kennis te kunnen nemen van de informatie;
   g. het voorkomen van onevenredige bevoordeling of benadeling van bij de aangelegenheid betrokken natuurlijke personen of rechtspersonen dan wel van derden.
3. Het tweede lid, aanhef en onder e, is niet van toepassing voor zover de betrokken persoon heeft ingestemd met openbaarmaking.
4. Het eerste lid, aanhef en onder c en d, het tweede lid, aanhef en onder e, en het zevende lid, aanhef en onder a, zijn niet van toepassing voor zover het milieu-informatie betreft die betrekking heeft op emissies in het milieu. Voorts blijft in afwijking van het eerste lid, aanhef en onder c, het verstrekken van milieu-informatie uitsluitend achterwege voor zover het belang van openbaarmaking niet opweegt tegen het daar genoemde belang.

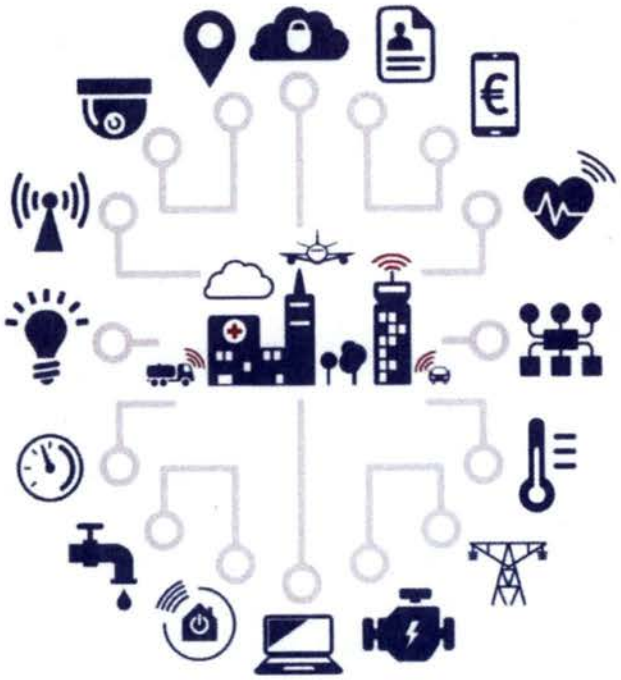
5. Het tweede lid, aanhef en onder b, is van toepassing op het verstrekken van milieu-informatie voor zover deze handelingen betreft met een vertrouwelijk karakter.
6. Het tweede lid, aanhef en onder g, is niet van toepassing op het verstrekken van milieu-informatie.
7. Het verstrekken van milieu-informatie ingevolge deze wet blijft eveneens achterwege voor zover het belang daarvan niet opweegt tegen de volgende belangen:
   a. de bescherming van het milieu waarop deze informatie betrekking heeft;
   b. de beveiliging van bedrijven en het voorkomen van sabotage.
8. Voor zover het vierde lid, eerste volzin, niet van toepassing is, wordt bij het toepassen van het eerste, tweede en zevende lid op milieu-informatie in aanmerking genomen of deze informatie betrekking heeft op emissies in het milieu.

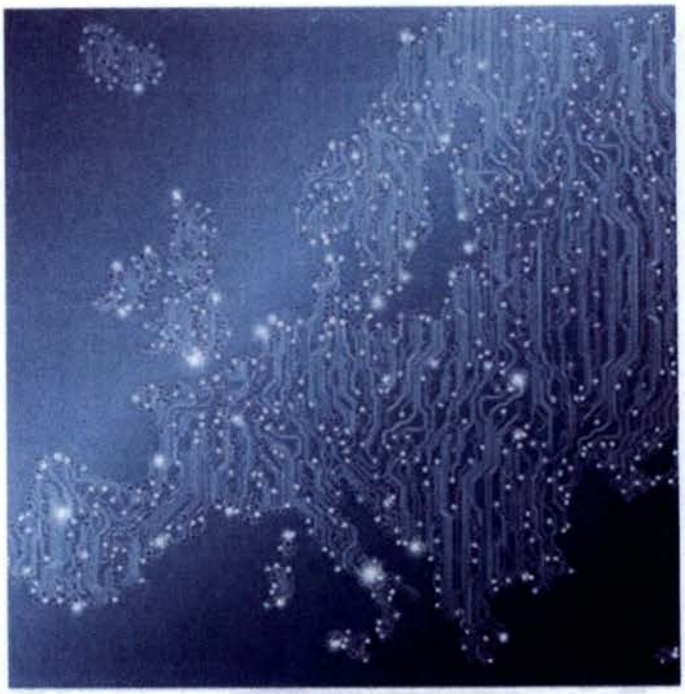
Artikel 11

1. In geval van een verzoek om informatie uit documenten, opgesteld ten behoeve van intern beraad, wordt geen informatie verstrekt over daarin opgenomen persoonlijke beleidsopvattingen.
2. Over persoonlijke beleidsopvattingen kan met het oog op een goede en democratische bestuursvoering informatie worden verstrekt in niet tot personen herleidbare vorm. Indien degene die deze opvattingen heeft geuit of zich erachter heeft gesteld, daarmee heeft ingestemd, kan de informatie in tot personen herleidbare vorm worden verstrekt.
3. Met betrekking tot adviezen van een ambtelijke of gemengd samengestelde adviescommissie kan het verstrekken van informatie over de daarin opgenomen persoonlijke beleidsopvattingen plaatsvinden, indien het voornemen daartoe door het bestuursorgaan dat het rechtstreeks aangaat aan de leden van de adviescommissie voor de aanvang van hun werkzaamheden kenbaar is gemaakt.
4. In afwijking van het eerste lid wordt bij milieu-informatie het belang van de bescherming van de persoonlijke beleidsopvattingen afgewogen tegen het belang van openbaarmaking. Informatie over persoonlijke beleidsopvattingen kan worden verstrekt in niet tot personen herleidbare vorm. Het tweede lid, tweede lid is van overeenkomstige toepassing.

Bijlage 2 - Inventarislijst

Nr.	Document	Beoordeling
1.	NCSC Maandmonitor januari 2016	JenV
2.	NCSC Maandmonitor april 2016	JenV
3.	NCSC Maandmonitor juni 2017	JenV
4.	NCSC Maandmonitor oktober 2018	JenV
5.	ENISA Baseline Security Recommendations for IoT	Reeds openbaar
6.	RWS Cyber Security Strategie 1.0	RWS
7.	RWS Cybersecurity Implementatie Objecten	Reeds openbaar





Baseline Security Recommendations for IoT

in the context of Critical Information Infrastructures

NOVEMBER 2017

www.enisa.europa.eu

European Union Agency For Network And Information Security

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact

For contacting the authors please use resilience@enisa.europa.eu.
For media enquiries about this paper, please use press@enisa.europa.eu.

Acknowledgements

Over the course of this study, we have received valuable input and feedback from:

Mirko Ross	Digital Worx GmbH
Hannes Tschofenig	ARM Ltd.
Antonio J. Jara	HOP Ubiquitous S.L. (HOPU)
Carlos Valderrama	Geomantis Corporation Limited
Alessandro Cosenza	Bticino S.p.A.
Vyacheslav Zolotnikov	Kaspersky Lab
Yun Shen	Symantec Corporation
Sylvie Wuidart	STMicroelectronics N.V.
Paul Murdock	Landis+Gyr AG
Caroline Greer	Cloudflare, Inc.
Marc Rogers	Cloudflare, Inc.
Julio Hernández Castro	University of Kent
Jacques Kruse-Brandao	NXP Semiconductors N.V.
Barbara Pareglio	GSM Association (GSMA)
Jesus Luna Garcia	Robert Bosch GmbH
Vangelis Gazis	Huawei Technologies Co., Ltd.
Wolfgang Klasen	Siemens AG
Hans Aschauer	Siemens AG
Cédric Lévy-Bencheton	
Andrei Robachevsky	Internet Society (ISOC)
Steve Olshansky	Internet Society (ISOC)
Gianmarco Baldini	EC DG Joint Research Centre (JRC)
Michael Glenn	Cable Television Laboratories, Inc. (CableLabs)
Benedikt Abendroth	Microsoft Corporation
Aaron Kleiner	Microsoft Corporation
Mike Edwards	International Business Machines Corporation (IBM)
Filip Chytrý	Avast Software s.r.o.
Mahmoud Ghaddar	Legrand S.A.
Europol/EC3	

EC DG CONNECT E4

Finally, we thank the experts of the ENISA IoT Security (IoTSec) Expert Group and all participants to the ENISA validation workshop in The Hague in October 2017 for providing us useful feedback during discussions and interviews.

ISBN: 978-92-9204-236-3, doi: 10.2824/03228

Table of Contents

Executive Summary 7

Index of tables 9

Index of figures 10

1. Introduction 11

1.1 Objectives 11

1.2 Scope 12

1.3 EU and International Policy context 13

1.4 Target audience 15

1.5 Methodology 16

1.6 Structure 16

2. The IoT paradigm 18

2.1 Elements of IoT 19

2.1.1 Things in the Internet of Things 19
2.1.2 Intelligent decision making 19
2.1.3 Sensors and actuators 19
2.1.4 Embedded systems 20
2.1.5 Communications 21

2.2 Security considerations 22

2.3 Challenge of defining horizontal baseline security measures 23

2.4 Architecture 24

2.5 Asset taxonomy 26

3. Threats and risk analysis 30

3.1 Security incidents 30

3.2 Threat taxonomy 31

3.3 Examples of IoT cyber security attack scenarios 35

3.4 Critical attack scenarios 38

3.4.1 Attack scenario 1: IoT administration system compromise 39
3.4.2 Attack scenario 2: Value manipulation in IoT devices 41
3.4.3 Attack scenario 3: Botnet / Commands injection 43

4. Security measures and good practices 46

4.1 Policies 47

4.1.1 Security by design 47
4.1.2 Privacy by design 47
4.1.3 Asset Management 48
4.1.4 Risk and Threat Identification and Assessment 48

4.2 Organisational, People and Process measures 48
4.2.1 End-of-life support 48
4.2.2 Proven solutions 48
4.2.3 Management of security vulnerabilities and/or incidents 48
4.2.4 Human Resources Security Training and Awareness 48
4.2.5 Third-Party relationships 48

4.3 Technical Measures 49
4.3.1 Hardware security 49
4.3.2 Trust and Integrity Management 49
4.3.3 Strong default security and privacy 49
4.3.4 Data protection and compliance 49
4.3.5 System safety and reliability 50
4.3.6 Secure Software / Firmware updates 50
4.3.7 Authentication 50
4.3.8 Authorisation 50
4.3.9 Access Control - Physical and Environmental security 50
4.3.10 Cryptography 51
4.3.11 Secure and trusted communications 51
4.3.12 Secure Interfaces and network services 51
4.3.13 Secure input and output handling 51
4.3.14 Logging 52
4.3.15 Monitoring and Auditing 52

5. Gaps analysis 53

5.1 Gap 1: Fragmentation in existing security approaches and regulations 53

5.2 Gap 2: Lack of awareness and knowledge 54

5.3 Gap 3: Insecure design and/or development 54

5.4 Gap 4: Lack of interoperability across different IoT devices, platforms and frameworks 55

5.5 Gap 5: Lack of economic incentives 55

5.6 Gap 6: Lack of proper product lifecycle management 55

6. High-level recommendations to improve IoT cybersecurity 57

6.1 Recommendations 57

6.2 Detailed recommendations 57
6.2.1 Promote harmonization of IoT security initiatives and regulations 57
6.2.2 Raise awareness for the need for IoT cybersecurity 58
6.2.3 Define secure software/hardware development lifecycle guidelines for IoT 58
6.2.4 Achieve consensus for interoperability across the IoT ecosystem 59
6.2.5 Foster economic and administrative incentives for IoT security 59

6.2.6	Establishment of secure IoT product/service lifecycle management	59
6.2.7	Clarify liability among IoT stakeholders	60
Glossary		**61**
Annex A:	**Detailed Security measures / Good practices**	**63**
Annex B:	**Security measures and threats mapping**	**82**
Annex C:	**Security standards and references reviewed**	**88**
Annex D:	**Description of indicative IoT security incidents**	**100**

Executive Summary

The Internet of Things (IoT) is a growing paradigm with technical, social, and economic significance. For ENISA, IoT is an emerging concept comprising a wide ecosystem of interconnected services and devices, such as sensors, consumer products and everyday smart home objects, cars, and industrial and health components. These technologies collect, exchange and process data in order to dynamically adapt to a specific context, transforming the business world and the way we live as a whole. IoT is tightly bound to cyber-physical systems and, in this respect, safety implications are pertinent.

Nevertheless, IoT poses very important safety and security challenges that need to be addressed for IoT to reach its full potential. Many security considerations regarding IoT are not necessarily new; they are inherited from the use of networking technologies. However, the characteristics of some IoT implementations present new security challenges, threats and risks that are manifold and evolve rapidly. The protection of IoT deployments depends on the protection of all systems involved (the devices themselves, cloud backend and services, applications, maintenance and diagnostic tools, etc.).

Addressing these challenges and ensuring security in IoT products and services is a fundamental priority. One of the main concerns is the impact that the different threats may have since attacks on IoT deployments could dramatically jeopardise people's security, privacy and safety, while additionally IoT in itself can be used as an attack vector against other critical infrastructures. Also, since IoT can drastically change the ways personal data is collected, analysed, used, and protected, privacy concerns have been raised. These need to be addressed to ensure user trust and confidence in the Internet, connected devices, and related services.

However, beyond technical security measures, the adoption of IoT has raised many new legal, policy and regulatory challenges, broad and complex in scope, that remain unanswered, amplifying at the same time some existing issues. The rapid rate of change in IoT technology has outpaced the ability of the associated policy, legal, and regulatory structures to adapt, leaving no clear security framework to follow. This has led most companies and manufacturers to take their own approach when designing IoT devices, causing interoperability issues between devices from different manufacturers, and between IoT devices and legacy systems.

For these reasons, ENISA is defining a set of Baseline Security Recommendations for IoT. The aim of this work as reported here is to provide insight into the security requirements of IoT, mapping critical assets and relevant threats, assessing possible attacks and identifying potential good practices and security measures to apply in order to protect IoT systems.

As a result of this work, after taking into consideration all the background research carried out, the views expressed by the experts interviewed, and the good practices and security measures identified, a series of recommendations has been developed, namely:

- Promote harmonization of IoT security initiatives and regulations
  Intended for IoT industry, providers, manufacturers, associations
- Raise awareness for the need for IoT cybersecurity
  Intended for IoT industry, providers, manufacturers, associations, academia, consumer groups, regulators
- Define secure software/hardware development lifecycle guidelines for IoT
  Intended for IoT developers, platform operators, industry, manufacturers

- Achieve consensus for interoperability across the IoT ecosystem
  Intended for IoT industry, providers, manufacturers, associations, regulators
- Foster economic and administrative incentives for IoT security
  Intended for IoT industry, associations, academia, consumer groups, regulators
- Establishment of secure IoT product/service lifecycle management
  Intended for IoT developers, platform operators, industry, manufacturers
- Clarify liability among IoT stakeholders
  Intended for IoT industry, regulators

Index of tables

Table 1	Indicative listing of communication protocols for IoT	**22**
Table 2	Asset taxonomy	**28**
Table 3	Threat taxonomy	**35**
Table 4	IoT attack scenarios	**36**
Table 5	Attack 1 – IoT administration system compromise	**41**
Table 6	Attack 2 – Value manipulation in IoT devices	**43**
Table 7	Attack 3 – Botnet / Commands injection	**45**
Table 8	IoT Security Recommendations	**57**

Index of figures

Figure 1: Methodology followed in the study 16

Figure 2: IoT pervasive ecosystem 18

Figure 3: Structure of an IoT embedded system 21

Figure 4: IoT High-level reference model 25

Figure 5: Asset taxonomy 26

Figure 6: Asset criticality 28

Figure 7: Indicative timeline of IoT security incidents 30

Figure 8: IoT Threat taxonomy 32

Figure 9: IoT threats impact 33

Figure 10: Threat impact weighted average 33

Figure 11: Attack scenario criticality 39

Figure 12: Attack 1 – IoT administration system compromised 40

Figure 13: Attack 2 – Value manipulation in IoT devices 42

Figure 14: Attack 3 – Botnet / Commands injection 44

1. Introduction

The Internet of Things (IoT) is concept paradigm that has emerged over the last years. Kevin Ashton introduced the concept of IoT back in 1999[1]. It describes a wide ecosystem where interconnected devices and services collect, exchange and process data in order to adapt dynamically to a context. The Internet of Things is tightly bound to cyber-physical systems and in this respect is an enabler of Smart Infrastructures by enhancing their quality of service provisioning.

The IoT is the natural evolution of computing and it brings its own challenges – an immature ecosystem bearing a fragmentation of standards and security concerns in a non-homogeneous IoT market, as at the moment each industry and application is different. Another IoT challenge worth highlighting is its ability to scale globally[2]; according to Gartner, IoT will involve 8.4 billion connected 'things' in use in 2017, up 31% from 2016, and by 2020 the number of connected devices is envisioned to reach 20 billion[4][1]. Currently there are different solutions available in the market through various manufacturers such as Google, Microsoft, Amazon, Apple or Samsung, among others, many of which use their proprietary cloud service, protocols and operating system[3].

The threats and risks related to the Internet of Things devices, systems and services are manifold, and evolve rapidly. With a great impact on citizens' safety, security and privacy, the threat landscape concerning the Internet of Things is extremely wide. Hence, it is important to understand what needs to be secured and to develop specific security measures to protect the Internet of Things from cyber threats.

Involving billions of intelligent systems and millions of applications, IoT will drive new consumer and business behaviours, which will demand increasingly intelligent solutions. This, in turn, is expected to drive by 2020 almost 3 trillion dollars (circa 2.85 trillion euros) in new business opportunities for the different vendors and companies that capitalise on the IoT[4][1]. Examples of these opportunities include[4]:

- New business models: New value streams for customers, with a faster response.
- Diversification of revenue streams: Monetising added services on top of traditional lines of business.
- Real-time information: Capturing data about products and processes more swiftly, improving market agility and allowing prompt decision making.
- Global visibility: Making tracking easier from one end of a supply chain to the other.

1.1 Objectives

The goal of this report is to elaborate baseline cybersecurity recommendations for IoT with a focus on Critical Information Infrastructures, which encompass facilities, networks, services and physical and information technology equipment. These infrastructures are considered critical because their destruction or disruption could bring about major consequences for the health, safety and economic wellbeing of citizens, for the efficient functioning of State institutions and Public Administrations[5,6], and for the asset owners who make use of IoT to provide their services.

---

[1] See http://www.rfidjournal.com/articles/view?4986
[2] See https://www.emc.com/leadership/digital-universe/2014iview/internet-of-things.htm
[3] See https://hacks.mozilla.org/2017/06/building-the-web-of-things/
[4] See https://www.emc.com/leadership/digital-universe/2014iview/internet-of-things.htm
[5] See https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure_en
[6] See https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services

In this respect, the baseline security measures for IoT put forward in this report can serve as a springboard for further related efforts towards a harmonised EU approach, paving the way for a tacit adoption of the measures, and as criteria for other initiatives such as labelling or certification.

A major challenge in defining baseline security measures for IoT is the entailed complexity that is brought by the diversity of application areas for IoT. Striking a balance between the particularities of each domain is essential and accordingly it is important to consider the differences in apportioning risk to distinct environments. Accordingly, this report builds on the expertise and insight gained by previous work by ENISA, covering a series of vertical application areas of IoT namely:

- Smart Homes[7]
- Smart Cities and Intelligent Public Transport[8]
- Smart Grids[9]
- Smart Cars[10]
- Smart Airports[11]
- eHealth and Smart Hospitals[12]

This report aims to cover the threat model of the Internet of Things in the context of Critical Information Infrastructures (CII), as well as to detail available security measures to counter the identified threats. This report also provides a series of recommendations to shape future efforts and initiatives in the direction of a holistic approach to secure the Internet of Things.

1.2 Scope

ENISA defines the Internet of Things (IoT) as *a cyber-physical ecosystem of interconnected sensors and actuators, which enable decision making*. Information lies at the heart of IoT, feeding into a continuous cycle of sensing, decision making, and actions. IoT is tightly bound to cyber-physical systems and in this respect is an enabler of Smart Infrastructures, e.g. Industry 4.0, smart grid, smart transport, by enabling services of higher quality and facilitating the provision of advanced functionalities.

ENISA identified and analysed existing IoT security practices, security guidelines, relevant industry standards and research initiatives in the area of IoT security for Critical Information Infrastructures (e.g. Industry 4.0, Machine-to-Machine (M2M) communications, IoT updatability). Having reviewed and thoroughly analysed existing work and ongoing activities, ENISA compared these practices and standards and developed baseline security measures to be adopted by relevant stakeholders.

ENISA focused, among other topics, on IoT resilience and communication, on the interoperability with proprietary systems, and on the reliability of IoT. Special emphasis was given to the privacy issues of such smart infrastructure and services. In this endeavour, ENISA additionally took into account existing European Union (EU) policies and regulatory initiatives such as the Directive on security of network and information systems (NIS Directive)[13], The EU General Data Protection Regulation (GDPR)[14], the Internet of Things - An

[7] See https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/smart-homes
[8] See https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/smart-cities
[9] See https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/smart-grids
[10] See https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars
[11] See https://www.enisa.europa.eu/publications/securing-smart-airports
[12] See https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/health
[13] See http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN
[14] See http://www.eugdpr.org/

action plan for Europe[15], as well as the work of the Alliance for the Internet of Things (AIOTI)[16] and the Staff Working Document on ICT Standardization[17], among others.

In 2017, ENISA launched the IoT Security Experts Group (IoTSEC)[18]. The ENISA IoTSEC group is an information exchange platform that brings together experts to ensure the security and resilience of the entire Internet of Things ecosystem. Experts of the IoTSEC group have background expertise in one or several of the following:

- Internet of Things with a focus on cyber security;
- Suppliers and developers of Internet of Things hardware and/or software with a focus on cyber security;
- Associations and non-profit organisations involved in Internet of Things security;
- Regulation bodies, academia, standardisation bodies and policy makers.

The first step of the process followed by ENISA in order to validate the results of the report was to carry out a series of interviews with the different members of the IoTSEC Experts Group, where we gathered their input, obtaining new information and validating information found during the desktop research. A total of 26 experts were interviewed, covering industry, policy, academia and research organisations from 9 EU member states and from the United States of America. After synthesising all findings into this report, a release candidate version was sent to the experts that compose the IoTSEC Group for a first round of comments. Finally, during the first workshop meeting of the ENISA IoT Security Experts Group that took place in The Hague, Netherlands, on 20th of October 2017, the findings of the report were discussed and the experts shaped the final recommendations in order to reflect the needs of the IoT security community in Europe.

1.3 EU and International Policy context

In the last years, the European Commission has been working to facilitate the embracement of the IoT in Europe, and to unleash its full potential, by adopting a set of supporting policy actions and launching a series of relevant initiatives[19].

In March 2015, the European Commission launched the Alliance for Internet of Things Innovation (AIOTI)[20], with the intention of creating an innovative and industry-driven European IoT ecosystem. The AIOTI has come to be the largest European IoT Association to date, emphasising the European Commission's ambition to work closely with all IoT stakeholders on the establishment of a competitive IoT market and new business models for the benefit of the European citizens and businesses.

The Digital Single Market (DSM) Strategy[21], adopted two months later in May 2015, underlines the need to avoid fragmentation and to foster interoperability for IoT to reach its potential, leading Europe a step further in terms of IoT development. In order to meet the DSM needs and to inform about its upcoming policy, in April 2016 the European Commission specified the EU's IoT vision in the document 'Advancing the Internet of Things in Europe'[22], as part of the 'Digitising European Industry' (DEI) initiative[23].

---

[15] See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0278:FIN:EN:PDF
[16] See https://ec.europa.eu/digital-single-market/en/news/alliance-internet-things-innovation-aioti-defines-its-long-term-strategy
[17] See https://ec.europa.eu/digital-single-market/en/news/communication-ict-standardisation-priorities-digital-single-market
[18] See https://resilience.enisa.europa.eu/iot-security-experts-group-1
[19] See https://ec.europa.eu/digital-single-market/en/internet-of-things
[20] See https://ec.europa.eu/digital-single-market/en/alliance-internet-things-innovation-aioti
[21] See https://ec.europa.eu/commission/priorities/digital-single-market/
[22] See https://ec.europa.eu/digital-single-market/en/news/staff-working-document-advancing-internet-things-europe
[23] See https://ec.europa.eu/digital-single-market/en/policies/digitising-european-industry

This vision is based on three different pillars:

- A thriving IoT ecosystem,
- A human centred IoT approach,
- A single market for IoT.

The achievement of a single market for the IoT will potentially face issues linked to the capacity to handle a vast number and diversity of connected devices and the ability to identify them unequivocally and universally, so it is important to foster an open system for object identification and authentication, as well as an interoperable IoT numbering space that transcends geographical limits. Some aspects of numbering were already addressed in the 2016 review of the EU telecom rules[24].

The Commission, in their ICT Standardisation roadmap for the Digital Single Market[25], identified five priority areas that aim to guarantee a fresh approach to standards, and IoT is identified as one of these five priorities. These areas should increase competitiveness and help European innovations better access the global market. The other priorities are 5G communication, cybersecurity, cloud and Big Data.

In the context of promoting a European single market for IoT, in January 2017 the 'European data economy' initiative was presented[26]. It proposes policy and legal solutions concerning the free flow of data across national borders in the EU, and liability issues decisive to enhance legal certainty around IoT products and services. In addition to all these initiatives, the EU has arranged specific IoT objectives in the Horizon 2020 research and innovation programme[27]. The midterm review of the Digital Single Market makes numerous references to the Internet of Things, with liability and cyber security being the main areas of focus[28]. Moreover, Article 29 Data Protection Working Party Committee's "Opinion 8/2014 on the on Recent Developments on the Internet of Things" identifies the main data protection risks that lie within the ecosystem of the IoT before providing guidance on how the EU legal framework should be applied in this context[29].

The most recent action taken by the EU was on September 2017, when the new "Proposal for a Regulation Of The European Parliament And Of The Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act")" was published[30,31].

On the same date, the European Commission published the "Joint Communication To The European Parliament And The Council Resilience, Deterrence and Defence: Building strong cybersecurity for the EU"[32], which describes the overall cybersecurity strategy of the EU. The goal is to build greater EU resilience to cyber-attacks, improving detection mechanisms and strengthening international cooperation, and to do so, the document provides a series of measures, with some of them specifically oriented to IoT, such as the encouragement of "security by design" through the whole lifecycle of the devices that make up the Internet of Things. With this measure, schemes under this framework would indicate that the products are built using

---

[24] See https://ec.europa.eu/digital-single-market/en/connectivity-european-gigabit-society
[25] See https://ec.europa.eu/digital-single-market/en/news/communication-ict-standardisation-priorities-digital-single-market
[26] See https://ec.europa.eu/digital-single-market/en/building-european-data-economy
[27] See https://ec.europa.eu/digital-single-market/en/research-innovation-iot
[28] See https://ec.europa.eu/digital-single-market/en/news/digital-single-market-commission-calls-swift-adoption-key-proposals-and-maps-out-challenges
[29] See http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf
[30] See http://eur-lex.europa.eu/resource.html?uri=cellar:1985b4b4-985e-11e7-b92d-01aa75ed71a1.0001.02/DOC_1&format=PDF
[31] See http://eur-lex.europa.eu/resource.html?uri=cellar:1985b4b4-985e-11e7-b92d-01aa75ed71a1.0001.02/DOC_2&format=PDF
[32] See http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=JOIN:2017:450:FIN&from=EN

state-of-the-art secure development methods, that they have undergone adequate security testing, and that the vendors have committed to update their software in the event of newly discovered vulnerabilities or threats.

Moving from the EU to the US, it is worth highlighting the "Internet of Things Cybersecurity Improvement Act of 2017"[33], introduced on the 1st of August of 2017 by four U.S. senators, which was developed in response to a series of IoT-related cyber-attacks that took place in 2016[34]. This improvement act establishes minimum cybersecurity requirements for connected devices purchased by the U.S. Government, including[35]:

- Requiring vendors to ensure their devices are patchable, rely on industry standard protocols, do not use hard-coded passwords, and do not contain any known security vulnerabilities;
- Requiring vendors selling IoT devices are "to provide written certification that the device does not contain, at the time of submitting the proposal, any hardware, software, or firmware component with any known security vulnerabilities or defects"[36]. If a vendor identifies vulnerabilities, it must disclose them and patch them in a timely manner[37];
- Requiring each executive agency to inventory all Internet-connected devices in use by the agency;
- Along with NIST, specifying particular measures, e.g. network segmentation, for agencies to employ them;
- Directing the Department of Homeland Security's (DHS) National Protection and Programs Directorate (NPPD) to develop coordinated disclosure guidelines, allowing researchers to uncover vulnerabilities in and share them with the vendors; and
- Requiring an effectiveness report, with recommendations for updates, to be submitted to Congress after 5 years.

1.4 Target audience

This report provides a set of specific baseline security measures and recommendations that can be applied to protect IoT systems and environments. The primary target audience of the report are organisations that want to adopt IoT or are already adopting IoT solutions as well as the manufacturers and operators that provide IoT products, solutions and services. This report is also aimed at the personnel responsible for IT and/or innovation activities in their organisations, including the following profiles:

- IoT experts, software developers and manufacturers
- Information security experts
- IT/Security solutions architects
- Chief Information Security Officers (CISOs)
- Critical Information Infrastructure Protection (CIIP) experts

It is noteworthy that the recommendations of the report can prove to be beneficial to support policy making initiatives in regard to IoT security and hence are also aimed at corresponding regulators.

---

[33] See https://www.congress.gov/bill/115th-congress/senate-bill/1691/text
[34] See https://krebsonsecurity.com/tag/iot-cybersecurity-improvement-act-of-2017/
[35] See https://www.helpnetsecurity.com/2017/08/02/iot-security-legislation/
[36] See https://dzone.com/articles/internet-of-things-cybersecurity-improvement-act-o
[37] See https://www.wired.com/beyond-the-beyond/2017/08/spime-watch-fact-sheet-internet-things-cybersecurity-improvement-act-2017/

1.5 Methodology

This study was carried out using a five-step methodology (shown in Figure 1) which begins with the scope definition, the initial information gathering from official sources and experts in the field and ends in the development of a report summarizing the findings and the recommendations to the target audience.

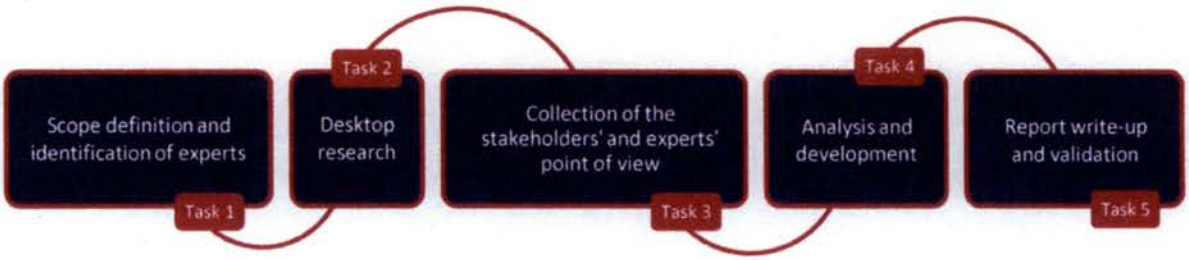


Figure 1: Methodology followed in the study

1. Scope definition and identification of experts: The first step was to establish the report's scope and perimeter and then to identify the IoT experts, so as to gather their input and knowledge in relation to the objectives of this report.

2. Desktop research: In parallel with the expert identification, an investigation was carried out to identify existing publications and information on the topics related to the objectives of the report, which will serve as support for the analysis of the threats and for the development of the security measures.

3. Collection of stakeholders' and experts' point of view: A series of interviews were conducted with the experts from the IoTSEC Experts Group, using an internally developed questionnaire to guide them and to ensure that we obtained the most relevant input.

4. Analysis and development: The results from the desktop research and the interviews were analysed and contrasted to align them with the objectives of the report, developing the assets and threats taxonomies and identifying the attack scenarios, as well as identifying the baseline security measures, the gaps and the recommendations to address them.

5. Report write-up and validation: The last step was to synthesise all the findings from the desktop research and the interviews with the experts, shaping this report, which was finally validated in the workshop meeting with the IoT experts that have collaborated in the study.

1.6 Structure

The rest of the report is structured as follows:

- Chapter 1: Introduction to the report and definition of the objective and the methodology followed to achieve it.
- Chapter 2: Definition and documentation about IoT key elements and environments.
- Chapter 3: Analysis of the main threats, vulnerabilities, risks and the development of the main attack scenarios.
- Chapter 4: Development, mapping and categorisation of the main security measures that have been identified and that apply in the scope of the report.
- Chapter 5: Gaps and future challenges applicable to the scope of the project.

- Chapter 6: Security recommendations based on the security measures developed and the gaps and challenges identified in the previous chapters.

2. The IoT paradigm

ENISA defines IoT as **"a cyber-physical ecosystem of interconnected sensors and actuators, which enable intelligent decision making"**. Stemming from the definition is the fact that information lies at the heart of IoT, feeding into a continuous cycle of sensing, decision making, and actions.

Figure 2: IoT pervasive ecosystem

Figure 2 illustrates the pervasive nature of IoT in that it is at the core of a plethora of both critical and non-critical infrastructures. IoT is pertinent to almost all aspects of daily life, affecting commercial applications, the industrialisation, or the private sphere, to name a few. Inherently, IoT builds on embedding "intelligence" in everyday objects, thus increasing the usefulness of what used to be common "things", and therefore facilitating all aspects of daily life by providing a greater automation and control in sectors such as industry, energy, transport, health, retail, etc. The majority of the sectors associated with IoT are critical, and any incident affecting them can thus severely affect society as a whole.

Industry 4.0 and Industrial Internet of Things (IIoT) are frequently and rightfully associated with IoT focusing on digitising industries[23]. Industry 4.0 is the term coined to refer to the world's fourth industrial revolution[38]. It is defined as the brisk transformation in the design, manufacture, operation and service of manufacturing systems and products, where digital technology and the Internet merge together with the conventional industry, achieving digitally connected manufacturing operations with a highly integrated value chain[38]. In this study, we focus on the more generic concept of IoT.

This chapter will provide a brief insight into the IoT elements and architecture, including the different security considerations to be taken into account.

[38] See EPRS, Ron Davies, «Industry 4.0», http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/568337/EPRS_BRI(2015)568337_EN.pdf

2.1 Elements of IoT

The following sections provide an overview of the different elements that shape the IoT ecosystem, namely the Things in the IoT, intelligent decision making, sensors and actuators, communications and embedded systems. A detailed IoT asset taxonomy can be found later in chapter 2.5.

2.1.1 Things in the Internet of Things

In IoT environments, **a thing is a physical or virtual object capable of being identified and integrated into communication networks**. It is imperative for things to have the capability of communication – exchanging data over a network between them and/or with the cloud backend services. Additionally, things may have other optional features, such as sensing and capturing data, actuating, storing and processing data, executing native or cloud-based applications, machine learning, etc[39]. The set of 'things' that compose an IoT ecosystem can be managed by intelligent systems, which are able to autonomously connect to things for monitoring and controlling them. Moreover, these intelligent systems can retrieve data from a thing or a set of things and process that data, obtaining useful information in order to make an intelligent decision[40].

2.1.2 Intelligent decision making

The number of devices connected to 'intelligent systems' that can store, process, analyse and share data is sharply increasing. This will result in billions of 'things' and machines connected to networks and producing even more data[41]. Hence, there is a need to deploy data analytics and smart data management techniques in order to draw meaningful insight from the colossal volume of data being generated[40]. Moreover, IoT encompasses the notion of actuating, for which decision making is necessary.

Intelligent decision-making depends first and foremost on the information available to make the decisions. These decisions can be as simple as a threshold-crossing mechanism, or as advanced as machine learning or deep learning systems[42]. The output of these decisions will eventually lead to actions and may feed new information into the ecosystem. The information used to make intelligent decisions can be either analysed locally, since some 'things' can process the data they gather themselves, or delegated to another element of the IoT ecosystem, such as the cloud backend service, the aggregator/gateway, another 'thing', etc.

This whole process supports several aspects, such as context awareness and adaptation, autonomy, and self-optimisation/configuration/healing/protection, to name a few.

2.1.3 Sensors and actuators

Sensors are one of the key building blocks of IoT, since they are an integral element that allows to monitor the environment and the context on which IoT systems operate. They can be as small as millimetres in size, making them easy to embed in physical objects – from roadways to pacemakers[43].

On the physical level, sensors can measure defined physical, chemical or biological indicators, and on the digital level, they collect information about the network and applications. They then generate associated quantitative data, which can be processed in real-time, or stored for later retrieval, and that can be received

---

[39] ITU-T Y.2060, «Overview of the Internet of things». See https://www.itu.int/rec/T-REC-Y.2060-201206-I

[40] European Commission, «Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination». See https://ec.europa.eu/digital-single-market/en/news/definition-research-and-innovation-policy-leveraging-cloud-computing-and-iot-combination

[41] See http://www.gartner.com/newsroom/id/3598917

[42] See https://www.forbes.com/sites/mikekavis/2014/09/04/making-sense-of-iot-data-with-machine-learning-technologies/

[43] McKinsey&Company, «The Internet of Things». See http://www.mckinsey.com/industries/high-tech/our-insights/the-internet-of-things

hundreds of kilometres away[44]. Some examples of sensors are accelerometers, temperature sensors, pressure sensors, light sensors and acoustic sensors, among others.

Even if they are left unattended in some cases (e.g. roadways), sensors have become essential in a large number of industries, gathering data for the network and applications to dynamically adapt to optimal processes at any moment[44].

An actuator can be considered as the entity responsible for moving or controlling a system or mechanism. In simple terms, an actuator operates in the reverse direction of a sensor. It takes an electrical input and turns it into physical action. Taking the example of smart lamps and smart thermostats, their actuators can make use of the signal coming from a light sensor to regulate brightness, and of the signal coming from a temperature sensor to regulate temperature, respectively. Actuators are also commonly used in manufacturing and assembly processes, where motors and solenoids are the primary examples of actuators – for example, valves are a type of actuator, used to control a hydraulic system[45].

To summarise, the functions of input devices are performed by sensors that gather information about their environment and its context, which will be subsequently processed. In contrast, actuators serve as output units – they act based on the processed information, executing decisions. It should be noted that, in most IoT deployments, sensors and actuators are not only found standalone, but also integrated into embedded systems.

2.1.4 Embedded systems

Sensors and actuators are the fundamental elements of IoT. They may be connected to the cloud backend through gateways to have the data coming from the sensors processed, in order to make a decision. Instead of only having sensor and/or actuator networks, IoT devices can also be found as embedded systems, which include embedded sensors and/or actuators, as well as network capabilities to connect directly to a LAN or to the cloud, a memory footprint and the ability to run software. Additionally, IoT embedded systems are based on a processing unit that enables them to process data on their own. Some examples of devices that contain embedded systems comprise medical implants, wearables such as smart watches, connected lights, smart thermostats, etc. Figure 3 illustrates the structure of an embedded IoT system.

[44] IEEE, «Towards a definition of the Internet of Things (IoT)». See http://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf
[45] Amirul Rayes, Samer Salam, «The Things in IoT: Sensors and Actuators». See https://link.springer.com/chapter/10.1007/978-3-319-44860-2_3

Figure 3: Structure of an IoT embedded system

2.1.5 Communications

Communication requirements vary widely among the different types of IoT networks, depending on their purpose and resource constraints[46]. The selection of protocols to be used in a particular deployment of IoT ecosystems depends on the requirements of its use-case. The combination of different protocols within IoT ecosystems is a common practice, using gateways to ensure interoperability.

IoT communication systems rely on the ability to both transmit and receive information units in a structured manner, with services located either nearby or in a distant location, using different but interoperable kinds of network types. These networks have different set of properties such as QoS, resilience, security and management[47].

The communication protocols within IoT ecosystems can be either wireless or wireline-based. There exists a plethora of wireless communication protocols, including **short-range radio protocols** such as ZigBee[48], Bluetooth/Bluetooth Low Energy (BLE)[49], Wi-Fi/Wi-Fi HaLow[50], Near Field Communication (NFC)[51] or Radio Frequency Identification (RFID)[52]; **mobile networks** and **longer-range radio protocols** such as LoRaWAN[53], SigFox[54] NarrowBand-IoT (NB-IoT)[55], or LTE-M[56]. Each of them is defined in its own standard, for example ZigBee and ZigBee 3.0 are based on IEEE 802.15.4. Wired communication protocols and links, such as Ethernet, USB, SPI, MIPI and I2C, among others, also provide access to the devices. Moreover, it is worth highlighting that IoT communications also support non-IP based protocols, such as SMS, LiDar, Radar, etc.

---

[46] Tara Salman, «Networking Protocols and Standards for Internet of Things». See https://www.cse.wustl.edu/~jain/cse570-15/ftp/iot_prot.pdf
[47] ISO/IEC, «ISO/IEC CD 30141:20160910(E) - Internet of Things Reference Architecture (IoT RA)». See https://www.w3.org/WoT/IG/wiki/images/9/9a/10N0536_CD_text_of_ISO_IEC_30141.pdf
[48] See http://www.zigbee.org/zigbee-for-developers/network-specifications/
[49] See https://www.bluetooth.com/what-is-bluetooth-technology/how-it-works/le-p2p
[50] See http://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-low-power-long-range-wi-fi-halow
[51] See http://nfc-forum.org/nfc-and-the-internet-of-things/
[52] See http://www.rfidjournal.com/articles/view?392
[53] See https://www.lora-alliance.org/technology
[54] See https://www.sigfox.com/
[55] See https://www.gsma.com/iot/narrow-band-internet-of-things-nb-iot/
[56] See https://www.gsma.com/iot/long-term-evolution-machine-type-communication-lte-mtc-cat-m1/

Wireless technologies have different characteristics, such as a specific signal range, bandwidth, etc. and can be classified as Wireless Personal Area Networks (WPAN), Wireless Local Area Networks (WLAN) or Wireless Wide Area Networks (WWAN). In ENISA's Smart Homes study[7], the different kinds of networks were also listed. Nevertheless, given the context of this study, a more generic/horizontal approach has been followed, thus remaining consistent with the Smart Homes study.

Table 1 depicts an indicative listing of different protocols grouped by communication layer. The datalink layer handles the connection between IoT devices across a physical link, either wired or wireless, for example between sensors or between a sensor and the gateway that connects a set of sensors to the Internet. The network layer is divided into the routing layer, which handles the packet transfer from the source to the destination, and into the encapsulation layer, which builds the packets. The session layer defines the protocols enabling messaging capabilities among the elements of the IoT communication subsystem[46].

SESSION		AMQP, CoAP, DDS, MQTT, XMPP
NETWORK	ENCAPSULATION	6LowPAN, Thread
	ROUTING	CARP, RPL
DATALINK		Bluetooth / BLE, Wi-Fi / Wi-Fi HaLow, LoRaWAN, Neul, SigFox, Z-Wave, ZigBee, USB

Table 1: Indicative listing of communication protocols for IoT[46]

As stated before, IoT 'things' need to both transmit and receive data, yet they do not necessarily need an Internet connection to do so, only the ability to pass the data they collect/receive on to other 'things' capable of processing that information and/or sending it over an Internet connection. Therefore, it is possible for an IoT ecosystem made up of multiple 'things' to operate without any of them being capable of connecting to the Internet[57]. The use of the word 'Internet' in the term 'Internet of Things' should simply be seen as a generalisation, implying the notion of connectivity. It should not be interpreted in a stricter, technical sense, whereby an Internet connection or the IP protocol stack would be a requirement of the IoT ecosystem.

2.2 Security considerations

As we become increasingly reliant on intelligent, interconnected devices in every aspect of our lives, the billions of "things" can be the target of intrusions and interferences that could dramatically jeopardise personal privacy and threaten public safety[58]. Therefore, security is one of the main concerns regarding IoT, which needs to be addressed along with the paramount need for safety, since both matters are tightly intertwined with the physical world. Another important aspect involves administration of IoT devices, namely who is going to be responsible for this especially considering the inherent complexity and heterogeneity of the IoT ecosystem, as well as taking into account scalability concerns.

The following are generic issues identified by this study that hinder the consolidation of secure IoT ecosystems:

- Very large attack surface: The threats and risks related to IoT are manifold and evolve rapidly. Considering their impact on citizens' health, safety and privacy (data collection and processing may be unclear to the users, since IoT is heavily based on the gathering, exchange and processing of large amounts of data from a variety of sources, sometimes including sensitive data), the threat landscape concerning IoT is extremely wide.

[57] See https://qz.com/228750/the-internet-of-things-may-not-need-an-internet-connection/
[58] See https://www.windriver.com/whitepapers/security-in-the-internet-of-things/wr_security-in-the-internet-of-things.pdf

- Limited device resources: Applying conventional security practices in IoT could require a substantial reengineering due to technical constraints. The majority of IoT devices have limited capabilities, e.g. processing, memory and power, and therefore advanced security controls cannot be effectively applied.
- Complex ecosystem: Security concerns are exacerbated since IoT should not be seen as a collection of independent devices, but rather as a rich, diverse and wide ecosystem involving aspects such as devices, communications, interfaces, and people.
- Fragmentation of standards and regulations: The fragmented and slow adoption of standards and regulations to guide the adoption of IoT security measures and good practices, as well as the continuous emergence of novel technologies, further complicate relevant concerns.
- Widespread deployment: Apart from commercial applications of IoT, recent trends have seen Critical Infrastructures (CIs) migrating toward Smart ones by employing IoT on top of legacy infrastructures.
- Security integration: This is a very challenging task, due to the presence of possibly contradicting viewpoints and requirements from all involved stakeholders. For example, different IoT devices and systems may be based on different authentication solutions, which must be integrated and made interoperable.
- Safety aspects: They are very relevant in the IoT context because of the presence of actuators, which act on the physical world. Security threats can become safety threats as, for instance, the recent cybersecurity attacks on connected vehicles have demonstrated[10].
- Low cost: The wide penetration of IoT and the advanced functionalities it offers in several critical sectors denotes the potential for significant cost savings by exploiting features such as data flows, advanced monitoring, and integration to name a few. Conversely, it is often the case that the low cost that is usually associated with IoT devices and systems will have implications in terms of security. Manufacturers might be inclined to limit security features to ensure a low cost and thus product security might not be able to protect against certain types of IoT attacks.
- Lack of expertise: This is a rather novel domain and therefore there is a lack of people with the suitable skillset and expertise in IoT cybersecurity.
- Security updates: Applying security updates to IoT is extremely challenging, since the particularity of the user interfaces available to users does not allow traditional update mechanisms. Securing of those mechanisms is in itself a daunting task, especially considering Over-The-Air updates.
- Insecure programming: Since the "time to market" pressure for IoT products is higher than in other domains, this imposes constraints on the available efforts to develop security and privacy by design. For this reason, and sometimes also due to budget issues, companies developing IoT products generally place more emphasis on functionality and usability than on security.
- Unclear liabilities: The lack of a clear assignment of liabilities might lead to ambiguities and conflicts in case of a security incident, especially considering the large and complex supply chain involved in IoT. Moreover, the question of how to manage security if one single component were shared by several parties remains unanswered. Enforcing liability is another major issue.

2.3 Challenge of defining horizontal baseline security measures

ENISA together with the vast majority of the experts interviewed agree on the complexity of studying IoT security in a horizontal way, due to the security measures and the impact of the threats being determined by the criticality of the different assets, which differs depending on the use case, the application use and the use scenario.

For each IoT environment it is necessary to carry out a risk assessment to go through the threats that can affect the different assets, define the plausible attack scenarios, and put them in the context of the IoT service defined, working out which hazards are critical or not and which ones can be mitigated. These

reasons highlight the intricacy involved in approaching the IoT in a horizontal way, rather than tackling a specific IoT vertical[59] such as Smart Cars[10], Smart Airports[11], Smart Hospitals[12], Smart Homes[7], Intelligent Public Transport[60], ICS/SCADA[61], etc.

Nonetheless, this report considers the horizontal aspects of IoT as seen across vertical sectors and thus aims to satisfy the paramount need to define baseline security measures for IoT across Critical Information Infrastructures. In this respect, this report complements the aforementioned previous efforts of ENISA in the vertical sectors and thus promotes a holistic approach towards IoT security.

2.4 Architecture

Since IoT solutions are developed with specific technologies and focus on specific applications, they lack standardisation, which results in fragmented and heterogeneous architectures. ENISA studied and reviewed several existing IoT architectures and based on them, put forward an architecture that encompasses key elements of those architectures, promoting a significant degree of interoperability across different assets, platforms environments, etc., with the ambition of laying down a common architectural basis for IoT in a horizontal. The main IoT architectures studied are:

- AIOTI High Level Architecture functional model[62]
- FP7-ICT – IoT-A Architectural reference model[63]
- NIST Network of Things (NoT)[64]
- ITU-T IoT reference model[39]
- ISO/IEC CD 30141 Internet of Things Reference Architecture (IoT RA)[65]
- ISACA Conceptual IoT Architecture[66]
- oneM2M Architecture Model[67]
- IEEE P2413 - Standard for an Architectural Framework[68]

Having analysed the aforementioned architectures, we abstracted and extrapolated the fundamental elements into a consolidated high-level IoT reference model, which encompasses the key elements of these architectures. The objective was to utilise this high-level reference model (Figure 4) in order to define the assets for IoT security and to assist us in consistently applying our methodology in identifying threats and attacks. The following diagram depicts this high-level reference model.

[59] See https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures
[60] See https://www.enisa.europa.eu/publications/good-practices-recommendations
[61] See https://www.enisa.europa.eu/publications/ics-scada-dependencies
[62] See https://aioti-space.org/wp-content/uploads/2017/03/AIOTI-WG3-IoT-High-Level-Architecture-Release_2_1.pdf
[63] See http://www.meet-iot.eu/deliverables-IOTA/D1_5.pdf
[64] See http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-183.pdf
[65] See https://www.w3.org/WoT/IG/wiki/images/9/9a/10N0536_CD_text_of_ISO_IEC_30141.pdf
[66] See https://www.isaca.org/Journal/archives/2017/Volume-3/Pages/default.aspx
[67] See http://www.onem2m.org/images/files/deliverables/Release2/TS-0001-%20Functional_Architecture-V2_10_0.pdf
[68] See https://standards.ieee.org/develop/project/2413.html

Figure 4: IoT High-level reference model

The different elements that compose the IoT high-level reference model are illustrated in Figure 4. It should be noted that we do not aspire to set forth a novel IoT architecture or reference model. Conversely, by analysing existing such efforts we aim at abstracting their fundamental elements in order to coherently and systematically identify the assets to be protected. Moreover, the horizontal nature of security should be underlined in the context of the IoT ecosystem. It applies to all the different elements of the reference model – not only the devices that need to be secured logically and physically, but also the communications, the network elements, the stored information, the cloud platform, etc. With no intention of being exhaustive, there are several security considerations to take into account, such as for example authentication, availability, resilience and authorisation mechanisms, or the use of encryption to protect the confidentiality of data, both at rest and in transit. Figure 4 indicatively lists some of the security mechanisms that can be considered, whereas it should also be noted that privacy has an equally important place and should be also considered across the IoT ecosystem.

2.5 Asset taxonomy

Tackling cyber security starts from asset identification and decomposition. This section provides an overview of the key asset groups and assets to be protected in an IoT ecosystem. Since we are approaching IoT in a horizontal way, the level of protection for a given asset will vary depending on the use case, the application used and the use scenario of said IoT ecosystem.

The different IoT assets have been divided into the key asset groups defined. This asset taxonomy is depicted in Figure 5, and Table 2 details and elaborates on the different assets. It should be noted that the lowest level of the taxonomy is indicative and not exhaustive. For instance, not all sensor types are listed, just some representative ones. This also applies to the networks, the protocols, etc.

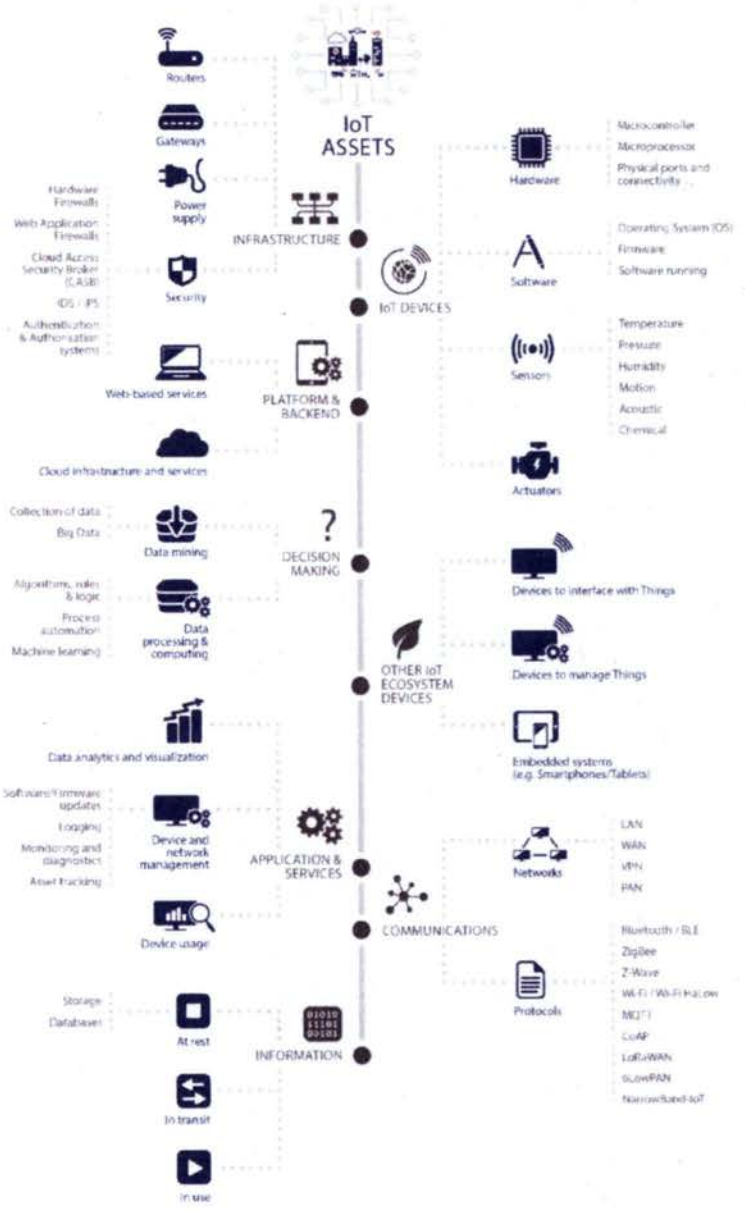


Figure 5: Asset taxonomy

ASSET GROUP	ASSETS	DESCRIPTION
IoT Devices	Hardware	The different physical components (except sensors and actuators) from which the IoT devices can be built. These include microcontrollers, microprocessors, the physical ports of the device, the motherboard, etc.
	Software	Software comprises the IoT device's OS, its firmware and the programs and applications installed/running.
	Sensors	These are the subsystems whose purpose is to detect and/or measure events in its environment and send the information to other electronics in order to be processed. There are sensors for a lot of purposes, such as to measure temperature, motion, etc.
	Actuators	These are IoT device's output units, which execute decisions based on previously processed information.
Other IoT Ecosystem Devices	Devices to interface with Things	These are devices whose purpose is to serve as an interface or as an aggregator between other IoT devices of a given IoT ecosystem. Moreover, devices used by users to interface and interact with IoT devices.
	Devices to manage Things	These are devices specially designed to manage other IoT devices, networks etc.
	Embedded systems	They are based on a processing unit that enables them to process data on their own. They include embedded sensors and/or actuators, network capabilities to connect directly to the cloud, a memory footprint and the ability to run software.
Communications	Networks	They allow the different nodes of an IoT ecosystem to exchange data and information with each other, via a data link. There are different kinds of networks according to their spatial coverage, which include (W)LANs, (W)PANs, PANs and (W)WANs, among others.
	Protocols	They define the set of rules on how communication between two or more IoT devices must be performed through a given channel. There are many communication protocols, which can be either wireless or wireline-based. Examples of IoT communication protocols are ZigBee, MQTT, CoAP, BLE, etc.
Infrastructure	Routers	They are the networking components that forward data packets between the different networks of the IoT ecosystem.
	Gateways	These are the network nodes used for interfacing with another network from the IoT environment that uses different protocols. Gateways may provide protocol translators, fault isolators, etc., to provide system interoperability.
	Power supply	It supplies electric power to an IoT device and to its internal components. The power source can be external and wired or a battery integrated in the device itself.
	Security assets	This group comprises the assets specifically focused on the security of the IoT devices, networks and information. Most prominently, these include firewalls, Web Application Firewalls (WAF), CASBs for protecting the cloud, IDSs, IPSs and authentication/authorisation systems.
Platform & Backend	Web-based services	These are services within the World Wide Web, which provide a web-based interface to web users or to web-connected applications. This means web technologies can be used in IoT for Human-to-Machine (H2M) communications and for M2M communications.
	Cloud infrastructure and services	In IoT, the cloud backend can be used to aggregate and process data from dispersed devices, and it also provides computing capabilities, storage, applications, services, etc.
Decision making	Data mining	This refers to algorithms and services to process collected data and transform it into a defined structure for further use, using big data technologies for discovering patterns in very large data sets.
	Data processing and computing	Services facilitating the processing of gathered data in order to obtain useful information, which can be used to apply rules and logic, to make decisions and to automate processes. Machine learning can be employed to learn from the use of information available over time.

Applications & Services	Data analytics and visualisation	Once the data has been collected and processed, the resulting information can be analysed and visualised in order to identify new patterns, improve operational efficiency, etc.
	Device and network management	The management of the IoT ecosystem devices and networks includes the software updates of the OS, firmware and applications. It also encompasses the tracking and monitoring of the devices and networks, collecting and storing logs that can later be used for diagnostics.
	Device usage	The contextualisation of the IoT ecosystem devices and networks, so as to understand the current status, usage patterns, performance, etc.
Information	At rest	Information stored in a database in the cloud backend or in the devices themselves.
	In transit	Information sent or exchanged through the network between two or more IoT elements.
	In use	Information used by an application, service or IoT element in general.

Table 2: Asset taxonomy

Figure 6 provides a view of the criticality of the main assets described in the asset taxonomy, based on the responses received by the subject matter experts in the interviews. These interviews involved a structured questionnaire where one of the questions the experts were asked was to evaluate the main IoT assets according to their criticality. The experts could classify the assets as not important, of low importance, of medium importance, of high importance and of crucial importance.

It is worth putting again special emphasis on the complexity of defining the criticality of a given asset in a horizontal way rather than considering a specific vertical use case. Abstracting from this fact is very challenging, but that is the goal of this report.

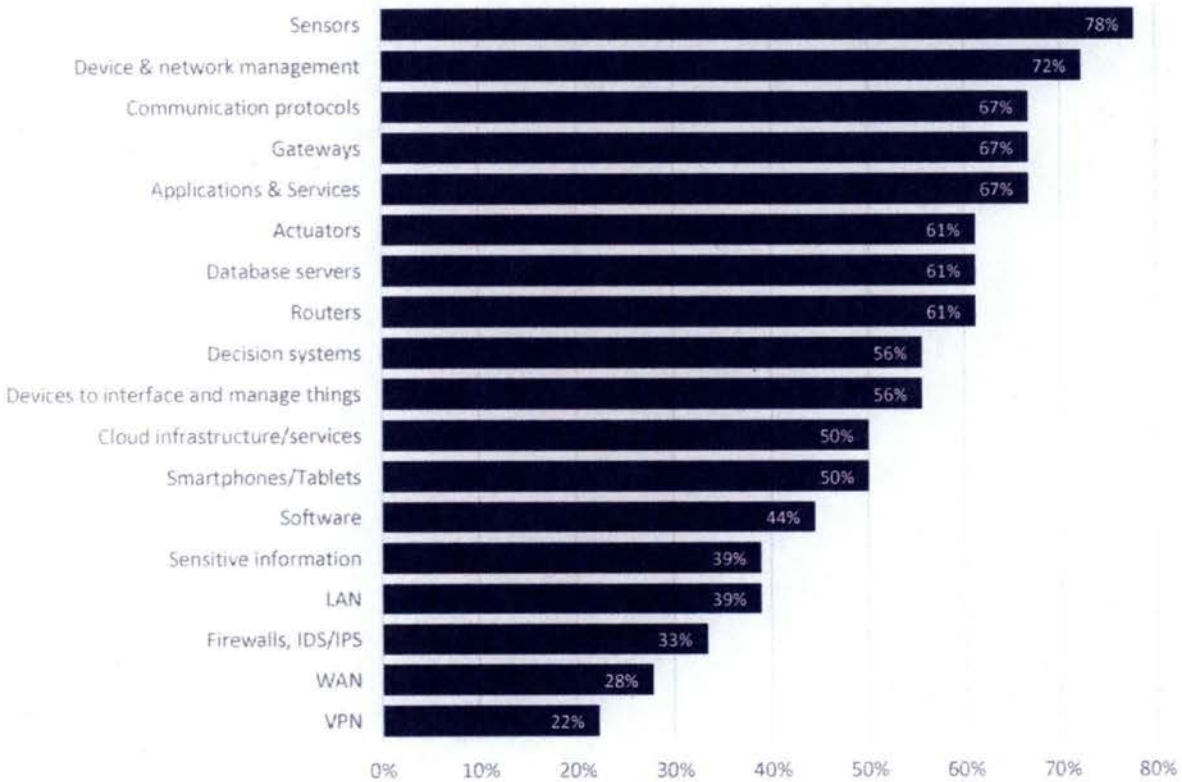


Figure 6: Asset criticality

The main findings here are that the most critical assets are the sensors, then the device and network management controls and thirdly the communication protocols, the gateways and the applications and services, all of them marked as critical by at least two thirds or more of the experts interviewed. Therefore, when addressing security in IoT, those assets should be prioritised. Once again, these results are based on a horizontal approach; hence, they could vary depending on the different deployments and use cases. Anyhow, conducting an asset and risk assessment is key to determine the criticality of the assets and threats that affect a specific IoT environment.

3. Threats and risk analysis

The main objective of this chapter is to determine and list the main security threats, vulnerabilities, risk factors and attack scenarios that affect IoT devices and networks, taking the different levels of importance and criticality the interviewed experts provided for each threat, risk and attack scenario into consideration. Furthermore, the three most critical attack scenarios are developed in detail in order to underline their intricacies and propose specific security measures to counter their impact and adverse effects.

3.1 Security incidents

The number of security threats targeting IoT devices has increased over the last years. Figure 7 illustrates some of the main IoT security incidents that have been discovered and/or have taken place since 2009, so as to highlight how the number attacks on IoT have greatly increased. It should be noted that this list is not exhaustive, it includes only the main examples. Given the ever wider penetration of IoT across the entire spectrum of daily activities and critical infrastructures, the occurrence of cybersecurity incidents is bound to have an increasing rate. A more detailed description of each security incident can be found in Annex D.

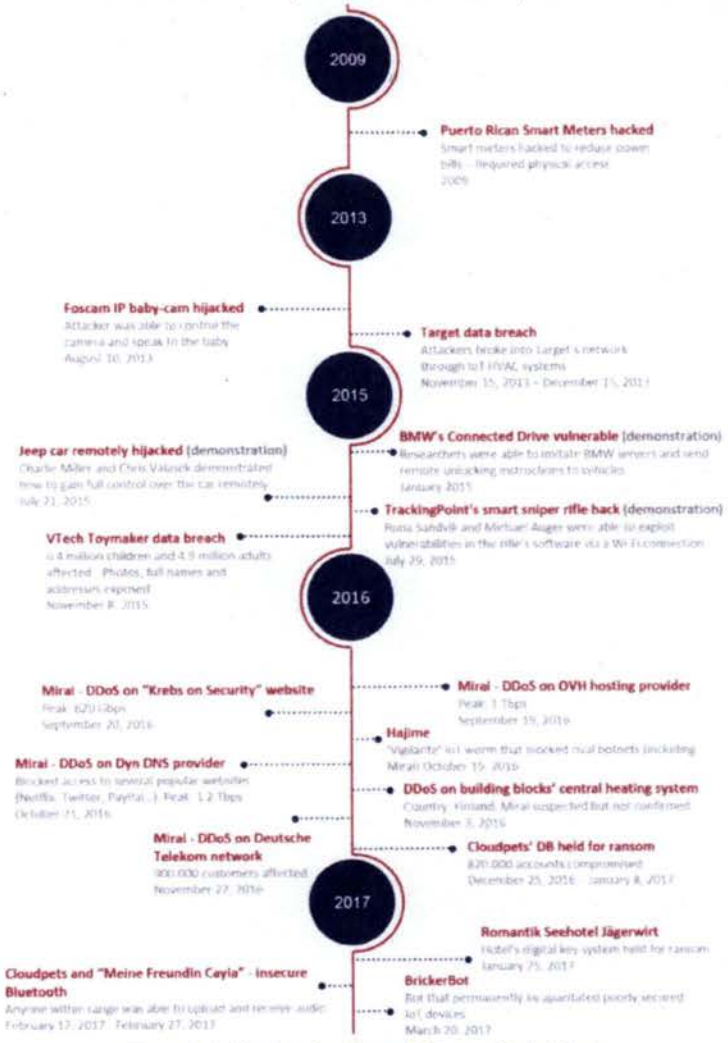


Figure 7: Indicative timeline of IoT security incidents

3.2 Threat taxonomy

As observed in the previous section, the number of attacks directly related to IoT has grown over the last few years reaching the point where it became mainstream news article in 2016 with the Mirai botnet attacks. These attacks, in their great majority, are related to devices that have been violated or to systems that have been compromised, increasing at the same time the number of hazards to be faced in IoT. Being consistent with the ENISA Threat Taxonomy[69], we depict in Figure 8 the threat taxonomy focused on IoT with some examples of attacks listed (non exhaustive listing).

[69] See https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/etl2015/enisa-threat-taxonomy-a-tool-for-structuring-threat-information

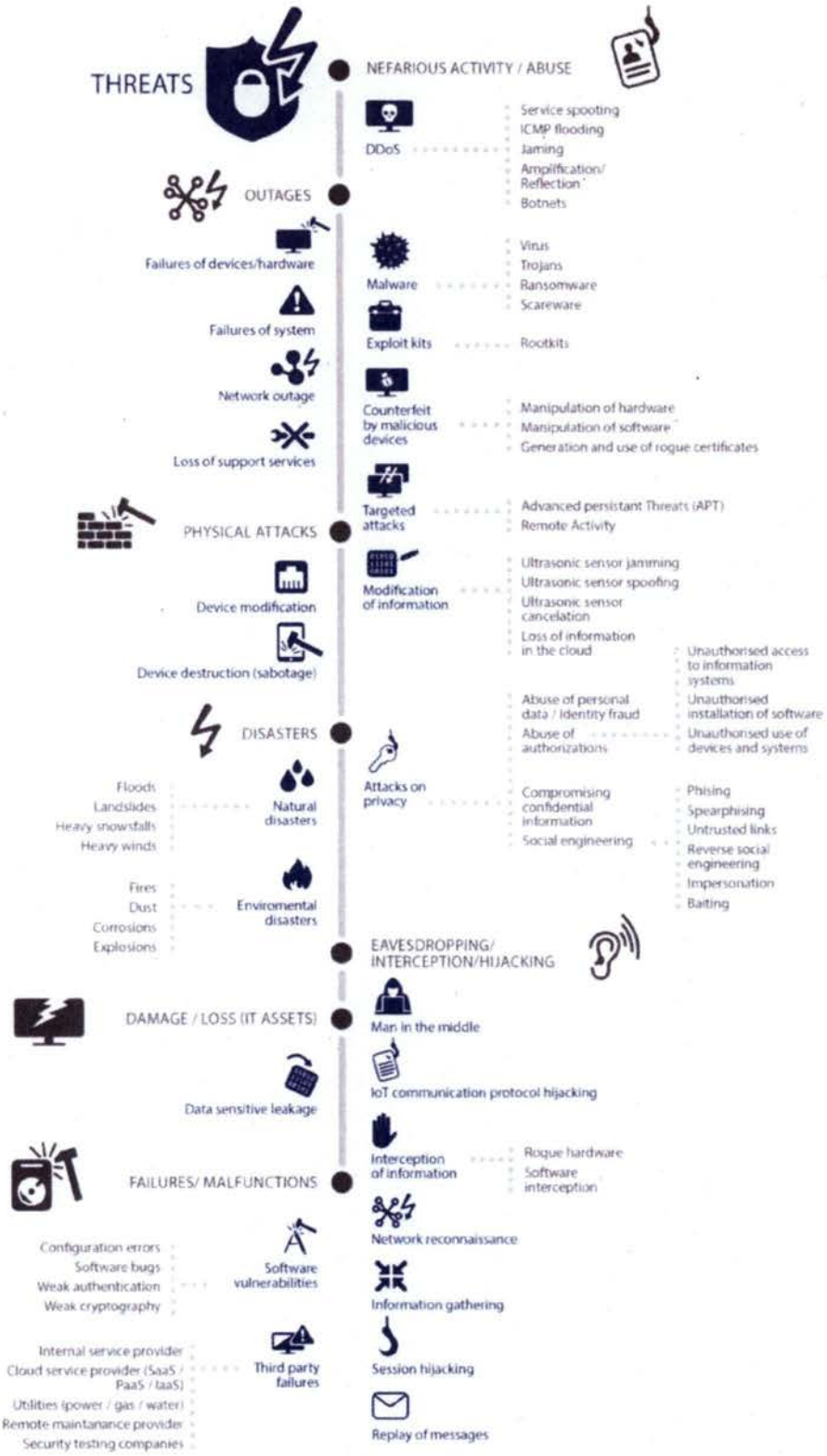


Figure 8: IoT Threat taxonomy

Nevertheless, the different threats have different potential impacts, since they vary according to the use case scenarios. In the interviews, the IoT experts provided insight into the varying impact of the threats. The most relevant ones are shown in Figure 9.

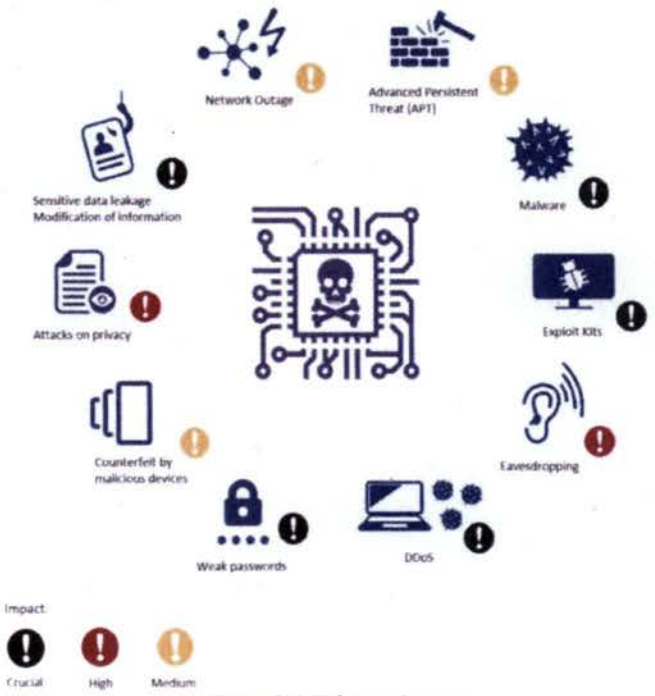


Figure 9: IoT threats impact

The impact of each threat was determined by calculating a weighted average of the responses from the interviewees, which were based on a five-step scale that ranged from no importance to crucial importance. While Figure 9 provides a visual representation of each threat's impact, Figure 10 depicts the exact result of the calculation, where values between 3 and 3.5 out of 5 represent medium-importance threats, values between 3.5 and 4 out of 5 represent high-importance threats, and values over 4 out of 5 represent crucial-importance threats. Values below 3 out of 5 represent low-importance and no-importance threat, but it should be noted that no threat got that rating. Moreover, it can be seen that the average impact is rated as high, since the value of the average impact is 3.7 out of 5.

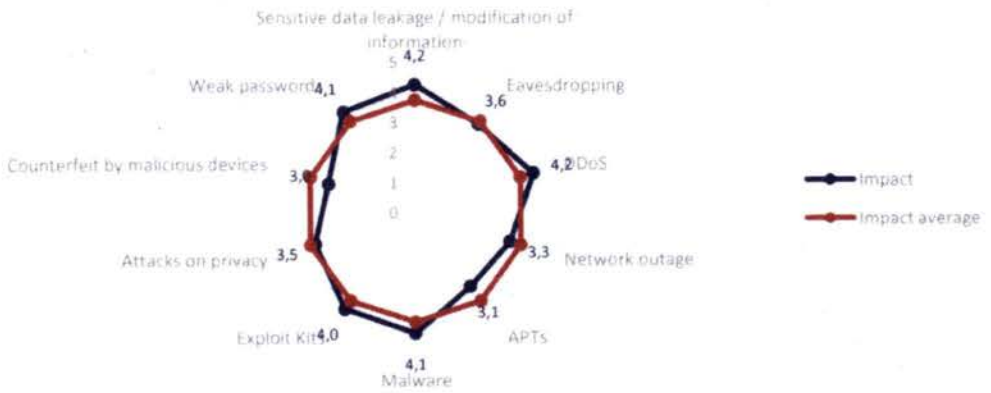


Figure 10: Threat impact weighted average

Table 3 briefly describes every threat identified in the threat taxonomy and the assets affected by them.

CATEGORY	THREAT	DESCRIPTION	ASSETS AFFECTED
Nefarious activity / Abuse	Malware	Software programs designed to carry out unwanted and unauthorised actions on a system without the consent of the user, resulting in damage, corruption or information theft. Its impact can be high.	- IoT devices - Other IoT Ecosystem devices - Platform & Backend
	Exploit Kits	Code designed to take advantage of a vulnerability in order to gain access to a system. This threat is difficult to detect and in IoT environments its impact ranges from high to crucial, depending on the assets affected.	- IoT devices - Other IoT Ecosystem devices - Infrastructure
	Targeted attacks	Attacks designed for a specific target, launched over a long period of time, and carried out in multiple stages. The main objective is to remain hidden and to obtain as much sensitive data/information or control as possible. While the impact of this threat is medium, detecting them is usually very difficult and takes a long time.	- Infrastructure - Platform & Backend - Information
	DDoS	Multiple systems attack a single target in order to saturate it and make it crash. This can be done by making many connections, flooding a communication channel or replaying the same communications over and over.	- IoT devices - Other IoT Ecosystem devices - Platform & Backend - Infrastructure
	Counterfeit by malicious devices	This threat is difficult to discover, since a counterfeit device cannot be easily distinguished from the original. These devices usually have backdoors and can be used to conduct attacks on other ICT systems in the environment.	- IoT devices - Other IoT Ecosystem devices - Infrastructure
	Attacks on privacy	This threat affects both the privacy of the user and the exposure of network elements to unauthorised personnel.	- IoT devices - Other IoT Ecosystem devices - Platform & Backend - Information
	Modification of information	In this case, the objective is not to damage the devices, but to manipulate the information in order to cause chaos, or acquire monetary gains.	- IoT Devices - Other IoT Ecosystem devices - Platform & Backend - Information
Eavesdropping / Interception / Hijacking	Man in the middle	Active eavesdropping attack, in which the attacker relays messages from one victim to another, in order to make them believe that they are talking directly to each other	- Information - Communications - IoT devices
	IoT communication protocol hijacking	Taking control of an existing communication session between two elements of the network. The intruder is able to sniff sensible information, including passwords. The hijacking can use aggressive techniques like forcing disconnection or denial of service.	- Information - Communications - IoT devices - Decision making
	Interception of information	Unauthorised interception (and sometimes modification) of a private communication, such as phone calls, instant messages, e-mail communications	- Information - Communications - IoT devices
	Network reconnaissance	Passively obtain internal information about the network: devices connected, protocol used, open ports, services in use, etc.	- Information - Communications - IoT devices - Infrastructure
	Session hijacking	Stealing the data connection by acting as a legitimate host in order to steal, modify or delete transmitted data.	- Information - Communications - IoT devices
	Information gathering	Passively obtain internal information about the network: devices connected, protocol used, etc.	- Information - Communications - IoT devices
	Replay of messages	This attack uses a valid data transmission maliciously by repeatedly sending it or delaying it, in order to manipulate or crash the targeted device.	- Information - IoT devices - Decision making

Outages	Network Outage	Interruption or failure in the network supply, either intentional or accidental. Depending on the network segment affected, and on the time required to recover, the importance of this threat ranges from high to critical.	- Infrastructure - Communications
	Failures of devices	Threat of failure or malfunction of hardware devices	- IoT devices
	Failure of system	Threat of failure of software services or applications	- IoT devices - Platform & Backend - Other IoT Ecosystem devices
	Loss of support services	Unavailability of support services required for proper operation of the information system.	- All assets
Damage / Loss (IT Assets)	Data / Sensitive information leakage	Sensitive data is revealed, intentionally or not, to unauthorised parties. The importance of this threat can vary greatly, depending on the kind of data leaked.	- IoT devices - Other IoT Ecosystem devices - Platform & Backend - Information
Failures / Malfunctions	Software vulnerabilities	The most common IoT devices are often vulnerable due to weak/default passwords, software bugs, and configuration errors, posing a risk to the network. This threat is usually connected to others, like exploit kits, and it is considered crucial.	- IoT devices - Other IoT Ecosystem devices - Platform & Backend - Infrastructure - Applications & Services
	Third parties failures	Errors on an active element of the network caused by the misconfiguration of another element that has direct relation with it.	- IoT devices - Other IoT Ecosystem devices - Platform & Backend - Infrastructure - Applications & Services
Disaster	Natural Disaster	These include events such as, floods, heavy winds, heavy snows, landslides, among others natural disaster, which could physically damage the devices.	- IoT devices - Other IoT Ecosystem devices - Platform & Backend - Infrastructure
	Environmental Disaster	Disasters in the deployment environments of IoT equipment and causing their inoperability.	- Other IoT Ecosystem devices - Platform & Backend - Infrastructure
Physical attacks	Device modification	Tampering a device by for example taking advantage of bad configuration of ports, exploiting those left open.	- Communications - IoT devices
	Device destruction (sabotage)	Incidents such devices theft, bomb attacks, vandalism or sabotage could damage devices	- IoT devices - Other IoT Ecosystem devices - Platform & Backend - Infrastructure

Table 3: Threat taxonomy

3.3 Examples of IoT cyber security attack scenarios

The threats and risks previously listed in chapter 3.2 could be used by attackers to cause cascade effects and further damages at different levels in the infrastructures. The different attack scenarios and the level of importance of each attack have been gathered from the desktop research as well as the information provided by the experts who have contributed to the report.

It is worth noting that the attacks may take place throughout the whole process, and the impact that attacks may have on each specific part of the process has also been analysed. The importance level provided for each sample attack scenario ranges from low and medium through high and crucial, representing the negative impact level these attacks could have in a real-life incident, according to the input of the experts interviewed. This information is synthesised in Table 4.

ATTACK SCENARIOS	IMPORTANCE LEVEL
1. Against the network link between controller(s) and actuators	High – Crucial
2. Against sensors, modifying the values read by them or their threshold values and settings	High – Crucial
3. Against actuators, modifying or sabotaging their normal settings	High – Crucial
4. Against the administration systems of IoT	High – Crucial
5. Exploiting protocol vulnerabilities	High
6. Against devices, injecting commands into the system console	High – Crucial
7. Stepping stones attacks	Medium – High
8. DDoS using an IoT botnet	Crucial
9. Power source manipulation and exploitation of vulnerabilities in data readings	Medium – High
10. Ransomware	Medium – Crucial[70]

Table 4: IoT attack scenarios

For these scenarios, additional relevant feedback in the context of this report was received. Each section includes a brief description, the potential impact, and threats:

1. Against the network link between controller(s) and actuators

Eavesdropping is a threat that allows an attacker to extract sensitive and operational information that can be used for multiple malicious activities, including later attacks against IoT systems. In Advanced Persistent Threat (APT) attacks, eavesdropping and information gathering comprise one of the first stages carried out in order to identify weak spots and potential entry/attack points.

- Impact: the main effect is the leakage of data. Depending on the environment, the severity can be lower or greater, but it may also be signalling a larger attack in progress.
- Threats related: eavesdropping and leakage of sensitive data.

2. Against sensors, modifying the values read by them or their threshold values and settings

The attacker manipulates the configuration of the sensors, changing the threshold values established on the sensors, to allow out-of-range read values to be accepted when they should not, posing a severe threat to the systems and installations. As larger installations usually have multiple and redundant sensors, the attacker would have to compromise multiple sensors for the attack to be efficient; if only one were compromised, the readings could be compensated with the input from the rest of the sensors.

- Impact: allowing sensors to report and accept incorrect values puts the IoT environment at risk; a malfunctioning sensor may allow a power spike to go through, physically damaging the systems.

[70] Depending on the target, the impact of the attack could range from medium through crucial. For instance, the impact of the ransomware attack against the digital key system of a hotel, example found in Figure 7 and in Annex D., was not critical. Nevertheless, a ransomware the size of WannaCry (https://www.enisa.europa.eu/publications/info-notes/wannacry-ransomware-outburst) aimed against IoT infrastructures could have an extreme impact and affect systems at an international scale.

- Threats related: attacks on privacy and leakages of sensitive data/modification of information.

3. Against actuators, modifying or sabotaging their normal settings

Manipulation of the actuators' configuration/parameters making them use wrong configurations, thresholds or data, and therefore affecting their normal behaviour by sabotaging their normal operation settings.

- Impact: it varies depending on the actuators affected. It can affect production processes.
- Threats related: network outage and counterfeit by malicious devices.

4. Against the administration systems of IoT

An attacker tries to gain full control over the administration system of an IoT system or device, potentially compromising the whole environment. It can be quite successful if weak or default passwords are used. This type of attack comprises different stages/phases and it is usually launched in a covert manner. It should be noted that this type of attack should be taken into account for the entire lifecycle of the device.

- Impact: the compromise, manipulation or interruption of certain IoT systems could affect many people, cause environmental issues and even extend to other systems, affecting their communications or even disabling them.
- Threats related: weak passwords, exploit kits, attacks on privacy, malware and DDoS.

5. Exploit Protocol vulnerabilities

This type of exploitation is usually the gateway to launch other types of attacks; it is a means to an end. Exploits are used to gain privileged unauthorised access to a system, which can lead to the installation of other malicious content or backdoors. It is used as part of an attack, regardless of whether the target is a single system/device or a whole network. It is difficult to detect these exploits, and it is much easier to detect the actions carried out after the exploit has been successful.

- Impact: if successful, the exploit creates an entry point to a system, in some cases with elevated privileges; if not, the system is likely to crash or become unstable. This attack is always used as part of a larger attack, which could be a simple data theft or a complex APT.
- Threats related: exploit kits, malware and APTs.

6. Against devices by injecting commands into the system console

This type of attack takes place when an attacker injects and executes commands with privileges in a compromised system through its console.

- Impact: if the attacker is able to inject commands into a device, he or she could manage to breach another machine in the environment. This would produce a cascade effect on the system, and the attacker would be able to use all these devices for malicious purposes.
- Threats related: Exploit kits, DDoS and network outage.

7. Stepping stone attacks

This type of attack is a common way to launch anonymous attacks. They are often used by network intruders to hide their identities, since they launch attacks not from their own computer but from intermediary hosts that they previously compromised.

- Impact: if an attacker launches a stepping stone attack, he or she could compromise a collection of hosts, using them as stepping stones to relay attack commands.
- Threats related: APTs, DDoS, counterfeit by malicious devices.

8. DDoS using an IoT botnet

This type of attack does not target IoT devices themselves, but instead it uses them to attack other devices, not necessarily IoT ones. Firstly, a malware automatically finds vulnerable Internet of Things devices, infecting and conscripting them into a botnet, which then can be used to mount DDoS attacks, flooding the target's servers with malicious traffic.

- Impact: the target device or service will be flooded with malicious traffic, taking it down.
- Threats related: exploit kits, DDoS and counterfeit by malicious devices.

9. Power source manipulation and exploitation of vulnerabilities in data readings

These attacks focus on manipulating power sources and exploiting vulnerabilities to modify the power data read. An attacker can tamper with the device's battery or power input cabling either physically, by manipulating the power source itself, or with malware, by manipulating the way a device reads the information coming from the power source in order to, for example, make the device believe the battery level is higher or lower than the actual level. Some types of smart devices may be dependent on batteries for their normal operation. This feature may seem like an advantage over the less usual cables but, far from this, it requires taking into account certain aspects of security.

- Impact: physical tampering a battery can damage it, potentially causing the device not being able to operate at all. The manipulation of the way a device reads the charge level coming from the battery can lead to the device believing the battery level is higher than the real one, causing the device to run out of battery and shut down, or lower than the real one, causing the device to enter a power-saving mode of operation, affecting the performance of the device.
- Threats related: malware, physical attacks.

10. Ransomware

These attacks are carried out by a malware that perpetually blocks access to the victim's data unless a ransom is paid. Since these attacks are malware-based, they can be evaded by updating/patching vulnerable devices. This can be also done outside the IoT ecosystem, such as with the WannaCry attack that took place on May 2017[70], where the patch for the vulnerability that WannaCry exploited was released months before the attack. The problem regarding IoT is the difficulty to update/patch the different devices - some of them do not even have the ability to be updated or patched.

- Impact: there are many possible targets for ransomware within IoT – an attacker could take control of a smart thermostat in the middle of winter and demand payment before the heat can be turned on, he could hold power grids or hospitals systems for ransom, etc., putting people safety at risk.
- Threats related: exploit kits, DDoS, malware, weak passwords.

3.4 Critical attack scenarios

During the interviews with experts and relevant stakeholders, the aforementioned attack scenarios regarding IoT environments were described and detailed. The experts were asked to rank the 10 example attack scenarios in terms of criticality and the following three were also the most worrisome ones for interviewees. Figure 11 depicts the average criticality of a given attack scenario based on the input gathered from the expert interviews. Again, the challenge lies in defining the criticality level of an attack on an IoT environment when doing so in a horizontal manner.

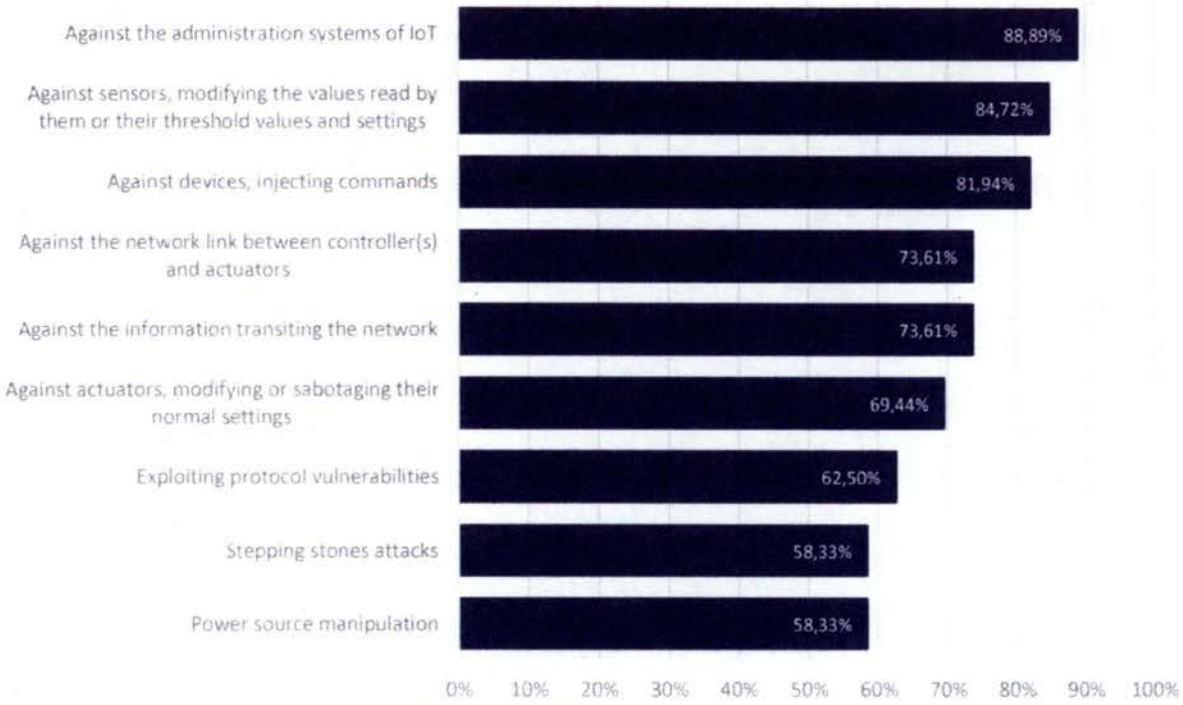


Figure 11: Attack scenario criticality

The three attack scenarios that stand out are:

- Attack Scenario 1: IoT administration system compromise
- Attack Scenario 2: Value manipulation in IoT devices
- Attack Scenario 3: Botnet / Commands Injection

The following sections detail each of these scenarios, including their impact, the stakeholders involved, the cascade effect risk, the gaps, the countermeasures that can be applied to protect against them, and more technical details. The detailed description of each one of those countermeasures can be found in Annex A: and in Annex B:.

3.4.1 Attack scenario 1: IoT administration system compromise

This attack covers an infection designed to take control over one or multiple IoT devices within an IoT environment, in order to manipulate or crash them and to be able to modify values, change their functioning/behaviour or deny access to them. This attack scenario is based on an Enterprise gateway attack[71,72].

As depicted in Figure 12, the first step is to gather information in the network about the different IoT devices used in the enterprise. Once an IoT device is identified and selected, the attacker gathers specific information about its vulnerabilities. The next step is to exploit the different vulnerabilities found in that device, and to compromise the network. After that, the attacker ensures the persistence of the access to the system by configuring a backdoor. At this point, the attacker only needs to update the system (e.g. with a modified firmware) for the device to be permanently compromised. This way, the attacker gains full control over the

[71] See http://www.csoonline.com/article/3148806/internet-of-things/the-iot-gateway-for-enterprise-hackers.html
[72] See https://securelist.lat/iot-el-da-que-ataqu-mi-propia-casa/72452/

device – he/she gains the ability to see all the data and information the device has gathered and has remote access to use whenever he/she wants, etc.

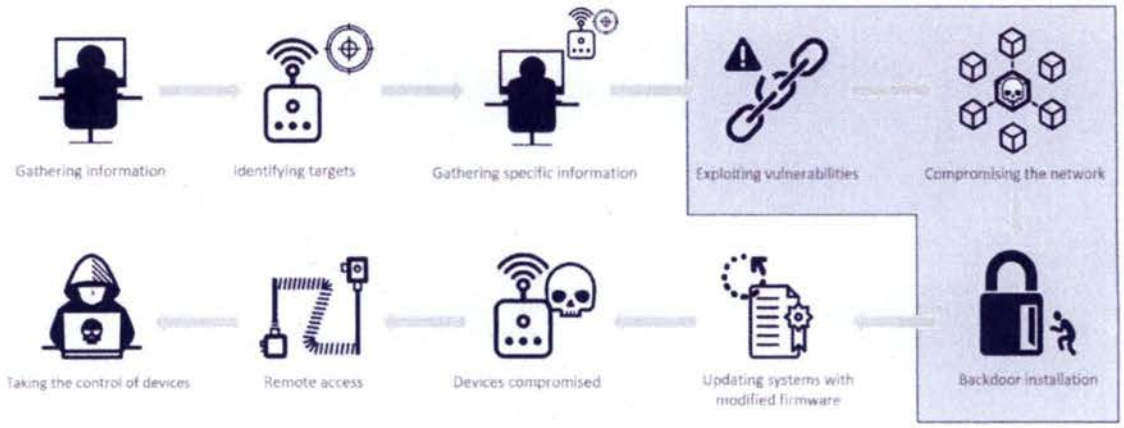


Figure 12: Attack 1 – IoT administration system compromised

IOT SYSTEM COMPROMISE

IMPACT	
Crucial: the compromise of an IoT administration system grants the attacker access to all the assets (devices, networks, etc.) which fall under the control of that administration system. When compromised, the attacker is capable of performing administrative tasks within those assets, such as extracting confidential information from them, making them malfunction and directly affecting the behaviour of the IoT environment, etc. Since a compromised administration system leads to several assets being compromised over a long period of time and without being detected, the impact of this attack can be critical.	
EASE OF DETECTION	CASCADE EFFECT RISK
Medium: the changes to an IoT administration system can be detected through a correct monitoring and a proper logging system.	**High:** the risk entailed is that, once an IoT device belonging to a specific IoT network is compromised, it becomes very easy to compromise the rest.
ASSETS AFFECTED	STAKEHOLDERS INVOLVED
Devices to interface with things Devices to manage things Smartphones / Tablets Gateways Software Sensitive information	IoT experts, software developers and manufacturers Information security experts IT/Security solutions architects Chief Information Security Officers (CISOs)
ATTACK STEPS (SAMPLE BASED ON A REAL-CASE ATTACK SCENARIO)	
1. Gathering of information about the infrastructure 2. Identification of system components 3. The attacker gathers further information to identify the vulnerable system 4. The vulnerable system is identified 5. Exploitation of vulnerabilities to compromise first the system and then through the system the network 6. A backdoor is installed in order to maintain access to that system 7. The attacker ensures the IoT systems are updated with modified firmware either by downloading and updating the firmware instantly, or by modifying the repository of update files. This is done to grant the attacker exclusive access and restrict other remote accesses 8. Finally the attacker takes control over the IoT environment	

RECOVERY TIME / EFFORT	GAPS AND CHALLENGES
Medium: it depends on the perimeter of the assets compromised and on the number of assets infected. It ranges from a few hours to up to several days if critical systems are compromised.	Insecure design or development Lack of proper product lifecycle management

COUNTERMEASURES

- ✓ **GP-TM-04**: Sign code cryptographically to ensure it has not been tampered after being signed as safe for the device, and implement run-time protection and secure execution monitoring to be sure malicious attacks do not overwrite code after it is loaded
- ✓ **GP-TM-05**: Control the installation of software on operational systems, to prevent unauthenticated software and files being loaded onto it
- ✓ **GP-TM-06**: Enable a system to return to a state that is known to be secure, after a security breach occurs or if an upgrade is not successful
- ✓ **Hardening assets**:
  - ✓ **GP-PS-11**: Identify significant risks using a defence-in-depth approach
  - ✓ **GP-TM-22**: Ensure default passwords and even default usernames are changed during the initial setup, and that weak, null or blank passwords are not allowed
  - ✓ **GP-TM-27**: Limit the permissions of actions allowed for a given system by Implementing fine-grained authorisation mechanisms and using the Principle of least privilege (POLP): applications must operate at the lowest privilege level possible
  - ✓ **GP-TM-23**: Authentication mechanisms must use strong passwords or personal identification numbers (PINs), and should consider using two-factor authentication (2FA) or multi-factor authentication (MFA) like Smartphones, Biometrics, etc., and certificates
  - ✓ **GP-TM-38**: Guarantee the different security aspects -confidentiality (privacy), integrity, availability and authenticity- of the information in transit on the networks or stored in the IoT application or in the Cloud
  - ✓ **GP-TM-55**: Implement a logging system that records events relating to user authentication, management of accounts and access rights, modifications to security rules, and the functioning of the system
  - ✓ **GP-TM-56**: Implement regular monitoring to verify the device behaviour, to detect malware and to discover integrity errors

Table 5: Attack 1 – IoT administration system compromise

3.4.2 Attack scenario 2: Value manipulation in IoT devices

The manipulation of calibration parameters established for the sensors allows undesired values to be accepted when they should not, which poses a severe threat to critical systems. This attack targets the sensor processing and knowledge model levels of the control system of an industrial robot in an Industry 4.0 environment[73].

Figure 13 describes this attack, which starts with the calibration of a robot sensing equipment after a configuration change or when connected to a controller. The calibration data initially stored in the sensing equipment is transmitted to the controller during the system boot. Since the robot uses its local copy of that data, an attacker can manipulate the calibration parameters, causing the robot to move erratically or unexpectedly (in decision making, wrong input values lead to wrong decisions).

[73] See https://documents.trendmicro.com/assets/wp/wp-industrial-robot-security.pdf

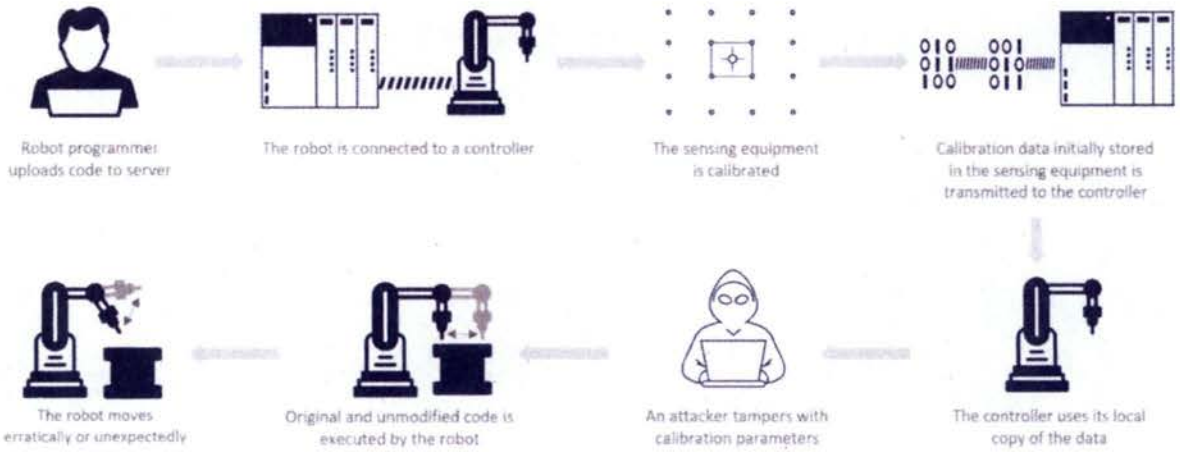


Figure 13: Attack 2 – Value manipulation in IoT devices

IOT SYSTEM COMPROMISE

IMPACT	
High – Crucial: By allowing the sensors to report and accept incorrect values, the IoT environment is put at risk – a malfunctioning industrial robot can cause severe physical damage to whatever it is working with, and in the worst case scenario, to the people working with it.	
EASE OF DETECTION	CASCADE EFFECT RISK
Easy – Medium: its detection is between easy and medium since an operator can see whether the outcome and the robot's behaviour are correct or not.	Medium: The cascade effect risk is medium, but it can vary depending on the number of sensors compromised in the robot, and on the number of robots involved.
ASSETS AFFECTED	STAKEHOLDERS INVOLVED
Sensors Actuators Decision making Software Sensitive information	IoT experts, software developers and manufacturers IT/Security solutions architects

ATTACK STEPS (SAMPLE BASED ON A REAL-CASE ATTACK SCENARIO)

1. The robot programmer uploads code to aserver
2. The robot is connected to a controller or its configuration has changed
3. The sensing equipment is calibrated
4. The calibration data initially stored in the sensing equipment is transmitted to the controller during the system boot
5. The controller uses its local copy of the data
6. An attacker remotely or locally tampers with calibration parameters
7. Original and unmodified code is executed by the robot
8. The robot moves erratically or unexpectedly because the true error is different from the error that the controller knows

RECOVERY TIME / EFFORT	GAPS AND CHALLENGES
Medium – High: depending on the number of sensors, and the robots involved, the recovery time can range from a few days to weeks.	Insecure design or development Lack of awareness and knowledge

COUNTERMEASURES

✓ GP-PS-10: Establish and maintain asset management procedures and configuration controls for key network and information systems ✓ GP-PS-11: Identify significant risks using a defence-in-depth approach ✓ GP-TM-15: Design with system and operational disruption in mind, preventing the system from causing unacceptable risk of injury or physical damage ✓ GP-TM-31: Measures for tamper protection and detection. Detection and reaction to hardware tampering should not rely on network connectivity ✓ GP-TM-54: Data input validation (ensuring that data is safe prior to use) and output filtering ✓ GP-TM-56: Implement regular monitoring to verify the device behaviour, to detect malware and to discover integrity errors ✓ GP-OP-09: Ensure the personnel practices promote privacy and security – train employees in good privacy and security practices

Table 6: Attack 2 – Value manipulation in IoT devices

3.4.3 Attack scenario 3: Botnet / Commands injection

This attack entails the exploitation of some vulnerability inside a device to inject commands and obtain administrator privileges, with the purpose of creating a botnet made up of those vulnerable IoT devices. A botnet is a network of automatic devices that interact to accomplish some distributed task. Due to the characteristic interconnection of IoT devices and their poor configuration, carrying out such an attack is simple. This attack scenario is based on the Mirai botnet[74], which has conducted several of the most forceful DDoS attacks in recent history, and has proven capable of attacking varied kinds of targets, from KrebsOnSecurity website to a whole country's telecommunication infrastructure[75]. Therefore, with potential targets such as a hazardous energy infrastructure, the impact of a Mirai's attack can reach extremely critical levels.

The steps to follow in order to carry out this type of attack are illustrated in Figure 14. The first one is scanning open ports in IoT devices that are accessible over the Internet, which are usually poorly protected by default usernames and passwords that, users never change. Once the attacker gains access to the device, he or she will inject commands into the device's console in order to obtain administrator privileges. If the attacker succeeds in obtaining these permissions, he or she will then make the device connect to a Command and Control (C&C) under his or her control, to download and execute a malicious script. The script will then be executed, deleting itself afterward and running in-memory. Then, it will begin to spread, attacking the same way other vulnerable devices, in order to gather an IoT device army, conscripting them into a botnet, which the attacker will be able to control from a C&C centre, in order to launch distributed attacks conducted by the botnet.

[74] See https://www.enisa.europa.eu/publications/info-notes/major-ddos-attacks-involving-iot-devices
[75] See http://www.energycollection.us/Companies/ICIT/Rise-Machines.pdf

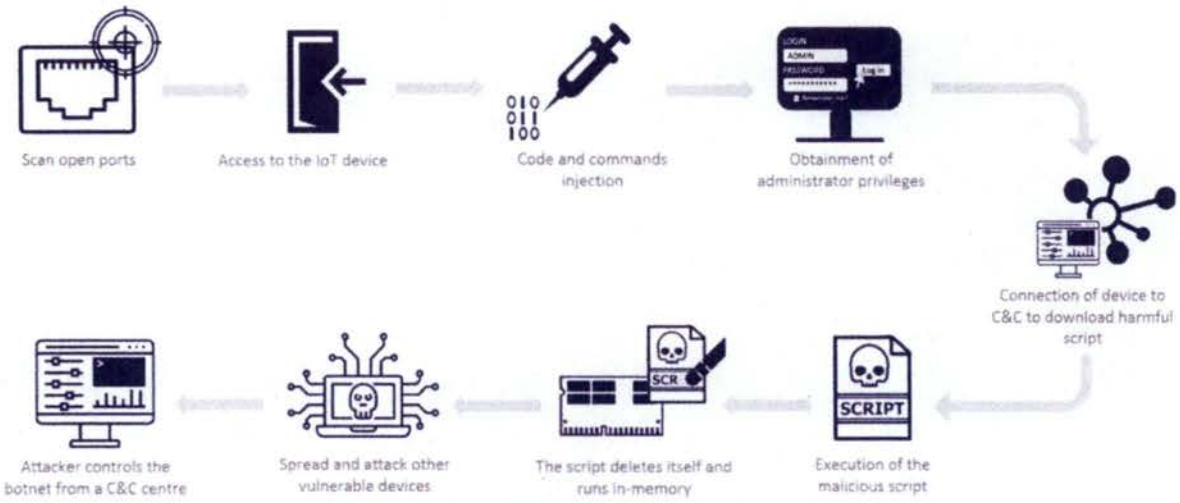


Figure 14: Attack 3 – Botnet / Commands injection

IOT SYSTEM COMPROMISE

IMPACT	
High – Crucial: The impact of the attacks carried out by a botnet ranges from high to critical, depending on the volume of the distributed attack, which is directly related to the number of compromised assets that are part of the botnet, and the criticality of the target.	
EASE OF DETECTION	**CASCADE EFFECT RISK**
Hard: due to the ignorance about the characteristics and configuration of these devices, these attacks tend to be hard to detect and identify the source, which allows them to pass undetected for long periods of time, and they are also complex to investigate and recover from.	**Critical:** this type of attack has a tremendous cascade effect. Once a device is infected, the goal is to identify other vulnerable devices to extend the network.
ASSETS AFFECTED	**STAKEHOLDERS INVOLVED**
Devices to interface with things Devices to manage things Device and network management Communications Software	IoT experts, software developers and manufacturers Information security experts IT/Security solutions architects Chief Information Security Officers (CISOs)

ATTACK STEPS (SAMPLE BASED ON A REAL-CASE ATTACK SCENARIO)

1. The attacker scans open ports in devices belonging to an IoT network
2. If there are any open ports, the attacker tries to gain access to the device using weaknesses such as weak or default passwords, or through exploiting the test/debug modes
3. Once inside, the attacker injects commands in order to obtain administrator privileges
4. With these permissions, the attacker tries to connect the device to the Command and Control of the botnet
5. The attacker downloads and executes a malicious script
6. The script deletes itself and runs in-memory
7. Then, it will begin to spread, attacking other vulnerable devices in the same way, in order to gather an IoT device army, conscripting them into a botnet.
8. The attacker can now control the botnet from a Command and Control (C&C) centre, from where he or she will launch distributed attacks conducted by the botnet.

RECOVERY TIME / EFFORT	GAPS AND CHALLENGES

High: the main issue is the amount of time it takes to detect that the system that has been manipulated, which can take several days/weeks, or even months in extreme cases	Insecure design or development Lack of proper product lifecycle management

COUNTERMEASURES
✓ **GP-TM-04**: Sign code cryptographically to ensure it has not been tampered after being signed as safe for the device, and implement run-time protection and secure execution monitoring to be sure malicious attacks do not overwrite code after it is loaded
✓ **GP-TM-05**: Control the installation of software on operational systems, to prevent unauthenticated software and files being loaded onto it
✓ **GP-TM-06**: Restore Secure State - Enable a system to return to a state that is known to be secure, after a security breach occurs or if an upgrade is not successful
✓ **GP-TM-08**: Enable security by default. Any applicable security features should be enabled by default, and any unused or insecure functionalities should be disabled by default
✓ **GP-TM-09**: Establish hard to crack device individual default passwords
✓ **GP-TM-22**: Ensure default passwords and even default usernames are changed during the initial setup, and that weak, null or blank passwords are not allowed
✓ **GP-TM-50**: Ensure only necessary ports are exposed and available
✓ **GP-TM-56**: Implement regular monitoring to verify the device behaviour, to detect malware and to discover integrity errors

Table 7: Attack 3 – Botnet / Commands injection

4. Security measures and good practices

This chapter provides a detailed list of security measures and good practices, which aim to mitigate the threats, vulnerabilities and risks identified in the study that affect IoT devices and environments. These security measures and good practices have been defined with the aim to apply to the different IoT environments and deployments in a horizontal manner, instead of providing IoT vertical-specific security. Therefore, the security measures defined cover a wide range of security considerations, such as security by design, data protection, risk analysis, etc.

The set of security measures / good practices of this report has been determined based on a very extensive and thorough desktop research, which took into account different security guidelines, standards, etc. The list of these resources can be found in Annex C:.

The different security measures and good practices identified fall into several security domains defined for the report. This domain division's purpose is to cover every IoT environment horizontally, so as to classify and define which security measures apply to which different IoT ecosystem areas. The proposed security domains are organised as follows:

- Information System Security Governance & Risk Management: Includes security measures regarding information system security risk analysis, policy, accreditation, indicators and audit, and human resource security.
- Ecosystem Management: Includes security measures regarding ecosystem mapping and ecosystem relations.
- IT Security Architecture: Includes security measures regarding systems configuration, asset management, system segregation, traffic filtering and cryptography.
- IT Security Administration: Includes security measures regarding administration accounts and administration information systems.
- Identity and access management: Includes security measures regarding authentication, identification and access rights.
- IT security maintenance: Includes security measures regarding IT security maintenance procedures and remote access.
- Physical and environmental security
- Detection: Includes security measures regarding detection, logging, and log correlation and analysis.
- Computer security incident management: Includes security measures regarding information system security incident analysis and response, and incident report.
- Continuity of Operations: Includes security measures regarding business continuity management and disaster recovery management.
- Crisis Management: Includes security measures regarding crisis management organization and process.

These security domains have been considered when developing the different security measures/good practices for IoT, which can be found below in points 4.1 through 4.3. The detailed description of each security measure/good practice and its security domain, along with the documents and references that have

been analysed in order to extract it, can be found in Annex A: together with all the relevant examples. Additionally, in Annex B:, each security measure can be found mapped to the threats related to it.

As mentioned earlier, these security domains classify the security measures based on which area of an IoT ecosystem they apply to. Apart from their area of application, each security measure can be arranged according to its nature – they can be policies that must be taken into account when developing the devices, organisational measures focused on the business and employees that need to be adopted by the organisation itself, and finally, technical measures aimed at reducing the potential risks that the IoT devices and other elements of the IoT ecosystem may be subject to. Accordingly, the identified IoT baseline security measures (denoted henceforth as GP-Good Practices) are presented here and arranged according to three main categories:

- Policies (PS)
- Organisational, People and Process measures (OP)
- Technical Measures (TM)

4.1 Policies

The first set of security measures refers to policies that generally target information security and aim at making it more concrete and robust. These should be adequate for the organisation's activity and must contain well documented information. In this context, the following security good practices have been defined.

It is worth mentioning that when referring to security and privacy by design, the security measures should reflect the particularities and the context in which the IoT device or system will be deployed (for example, security by design will refer to different specifications when an IoT device at a home environment is considered, compared to the case of an IoT device in a critical infrastructure). As discussed, when it comes to IoT the cyber risk is context-dependent (i.e. based on the application scenario) and in this respect the security measures should be applied with this consideration in mind.

4.1.1 Security by design

- GP-PS-01: Consider the security of the whole IoT system from a consistent and holistic approach during its whole lifecycle across all levels of device/application design and development, integrating security throughout the development, manufacture, and deployment.
- GP-PS-02: Ensure the ability to integrate different security policies and techniques.
- GP-PS-03: Security must consider the risk posed to human safety.
- GP-PS-04: Designing for power conservation should not compromise security.
- GP-PS-05: Design architecture by compartments to encapsulate elements in case of attacks.
- GP-PS-06: For IoT hardware manufacturers and IoT software developers it is necessary to implement test plans to verify whether the product performs as it is expected. Penetration tests help to identify malformed input handling, authentication bypass attempts and overall security posture.
- GP-PS-07: For IoT software developers it is important to conduct code review during implementation as it helps to reduce bugs in a final version of a product.

4.1.2 Privacy by design

- GP-PS-08: Make privacy an integral part of the system.
- GP-PS-09: Perform privacy impact assessments before any new applications are launched.

4.1.3 Asset Management

- GP-PS-10: Establish and maintain asset management procedures and configuration controls for key network and information systems.

4.1.4 Risk and Threat Identification and Assessment

- GP-PS-11: Identify significant risks using a defence-in-depth approach.
- GP-PS-12: Identify the intended use and environment of a given IoT device.

4.2 Organisational, People and Process measures

All businesses must have organisational criteria for information security. Their personnel practices need to promote good security, ensure the management of processes and safely operate the information in the organisation practices. Organisations should ensure that contractors and suppliers are responsible and accountable for the functions considered. In the event of an incident in the safety of the organisation, the organisation must be prepared (responsibilities, evaluation and response).

4.2.1 End-of-life support

- GP-OP-01: Develop an end-of-life strategy for IoT products.
- GP-OP-02: Disclose the duration and end-of-life security and patch support (beyond product warranty).
- GP-OP-03: Monitor the performance and patch known vulnerabilities up until the "end-of-support|" period of a product's lifecycle.

4.2.2 Proven solutions

- GP-OP-04: Use proven solutions, i.e. well known communications protocols and cryptographic algorithms, recognized by the scientific community, etc. Certain proprietary solutions, such as custom cryptographic algorithms, should be avoided.

4.2.3 Management of security vulnerabilities and/or incidents

- GP-OP-05: Establish procedures for analysing and handling security incidents.
- GP-OP-06: Coordinated disclosure of vulnerabilities.
- GP-OP-07: Participate in information-sharing platforms to report vulnerabilities and receive timely and critical information about current cyber threats and vulnerabilities from public and private partners.
- GP-OP-08: Create a publicly disclosed mechanism for vulnerability reports, e.g. Bug Bounty programs.

4.2.4 Human Resources Security Training and Awareness

- GP-OP-09: Ensure the personnel practices promote privacy and security – train employees in good privacy and security practices.
- GP-OP-10: Document and monitor the privacy and security training activities.
- GP-OP-11: Ensure that cybersecurity roles and responsibilities for all workforce are established and introduce personnel assignments in accordance with the specifics of the projects and security engineering needs.

4.2.5 Third-Party relationships

- GP-OP-12: Data processed by a third-party must be protected by a data processing agreement.
- GP-OP-13: Only share consumers' personal data with third parties with express consent of the consumers, unless otherwise required and limited for the use of product features or service operations.
- GP-OP-14: For IoT hardware manufacturers and IoT software developers it is necessary to adopt cyber supply chain risk management policies and to communicate cyber security requirements to its suppliers and partners.

4.3 Technical Measures

Evidently, the security measures and good practices need to consider and cover the technical elements, in order to diminish the vulnerabilities of IoT. Below we provide an overview of the necessary technical measures to preserve and protect the security of information in IoT. Since these are horizontal measures across vertical sectors/CIIs, given the particularities of each vertical, more concrete measures can be introduced for each vertical/CII.

Applying these technical measures should take into account the particularities of the IoT ecosystem such as scalability, namely given the huge number of involved devices certain measures might need to be carried out at the level of specialised architectural components, e.g. gateways.

4.3.1 Hardware security

- GP-TM-01: Employ a hardware-based immutable root of trust.
- GP-TM-02: Use hardware that incorporates security features to strengthen the protection and integrity of the device – for example, specialised security chips / coprocessors that integrate security at the transistor level, embedded in the processor, providing, among other things, a trusted storage of device identity and authentication means, protection of keys at rest and in use, and preventing unprivileged from accessing to security sensitive code. Protection against local and physical attacks can be covered via functional security.

4.3.2 Trust and Integrity Management

- GP-TM-03: Trust must be established in the boot environment before any trust in any other software or executable program can be claimed.
- GP-TM-04: Sign code cryptographically to ensure it has not been tampered with after signing it as safe for the device, and implement run-time protection and secure execution monitoring to make sure malicious attacks do not overwrite code after it is loaded.
- GP-TM-05: Control the installation of software in operating systems, to prevent unauthenticated software and files from being loaded onto it.
- GP-TM-06: Enable a system to return to a state that was known to be secure, after a security breach has occured or if an upgrade has not been successful.
- GP-TM-07: Use protocols and mechanisms able to represent and manage trust and trust relationships.

4.3.3 Strong default security and privacy

- GP-TM-08: Any applicable security features should be enabled by default, and any unused or insecure functionalities should be disabled by default.
- GP-TM-09: Establish hard to crack, device-individual default passwords.

4.3.4 Data protection and compliance

- GP-TM-10: Personal data must be collected and processed fairly and lawfully, it should never be collected and processed without the data subject's consent.
- GP-TM-11: Make sure that personal data is used for the specified purposes for which they were collected, and that any further processing of personal data is compatible and that the data subjects are well informed.
- GP-TM-12: Minimise the data collected and retained.
- GP-TM-13: IoT stakeholders must be compliant with the EU General Data Protection Regulation (GDPR).
- GP-TM-14: Users of IoT products and services must be able to exercise their rights to information, access, erasure, rectification, data portability, restriction of processing, objection to processing, and their right not to be evaluated on the basis of automated processing.

4.3.5 System safety and reliability

- GP-TM-15: Design with system and operational disruption in mind, preventing the system from causing an unacceptable risk of injury or physical damage.
- GP-TM-16: Mechanisms for self-diagnosis and self-repair/healing to recover from failure, malfunction or a compromised state.
- GP-TM-17: Ensure standalone operation - essential features should continue to work with a loss of communications and chronicle negative impacts from compromised devices or cloud-based systems.

4.3.6 Secure Software / Firmware updates

- GP-TM-18: Ensure that the device software/firmware, its configuration and its applications have the ability to update Over-The-Air (OTA), that the update server is secure, that the update file is transmitted via a secure connection, that it does not contain sensitive data (e.g. hardcoded credentials), that it is signed by an authorised trust entity and encrypted using accepted encryption methods, and that the update package has its digital signature, signing certificate and signing certificate chain, verified by the device before the update process begins.
- GP-TM-19: Offer an automatic firmware update mechanism.
- GP-TM-20: Backward compatibility of firmware updates. Automatic firmware updates should not modify user-configured preferences, security, and/or privacy settings without user notification.

4.3.7 Authentication

- GP-TM-21: Design the authentication and authorisation schemes (unique per device) based on the system-level threat models.
- GP-TM-22: Ensure that default passwords and even default usernames are changed during the initial setup, and that weak, null or blank passwords are not allowed.
- GP-TM-23: Authentication mechanisms must use strong passwords or personal identification numbers (PINs), and should consider using two-factor authentication (2FA) or multi-factor authentication (MFA) like Smartphones, Biometrics, etc., on top of certificates.
- GP-TM-24: Authentication credentials shall be salted, hashed and/or encrypted.
- GP-TM-25: Protect against 'brute force' and/or other abusive login attempts. This protection should also consider keys stored in devices.
- GP-TM-26: Ensure password recovery or reset mechanism is robust and does not supply an attacker with information indicating a valid account. The same applies to key update and recovery mechanisms.

4.3.8 Authorisation

- GP-TM-27: Limit the actions allowed for a given system by Implementing fine-grained authorisation mechanisms and using the Principle of least privilege (POLP): applications must operate at the lowest privilege level possible.
- GP-TM-28: Device firmware should be designed to isolate privileged code, processes and data from portions of the firmware that do not need access to them. Device hardware should provide isolation concepts to prevent unprivileged from accessing security sensitive code.

4.3.9 Access Control - Physical and Environmental security

- GP-TM-29: Data integrity and confidentiality must be enforced by access controls. When the subject requesting access has been authorised to access particular processes, it is necessary to enforce the defined security policy.
- GP-TM-30: Ensure a context-based security and privacy that reflects different levels of importance.
- GP-TM-31: Measures for tamper protection and detection. Detection and reaction to hardware tampering should not rely on network connectivity.

- GP-TM-32: Ensure that the device cannot be easily disassembled and that the data storage medium is encrypted at rest and cannot be easily removed.
- GP-TM-33: Ensure that devices only feature the essential physical external ports (such as USB) necessary for them to function and that the test/debug modes are secure, so they cannot be used to maliciously access the devices. In general, lock down physical ports to only trusted connections.

4.3.10 Cryptography

- GP-TM-34: Ensure a proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of data and information (including control messages), in transit and in rest. Ensure the proper selection of standard and strong encryption algorithms and strong keys, and disable insecure protocols. Verify the robustness of the implementation.
- GP-TM-35: Cryptographic keys must be securely managed.
- GP-TM-36: Build devices to be compatible with lightweight encryption and security techniques.
- GP-TM-37: Support scalable key management schemes.

4.3.11 Secure and trusted communications

- GP-TM-38: Guarantee the different security aspects -confidentiality (privacy), integrity, availability and authenticity- of the information in transit on the networks or stored in the IoT application or in the Cloud.
- GP-TM-39: Ensure that communication security is provided using state-of-the-art, standardised security protocols, such as TLS for encryption.
- GP-TM-40: Ensure credentials are not exposed in internal or external network traffic.
- GP-TM-41: Guarantee data authenticity to enable reliable exchanges from data emission to data reception. Data should always be signed whenever and wherever it is captured and stored.
- GP-TM-42: Do not trust data received and always verify any interconnections. Discover, identify and verify/authenticate the devices connected to the network before trust can be established, and preserve their integrity for reliable solutions and services.
- GP-TM-43: IoT devices should be restrictive rather than permissive in communicating.
- GP-TM-44: Make intentional connections. Prevent unauthorised connections to it or other devices the product is connected to, at all levels of the protocols.
- GP-TM-45: Disable specific ports and/or network connections for selective connectivity.
- GP-TM-46: Rate limiting. Controlling the traffic sent or received by a network to reduce the risk of automated attacks.

4.3.12 Secure Interfaces and network services

- GP-TM-47: Risk Segmentation. Splitting network elements into separate components to help isolate security breaches and minimise the overall risk.
- GP-TM-48: Protocols should be designed to ensure that, if a single device is compromised, it does not affect the whole set.
- GP-TM-49: Avoid provisioning the same secret key in an entire product family, since compromising a single device would be enough to expose the rest of the product family.
- GP-TM-50: Ensure only necessary ports are exposed and available.
- GP-TM-51: Implement a DDoS-resistant and Load-Balancing infrastructure.
- GP-TM-52: Ensure web interfaces fully encrypt the user session, from the device to the backend services, and that they are not susceptible to XSS, CSRF, SQL injection, etc.
- GP-TM-53: Avoid security issues when designing error messages.

4.3.13 Secure input and output handling

- GP-TM-54: Data input validation (ensuring that data is safe prior to use) and output filtering.

4.3.14 Logging

- GP-TM-55: Implement a logging system that records events relating to user authentication, management of accounts and access rights, modifications to security rules, and the functioning of the system. Logs must be preserved on durable storage and retrievable via authenticated connections.

4.3.15 Monitoring and Auditing

- GP-TM-56: Implement regular monitoring to verify the device behaviour, to detect malware and to discover integrity errors.
- GP-TM-57: Conduct periodic audits and reviews of security controls to ensure that the controls are effective. Perform penetration tests at least biannually.

5. Gaps analysis

This section provides an analysis of the main gaps in relation to cyber security in IoT. A critical part to address cyber security in IoT is the identification and definition of gaps -the space between the present state and the desired state- so as to determine what steps need to be taken in order to close those gaps, namely, to move from the current immature state to the future and more mature state. In the interviews conducted with IoT experts there was a common denominator – in terms of maturity, the security in IoT is in an initial stage of development. The following gaps were identified as being the most prominent ones by the experts who took part in the study and by conducting a comparative analysis of existing IoT security resources as listed in Annex C.

We examine the gaps by taking into account two aspects, namely beginning with the analysis of the barriers and ending with the changes that need to be considered to improve and guarantee security in IoT. We also outline the relevant challenges that act as hindering factors towards a more mature IoT security landscape. The ultimate goal of addressing the IoT security and safety gaps is to ensure the priotection of all assets, to preserve the required level of privacy, as well as attain and sustain a high level of resiliency against cyber attacks thus ensures physical safety alongside cyber security.

5.1 Gap 1: Fragmentation in existing security approaches and regulations

Currently, there is no common EU-wide approach to cyber security in IoT, or a common multi-stakeholder model on cyber security. In the interviews carried out throughout the study, the majority of experts considered the lack of mature security frameworks, and the breadth of security considerations to take into account, big barriers for the improvement of security. Therefore, most companies and manufacturers are taking their own approach when implementing security into IoT, resulting in a lack or slow embracement of standards to guide the adoption of IoT security measures and good practices.

Whereas stringent measures and legislation introduced by regulators could become restrictive for security research, development and innovation, it could be more effective if initiatives were put in place to stimulate the development of security in private companies. Nevertheless, the key to rapid progress in this area is **to get the public and private sectors to work together** and understand that security does not only concern a single manufacturer, customer or IT professional[76], but rather everyone involved in the process. Cybersecurity is a shared responsibility.

The fragmentation of the regulations also poses a barrier when Critical Information Infrastructures are seen hand in hand with the IoT world, since there is no regulation that forces security measures and protocols in the different levels of an IoT ecosystem, including the devices, the network, etc. This could potentially allow for a more complete integration of safety and security in the development lifecycles. Conversely, the application of one-size fits all standards across the IoT ecosystem might be seen as a hindering factor for innovation and research in the area. As discussed throughout the report, one needs to also consider the fact that different application areas have diverse security requirements.

Another significant problem to tackle is that of unclear liabilities – there is a barrier of non-responsibility, both moral and legal, which can be mitigated or solved by enforcing responsibilities. There has been no chance to enforce a perfect isolation between the different elements of an IoT ecosystem, which will

[76] See https://www.govtechworks.com/iot-security-risks-begin-with-supply-chains/

unavoidably be developed by different manufacturers and/or operated by different parties. In this context, there is a need to clarify the liability of each actor in case of a security event.

5.2 Gap 2: Lack of awareness and knowledge

There is a gap in relation to the increasing move towards connected and interdependent systems and devices as far as knowledge is concerned. In the interviews with IoT experts, differences in fundamental terminology were encountered, such as the difference between the concepts of safety and security. Security experts are more commonly familiar with "business IT" security, but not with IoT security.

There is an overall lack of awareness regarding the need of security in IoT devices. Even more worrisome is the lack of knowledge regarding the threats they are exposed to – most IoT consumers do not have a basic understanding of their IoT devices and the impact on their environment. This may result in the devices not being updated, with a subsequent breach of security.

Moreover, companies should train their employees in good security practices, recognising that technological expertise does not necessarily equate with security expertise. In general, there is a need to properly educate a new generation of consumers, developers, manufacturers, etc. about the use and the security risks posed by IoT, and how to be prepared. It is also necessary to train them in both safety and cyber security to increase awareness.

Many security incidents could be avoided if developers and manufacturers were aware of the risks they face on a daily basis, considering not only those affecting IoT devices but also those affecting the whole IoT environment. This is becoming a common need in order to raise awareness about current threats and risks and to provide knowledge on how to prevent, protect and act in case of a security incident.

5.3 Gap 3: Insecure design and/or development

There have been several studies on design and development concerns related to IoT security[77,78,79,80]. During the interviews engaged within the context of this report we validated the findings of these studies and in this respect the following issues seem particularly significant in the context of IoT design and development:

- No defence-in-depth strategy during the design of the system, such as a secure boot process, isolation of a Trusted Computing Base, limitation of the number of open ports, self-protection, etc.
- No security-by-design or privacy-by-design. In some cases, information is exchanged with a third-party, and it should be ensured that not more information than strictly needed is exported outside of the IoT environment.
- Lack of communication protection, on internal as well as external interfaces.
- Lack of strong authentication and authorisation:
  - No validation or signing of firmware updates,
  - Software updates without server authentication and file trust verification,
  - No secure boot mechanisms.
- Lack of hardening:
  - No data execution prevention or attack mitigation technologies used on the firmware,

[77] See http://otalliance.actonsoftware.com/acton/attachment/6361/f-008e/1/-/-/-/-/IoT Framework Resource Guide.pdf
[78] See http://www.gsma.com/connectedliving/wp-content/uploads/2016/11/CLP.12-v1.1.pdf
[79] See https://cloudsecurityalliance.org/download/new-security-guidance-for-early-adopters-of-the-iot/
[80] See https://www.symantec.com/security-center/threat-report

- Public vulnerabilities (DNS proxy, HTTP service...) left unfixed,
- Some services are exposed through different entry points, with unnecessary communication ports left open – services such as Telnet or ssh are sometimes bound to all network interfaces,
- Weak passwords policies or default passwords left unchanged,
- Configuration flaws.

- Lack of diagnosis / response capabilities.

5.4 Gap 4: Lack of interoperability across different IoT devices, platforms and frameworks

The great majority of IoT ecosystems include IoT devices connected with legacy systems, especially in the case of Critical Information Infrastructures. Moreover, as previously mentioned, due to the lack of a common regulation, most companies and manufacturers are taking their own approach when designing IoT devices, causing interoperability issues between devices from different manufacturers as well as the emergence of different security models, incompatible concepts and taxonomies, etc. Therefore, it is very important to develop measures that ensure a correct and secure interconnection and interoperability between the IoT environment and legacy systems, and the other IoT devices manufactured by third-parties.

Most IoT devices use proprietary protocols designed by their manufacturers in order to interconnect devices. While this is not an issue for devices from the same manufacturer, it becomes a problem when interconnecting devices from different manufacturers. This requires the development and use of standard protocols that need to be supported by all manufacturers to ensure a good level of interoperability with the least efficiency and security loss. A good practice in this regard is to avoid the use of close-source and proprietary protocols, as their security cannot be verified, and many incidents have already proven that security through obscurity does not necessarily equate proper security coverage.

In the same spirit, apart from protocols, the use of common frameworks can also help to improve the efficiency and security of the devices when interconnecting several ones from different manufacturers.

5.5 Gap 5: Lack of economic incentives

The main IoT manufacturers and vendors usually consider functionality and usability much more important than implementing secure design and programming. Their economic interests are not aligned with spending much money on security, and in some cases they do not consider security at all. The main reason for these companies no to dedicate much of their budget to security is the general perception that there is no direct return-on-investment for security, which can be attributed to the economic cost and the difficulty to assess the financial impact of hypothetical security weaknesses.

This is worsened by the lack of economic incentives that would help to improve security, such as economic benefits (e.g. more grants to integrate better security in the devices), resources, perceived reputation, etc. Apart from this, the economic support is only accessible through very competitive programs such as H2020 in the case of research and development.

In general, the IoT experts interviewed agree that the different risks, threats and hazards are usually underestimated and left out because of budgetary issues – there is a tendency to handle security concerns a posteriori of incidents.

5.6 Gap 6: Lack of proper product lifecycle management

In general, safety measures are found lacking from the design phase to its later development. This demonstrates the need for a proper product lifecycle management of the different assets that compose a

given IoT environment, since the devices and networks are interconnected and, in most cases, exposed to the Internet, where they can be targeted by many and diverse threats.

IoT comprises such a variety of products that, if left unattended, it makes the entire surface of the traditional supply chain vulnerable. IoT expands the global attack surface and it is everyone's responsibility to manage the risks. The different devices and products will have to evolve in a secure way to consistently provide, through their whole lifecycle, the solution for which they were created.

In this process, it is necessary to involve the vendors and, since they are in charge of designing and developing the devices, they are in an ideal position to implement the changes needed – they are able to proficiently and cost-efficiently include new security features or characteristics. This, however, is not only dependent on manufacturers adding these new features, but also on organisations accepting the related costs; therefore, a balance between security and cost must be maintained.

Through their lifecycle, IoT devices must be able to be patched and updated rapidly to ensure their correct operation and to amend all the vulnerabilities that are continuously being discovered. As mentioned before, in consumer environments most IoT users do not have a basic understanding of their IoT devices and their impact on their environment, which may result in the devices not being updated and a subsequent breach of security.

In addition, one important phase of the device lifecycle management is the deployment phase. Best practices for IoT deployment could be defined. They may include recommendations for specific configurations of devices and networks or the need to implement cybersecurity monitoring systems to detect anomalies in the deployed infrastructure.

6. High-level recommendations to improve IoT cybersecurity

This chapter includes a list of high-level recommendations for developers, operators and security experts that will help them to improve the security level of IoT devices and communications among them. The recommendations discussed here concern stakeholders that span the entire IoT spectrum and aim to address the gaps defined in Chapter 5.

6.1 Recommendations

The recommendations proposed are listed in the following table, and they have been further developed in section 6.2:

ID	DESCRIPTION
1	Promote harmonization of IoT security initiatives and regulations
2	Raise awareness for the need for IoT cybersecurity
3	Define secure software/hardware development lifecycle guidelines for IoT
4	Achieve consensus for interoperability across the IoT ecosystem
5	Foster economic and administrative incentives for IoT security
6	Establishment of secure IoT product/service lifecycle management
7	Clarify liability among IoT stakeholders

Table 8: IoT Security Recommendations

6.2 Detailed recommendations

6.2.1 Promote harmonization of IoT security initiatives and regulations

Recommendation intended for: IoT industry, providers, manufacturers, associations

The current fragmentation of IoT security guidelines, initiatives, standards and other schemes needs to be addressed. A first and solid step in the direction is to define a list of best practices and guidelines for IoT security and privacy, which can be used as a baseline for the development and deployment of IoT systems in the market (for example consult reports from AIOTI and ECSO). The current ENISA report provides such a list and goes one step further by categorizing all security measures according to a well-defined and structured set of security domains.

In terms of harmonization of standards, it is interesting to note that the notion of standard is appreciated and supported by the industry but groups of stakeholders have different R&D chains and this inherently drives fragmentation. The recommendation to counter this fragmentation refers to establishing a set of practices, guidelines and security requirements in IoT, which are common over Europe. The Commission should be facilitator of this process and this ENISA report can serve as the springboard for related efforts. Subsequently, each sector can focus on defining the specific sets of practices, guidelines, requirements for its own needs based on the particular context and risk factors inherent in each sector. European Commission and member states government could drive the coordination and collaboration of stakeholders (industry, users) and ENISA can be an important facilitator in this process.

The procurement process is another means to impose harmonization of baseline standards and requirements for IoT systems. The harmonization should consider that there are many different sectors (e.g. energy, transportation) , so harmonization should be first achieved within each sector.

6.2.2 Raise awareness for the need for IoT cybersecurity

Recommendation intended for: IoT industry, providers, manufacturers, associations, academia, consumer groups, regulators

Cybersecurity is a shared responsibility among all involved stakeholders. It is thus essential for thse stakeholders to have a thorough understanding of related risks and threats, as well as ways to secure and protect against them. Raising awareness is therefore of paramount importance and initiatives to do so are highly recommended.

As evidenced by the growing threat landscape and the numerous security incidents concerning IoT, there is lack of knowledge present within IoT developers, industries as wll as end users and consumers. To overcome such deficiency it is important to define targeted recommendations for all three stakeholder categories, namely:

- Security education and training needs to be established in industries, including knowledge of state-of-the-art, best practices, reference architectures and availability of building blocks, methodologies and tools for secure IoT systems.
- End users and consumers have to be educated to be able to make informed decisions when buying IoT devices and systems. Campaigns raising awareness for IoT security are thus highly important, also in order to be able to maintain a basic level of cyber hygiene for the security of the "Things" that they have purchased or are operating. The role and initiatives of consumer rights associations should be highlighted in this respect.
- Among the developer community, awareness needs to be raised to adopt fundamental security principles that are cross vertical rather than being tied to any silo industry. Corporate trainings focused on IoT security are also beneficial and should be pursued.

Similarly, initiatives like café scientific and cyber security clinics can prove to be effective.Lastly, trainings and courses at schools and universities (considering localisation to reach a wider audience) will further promote a better understanding of IoT security among the younger generation and thus in the long-term contributed to raising awareness.

6.2.3 Define secure software/hardware development lifecycle guidelines for IoT

Recommendation intended for: IoT developers, platform operators, industry, manufacturers

Developers, manufacturers and providers of IOT products and solutions should integrate and adopt a secure software development lifecycle (SSDLC) for their IoT offerings and incorporate relevant processes in their operations. Security must be implemented as a whole, at the application level, and in each of the phases of the SDLC. It is therefore important to encourage more companies to offer secure components that are at the same time usable for developers and end users/consumers.

The notions of **security and privacy by default** and **security and privacy by design** naturally emerge as being foundation cornerstones of IoT security. Evidently, it is challenging to apply these concepts in several different environments that will have particular characteristics. In IoT the cyber risk is context-dependent (i.e. based on the application scenario) and in this respect the principles of security and privacy by design should be applied with this consideration in mind. Following relevant initiatives from other, more mature IT sectors can prove to be beneficial in adopting such principles for the IoT ecosystem.

As far as developers are concerned, secure by design hackathons and use of best practice cookbooks for IoT security can greatly enhance their perception of using principle of security and privacy by default and by design. The lessons learned from such exercises would assist developers in applying corresponding techniques within their projects and products. When focussing on companies, the use of proper security processes and well-defined and widely accepted tools (e.g. standards, checklists) for IoT security would strongly promote the cause for IoT security by default and by design.

6.2.4 Achieve consensus for interoperability across the IoT ecosystem

Recommendation intended for: IoT industry, providers, manufacturers, associations, regulators

The issue of interoperability is very pertinent to the IoT ecosystem due to the very large scale and penetration of the IoT ecosystem, the long and complex supply chains and the numerous involved stakeholders. Ensuring and fostering interoperability of IoT devices, platforms and frameworks, as well as security practices is therefore an essential element of IoT security and should thus be encouraged.

Recommendations that will undoubtedly assist in this direction include:

- Encourage the use of open interoperability frameworks that incorporate security
- Provide transparency on the security of interoperability frameworks
- Promote open and accessible interoperability laboratories and testbeds for security

It should be noted that said recommendations are indicative and continuous efforts towards promoting interoperability in the context of end-to-end and consistent cybersecurity should be pursued.

6.2.5 Foster economic and administrative incentives for IoT security

Recommendation intended for: IoT industry, associations, academia, consumer groups, regulators

It is clear that lack of security impacts business continuity and this is indeed the case also for IoT that is driven by R&D activities and a rush to push products and services in the market. In this respect, business continuity can serve as a driver for justifying costs in cyber security solutions.

Moreover, market demands on cybersecurity are somewhat low because of the lack of consumer perception in the added value of cybersecurity. Consumer involvement is quite important and it should be supported more. Communication campaigns should be implemented by the government (e.g., the Commission, member states) in order to increase and sustain said perception and thus inherently necessitate the adoption of further mechanisms to promote IoT cybersecurity.

In the case of IoT, competitive advantage is currently placed and focussed on the time to market rather than secure to market. This balance should be shifted so that a specific level of security and privacy before market deployment is encouraged. Defining security frameworks supported by baseline security measures can be a way forward in this direction. Use of other schemes such as certification and labelling can also encourage better understanding and transparency in terms of IoT security and thus should be considered (also benefitting end users and consumers in educating them and making them more aware of IoT security), albeit in a context and risk specific manner per use case/application sector. Subject to such approaches, subsequently regulative efforts and initiatiaves could then be put in place to follow the same path.

6.2.6 Establishment of secure IoT product/service lifecycle management

Recommendation intended for: IoT developers, platform operators, industry, manufacturers

Security plays an important role within all the phases of an IoT product's/service's lifecycle. These phases include design, development, testing, production, deployment, maintenance, end-of-support, and end-of-life (i.e. decommissioning). It is recommeneded that specific, focussed and targeted security processes be defined for all these phases.

Furthermore, security processes have to be properly implemented. In order to satisfy this need, fundamental security requirements and building blocks have to be specified to be available within each phase.

A noteworthy aspect involves security updates that constitute a significant issue in the context of IoT. After deployment, security updates need to be provided where practically possible whithout special knowledge requirements or financial obligations on the end user/consumer within a defined term and conditions until "end-of-support". The latter must be clearly defined by the manufacturer/provider of the IoT product and must be clearly communicated to the end user/consumer.

6.2.7 Clarify liability among IoT stakeholders

Recommendation intended for: IoT industry, regulators

As identified by the interviews with the experts a very important issue when IoT is considered is that of liability. It is of particular importance in the IoT domain, since the cyber-physical nature of IoT relates and tightly binds security to safety. The question of liability needs to be addressed. The question of where liability may fall lies between the different and diverse stakeholders of the IoT ecosystem, such as developers, manufacturers, providers, vendors, aftermarket support operators, third party providers and the end users, to name a few.

The liability issues have to be addressed in the context of European and national legislation and case law. Where gaps are identified in said legislation, these should be addressed.

Glossary

6LoWPAN	IPv6 over Low Power Wireless Personal Area Network
APT	Advanced Persistent Threat
AMQP	Advanced Message Queuing Protocol
BLE	Bluetooth Low Energy
CASB	Cloud Security Access Broker
CARP	Channel-Aware Routing Protocol
CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
CISO	Chief Information Security Officer
CoAP	Constrained Application Protocol
DDS	Data Distribution Service
(D)DoS	(Distributed) Denial of Service
IIC	Industrial Internet Consortium
ICT	Information and Communication Technology
IoT	Internet of Things
IoTSEC	Internet of Things SECurity
IIoT	Industrial Internet of Things
LPWAN	Low Power Wide Area Network
M2M	Machine-to-Machine
MQTT	Message Queue Telemetry Transport
NB-IoT	NarrowBand-IoT
NFC	Near Field Communication
QoS	Quality of Service
RBAC	Role-Based Access Control
RFID	Radio Frequency Identification
RPL	Routing Protocol for Low-Power and Lossy Networks

SME	Small and medium-sized enterprise
SDN	Software-Defined Networking
VPN	Virtual Private Network
WAF	Web Application Firewall
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network
WWAN	Wireless Wide Area Network
XMPP	eXtensible Messaging and Presence Protocol

Annex A: Detailed Security measures / Good practices

	SECURITY MEASURES / GOOD PRACTICES	SECURITY DOMAIN	REFERENCES
Security by design	GP-PS-01: Consider the security of the whole IoT system in a consistent and holistic approach along its whole lifecycle across all levels of device/application design and development, integrating security throughout the development, manufacturing, and deployment	Ecosystem Management IT Security Architecture	- ISO27001 #A14. System acquisition, development and maintenance - NIST SP 800-53 - System And Services Acquisition Control Family (SA) - NIST Framework for Improving Critical Infrastructure Cybersecurity - OWASP Security by Design Principles - DG Commissioned Study - Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination - Article 29 Data Protection Working Party - Opinion 8/2014 on the on Recent Developments on the Internet of Things
	GP-PS-02: Ensure the ability to integrate different security policies and techniques, so as to ensure a consistent security control over the variety of devices and user networks in IoT	Ecosystem Management	- U.S. Department of Homeland Security - Strategic Principles For Securing The Internet Of Things (IoT) - U.S. Department of Commerce, National Telecommunications and Information Administration, internet policy task force & digital economy leadership team - fostering the advancement of the internet of things
	GP-PS-03: Security must consider the risk to human safety	Physical and environmental security	- U.S. Federal Communications Commission, Public Safety & Homeland Security Bureau - FCC White Paper, Cybersecurity Risk Reduction - EC Alliance for Internet of Things Innovation (AIOTI) - FTC - Internet of Things: Privacy & Security in a Connected World
	GP-PS-04: Design for power conservation should not compromise security	IT Security Architecture	- Cloud Security Alliance (CSA) - New Security Guidance for Early Adopters of the IoT - IoT Security Foundation (IoTSF) - GSM Association (GSMA) - IoT Security Guidelines - Atlantic Council (Brent Scowcroft Center On International Security) - Smart Homes and the Internet of Things
	GP-PS-05: Design architecture by compartments to encapsulate elements in case of attacks	IT Security Architecture	- IETF (Internet Engineering Task Force) - IETF RFC 7452 Architectural Considerations in Smart Object Networking - IETF (Internet Engineering Task Force) - Best Current Practices for Securing Internet of Things (IoT) Devices
	GP-PS-06: For IoT hardware manufacturers and IoT software developers it is necessary to implement test plans to verify whether the product performs as it is expected. Penetration tests help to identify malformed input handling, authentication bypass attempts and overall security posture.	IT security maintenance	- OASIS (Organization for the Advancement of Structured Information Standards) - Technical Committees - ISACA - Performing a Security Risk Assessment - AIOTI. Digitisation of Industry Policy Recommendations - International Telecommunication Union (ITU) - Unleashing the potential of the Internet of Things
	GP-PS-07: For IoT software developers it is important to conduct code review during implementation as it helps to reduce bugs in a final version of a product.	IT security maintenance	- AT&T Cybersecurity Insights - Exploring IoT Security Volume 2 - Symantec - An Internet of Things Reference Architecture - Microsoft - Cybersecurity Policy For The Internet Of Things - Infineon - Hardware Security for Smart Grid End Point Devices

	SECURITY MEASURES / GOOD PRACTICES	SECURITY DOMAIN	REFERENCES
Privacy by design	GP-PS-08: Privacy must be a guiding principle when designing and developing systems, in order to make privacy an integral part of the system.	Information System Security Governance & Risk Management	- ISO27001 #A14. System acquisition, development and maintenance - NIST SP 800-53 - System And Services Acquisition Control Family (SA) - OWASP Security by Design Principles - DG Commissioned Study - Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination - ARTICLE 29 Data Protection Working Party - Opinion 8/2014 on the on Recent Developments on the Internet of Things - EC Alliance for Internet of Things Innovation (AIOTI) - IOT-A (Internet of Things Architecture) - U.S. Department of Commerce, National Telecommunications and Information Administration, Internet Policy Task Force & Digital Economy Leadership Team - Fostering The Advancement Of The Internet Of Things - U.S. Federal Communications Commission, Public Safety & Homeland Security Bureau - The President's National Security Telecommunications Advisory Committee - NSTAC Report to the President on the Internet of Things - Cloud Security Alliance (CSA) - Future-proofing the Connected World: 13 Steps to Developing Secure IoT Products - Cloud Security Alliance (CSA) - New Security Guidance for Early Adopters of the IoT - GSM Association (GSMA) - IoT Security Guidelines - International Electrotechnical Commission (IEC) - IEC White Paper on "IoT 2020: Smart and secure IoT platform" - AIOTI. Digitisation of Industry Policy Recommendations - ISO27001 #A8. Asset Management - NIST SP 800-53 - PE-20 Asset Monitoring And Tracking - U.S. Department of Health and Human Services Food and Drug Administration (FDA) Center for Devices and Radiological Health - Postmarket Management of Cybersecurity in Medical Devices Guidance for Industry and Food and Drug Administration Staff - GSM Association (GSMA) - IoT Security Guidelines
	GP-PS-09: Perform privacy impact assessments before any new applications are launched, using a top-down decomposition method that requires first answering three fundamental questions: - Where is the targeted application deployed (Legal constraints and cultural significance) - For what purpose (Scope) - For which scenarios (Business requirements)	Information System Security Governance & Risk Management	
Asset Management	GP-PS-10: Establish and maintain asset management procedures and configuration controls for key network and information systems, to identify and authenticate of the assets involved in the IoT Service (i.e. Gateways, Endpoint devices, home network, roaming networks, service platforms, etc.).	IT Security Architecture	

	SECURITY MEASURES / GOOD PRACTICES	SECURITY DOMAIN	REFERENCES
	GP-PS-11: Identify significant risks using a defence-in-depth approach. Conduct end-to-end risk assessments that account for both internal and third-party vendor risks, where possible. Developers and manufacturers should include vendors and suppliers in the risk assessment process, which will create transparency and enable them to gain awareness of potential third-party vulnerabilities and promote trust and transparency. Security should be readdressed on an ongoing basis as the component in the supply chain is replaced, removed or upgraded.	Information System Security Governance & Risk Management	- ISO27001 #6. Planning - NIST SP 800-30 - NIST SP 800-53 - Risk Assessment Control Family (SA) - NIST Framework for Improving Critical Infrastructure Cybersecurity - OWASP Testing Guide v4 - Risk Rating Methodology - IOT-A (Internet of Things Architecture) - U.S. Department of Homeland Security - Strategic Principles For Securing The Internet Of Things (IoT) - FTC - Internet of Things: Privacy & Security in a Connected World - U.S. Department of Health and Human Services Food and Drug Administration (FDA) Center for Devices and Radiological Health - Postmarket Management of Cybersecurity in Medical Devices Guidance for Industry and Food and Drug Administration Staff - Software Assurance Forum for Excellence in Code (SAFECode) - NPO - Call it the Internet of Connected Things: The IoT Security Conundrum - Cloud Security Alliance (CSA) - Future-proofing the Connected World: 13 Steps to Developing Secure IoT Products - Cloud Security Alliance (CSA) - New Security Guidance for Early Adopters of the IoT - IoT Security Foundation (IoTSF) - GSM Association (GSMA) - IoT Security Guidelines - oneM2M - Standards for M2M and the Internet of Things - Internet Research Task force (IRTF) - State-of-the-Art and Challenges for the Internet of Things Security - International Telecommunication Union (ITU) - Unleashing the potential of the Internet of Things - AT&T Cybersecurity Insights - Exploring IoT Security Volume 2 - U.S. Department of Homeland Security - Strategic Principles For Securing The Internet Of Things (IoT) - Cloud Security Alliance (CSA) - Future-proofing the Connected World: 13 Steps to Developing Secure IoT Products - EuroSMART (the voice of the Smart Security Industry) - Internet Of Trust Security And Privacy In The Connected World
Risks and Threats Identification and Assessment	Risk Assessment procedure should be initiated using a top-down decomposition method that requires first answering three fundamental questions: - Where is the targeted application deployed (Legal constraints and cultural significance) - For what purpose (Scope) - For which scenarios (Business requirements)		
	GP-PS-12: Identify the intended use and environment of a given IoT device. This will help developers and manufacturers determine the most suitable technical features for the IoT device's operation, and the security measures required. This will also help to effectively handle bugs or enhancement requests.	Information System Security Governance & Risk Management IT Security Architecture	
Hardware security	GP-TM-01: Employ a hardware-based immutable root of trust. The Hardware Root of Trust is a trusted hardware component which receives control at power-on. It then extends the chain of trust to other hardware, firmware, and software components. The Root of Trust should then be attestable by software agents running within and throughout the infrastructure.	IT Security Architecture Physical and environmental security	

	SECURITY MEASURES / GOOD PRACTICES	SECURITY DOMAIN	REFERENCES
	GP-TM-02: Use hardware that incorporates security features to strengthen the protection and integrity of the device – for example, specialised security chips / coprocessors that integrate security at the transistor level, embedded in the processor, that provide: - Chain of trust boot-loader which authenticates the operating system before loading it - Chain of trust operating system which authenticates application software before loading it - Hardware secure boot process and Locking Critical Sections of Memory - Protected memory (NVM/RAM/Cache) to avoid snooping and reverse engineering - Encryption and anonymity - Random Number Generation (RNG) - Tamper detection - Environment monitoring and internal control - Trusted Execution Environment. Secure Code fetching & Execution (Integrity checks) - Code and data signatures, built during compilation and stored and verified during execution - A trusted storage of device identity and authentication means, including protection of keys at rest and in use - Protection against unprivileged accessing security sensitive code Protection against local and physical attacks can be covered via functional security.	IT Security Architecture Physical and environmental security	- IETF (Internet Engineering Task Force) - IETF RFC 7452 Architectural Considerations in Smart Object Networking - ISACA - Performing a Security Risk Assessment - IoT Security Foundation (IoTSF) - GSM Association (GSMA) - IoT Security Guidelines - OpenFog Consortium - The 8 Pillars of the OpenFog Reference Architecture - International Electrotechnical Commission (IEC) - IEC White Paper on "IoT 2020: Smart and secure IoT platform" - Symantec - An Internet of Things Reference Architecture - Microsoft - Cybersecurity Policy For The Internet Of Things - Industrial Internet Consortium (IIC)
Trust and Integrity Management	GP-TM-03: The boot process initialises the main hardware components, and starts the operating system. Trust must be established in the boot environment before any trust in any other software or executable program can be claimed, so the booted environment must be verified and determined to be in an uncompromised state.	IT Security Architecture	- ISO27001 #A12. Operations security - NIST SP 800-30 - NIST SP 800-53 - SA-13 Trustworthiness - SI-7 Software, Firmware, And Information Integrity - CM-11 User-Installed Software
	GP-TM-04: Sign code cryptographically to ensure it has not been tampered with after being signed as safe for the device, and implement run-time protection and secure execution monitoring to be sure malicious attacks do not overwrite code after it is loaded. Only run signed code and never unsigned code. Measuring the boot-process enables the detection of manipulation of the host OS and software, so that malicious changes in the behaviour of the devices	IT Security Architecture	- NIST SP 800-160 - F.1.18 Trusted Communication Channels - European Commission - Advancing the Internet of Things in Europe - IERC European Research Cluster on the Internet of Things - The President's National Security Telecommunications Advisory Committee - NSTAC Report to the President on the Internet of Things - IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework (IIC:PUB:G4:V1.0:PB:20160926)

	SECURITY MEASURES / GOOD PRACTICES	SECURITY DOMAIN	REFERENCES
	can be detected. It enables boot-time detection of rootkits, viruses and worms.		- Trusted Computing Group (TCG) - Guidance for Securing IoT Using TCG Technology Reference Document - IoT Security Foundation (IoTSF) - Symantec - An Internet of Things Reference Architecture - Infineon - Hardware Security for Smart Grid End Point Devices
	GP-TM-05: Control the installation of software on operational systems, to prevent unauthenticated software and files being loaded onto it. In the event that the product is intended to allow un-authenticated software, such software should only be run with limited permissions and/or sandbox.	Identity and access management	
	GP-TM-06: Restore Secure State - Enable a system to return to a state that was known to be secure, after a security breach has occured or if an upgrade has not been successful.	Computer security incident management Continuity of Operations Crisis Management	
	GP-TM-07: Use protocols and mechanisms able to represent and manage trust and trust relationships. Each communication channel must be trustworthy to a level commensurate with the security dependencies it supports (i.e., how much it is trusted by other components to perform its security functions).	Ecosystem Management	
Strong default security and privacy	GP-TM-08: Enable security by default. Any applicable security features should be enabled by default, and any unused or insecure functionalities should be disabled by default. Strong security controls should be something the consumer has to deliberately disable rather than deliberately enable. GP-TM-09: Establish hard to crack device individual default passwords. Usernames and passwords for IoT devices supplied by the manufacturer are often never changed by the user and are easily cracked, and a hard to crack default password is still a weakness if it is used for more than one device.	Information System Security Governance & Risk Management IT Security Architecture Identity and access management	- IERC European Research Cluster on the Internet of Things - U.S. Department of Homeland Security - Strategic Principles For Securing The Internet Of Things (IoT) - U.S. Federal Communications Commission, Public Safety & Homeland Security Bureau - Article 29 Data Protection Working Party - Opinion 8/2014 on the on Recent Developments on the Internet of Things - Cloud Security Alliance (CSA) - Identity and Access Management for the Internet of Things - IoT Security Foundation (IoTSF) - GSM Association (GSMA) - IoT Security Guidelines - HM Government - National cyber security strategy 2016-2021 - Symantec - Internet Security Threat Report (ISTR)

	SECURITY MEASURES / GOOD PRACTICES	SECURITY DOMAIN	REFERENCES
Data protection and compliance	GP-TM-10: Personal data must be collected and processed fairly and lawfully. The fairness principle specifically requires that personal data should never be collected and processed without the data subject's consent. GP-TM-11: Make sure that personal data is used for the specified purposes for which they were collected, and that any further processing of personal data is compatible and that the data subjects are well informed. GP-TM-12: Minimise the data collected and retained. Many IoT stakeholders only need aggregated data and have no need of the raw data collected by IoT devices. Stakeholders must delete raw data as soon as they have extracted the data required for their data processing. As a principle, deletion should take place at the nearest point of data collection of raw data (e.g. on the same device after processing). GP-TM-13: IoT stakeholders must be compliant with the EU General Data Protection Regulation (GDPR). The complex mesh of stakeholders involved asks for/implies the necessity of a precise allocation of legal responsibilities among them with regard to the processing of the individual's personal data, based on the specificities of their respective interventions. GP-TM-14: Users of IoT products and services must be able to exercise their rights to information, access, erasure, rectification, data portability, restriction of processing, objection to processing, and their right not to be evaluated on the basis of automated processing.	Information System Security Governance & Risk Management Information System Security Governance & Risk Management Information System Security Governance & Risk Management Information System Security Governance & Risk Management Information System Security Governance & Risk Management	- ISO27001 #A18. Compliance - NIST SP 800-53 - AC-21 Information Sharing - AC-22 Publicly Accessible Content - AC-23 Data Mining Protection - OWASP I5. Internet of Things Top Ten - Data Protection Directive 95/46/EC - DG Commissioned Study - Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination - ARTICLE 29 Data Protection Working Party - Opinion 8/2014 on the on Recent Developments on the Internet of Things - EC Alliance for Internet of Things Innovation (AIOTI) - U.S. Federal Communications Commission, Public Safety & Homeland Security Bureau - The President's National Security Telecommunications Advisory Committee - NSTAC Report to the President on the Internet of Things - Cloud Security Alliance (CSA) - Future-proofing the Connected World: 13 Steps to Developing Secure IoT Products - GSM Association (GSMA) - IoT Security Guidelines - Online Trust Alliance (OTA) - IoT Trust Framework and Trust Framework Resource Guide - IETF (Internet Engineering Task Force) - IETF RFC 7452 Architectural Considerations in Smart Object Networking - AIOTI. Digitisation of Industry Policy Recommendations - International Telecommunication Union (ITU) - Unleashing the potential of the Internet of Things - Infineon - Hardware Security for Smart Grid End Point Devices
System safety and reliability	GP-TM-15: Design with system and operational disruption in mind. Build IoT devices to fail safely and securely, so that the failure does not lead to a greater systemic disruption. Have a fail-safe design that specifically ensures that no malfunction can impact the delivery of a commodity (e.g. energy, gas, heat or water), preventing the system from causing unacceptable risk of injury or physical damage, protecting the environment against harm, and avoiding interruption of safety-critical processes. GP-TM-16: Mechanisms for self-diagnosis and self-repair/healing to recover from failure, malfunction or a compromised state.	Physical and environmental security Computer security incident management	- ISO/IEC CD 30141 Internet of Things Reference Architecture (IoT RA) - NIST SP 800-53 - SI-13 Predictable Failure Prevention - Article 29 Data Protection Working Party - Opinion 8/2014 on the on Recent Developments on the Internet of Things - U.S. Department of Homeland Security - Strategic Principles For Securing The Internet Of Things (IoT) - IoT Security Foundation (IoTSF) - Atlantic Council (Brent Scowcroft Center On International Security) - Smart Homes and the Internet of Things - GSM Association (GSMA) - IoT Security Guidelines - BITAG (Broadband Internet Technical Advisory Group) - Internet of Things (IoT) Security and Privacy Recommendations Technical Working Group Report - BSI (Bundesamt für Sicherheit in der Informationstechnik) - Protection Profile for the Gateway of

	SECURITY MEASURES / GOOD PRACTICES	SECURITY DOMAIN	REFERENCES
		Continuity of Operations	a Smart Metering System (Smart Meter Gateway PP), Certification-ID: BSI-CC-PP-0073 - International Electrotechnical Commission (IEC) - IEC White Paper on "IoT 2020: Smart and secure IoT platform" - International Telecommunication Union (ITU) - Unleashing the potential of the Internet of Things - I am the cavalry - Five Star Automotive Cyber Safety Framework - AT&T Cybersecurity Insights - Exploring IoT Security Volume 2 - Symantec - Internet Security Threat Report (ISTR)
	GP-TM-17: Ensure standalone operation - essential features should continue to work with a loss of communications and chronicle negative impacts from compromised devices or cloud-based systems. A loss of communications shall not compromise the integrity of the device, and IoT devices should continue to function if the cloud back-end fails.	Continuity of Operations	
Secure Software / Firmware updates	GP-TM-18: Ensure the device software/firmware, its configuration and its applications have the ability to update Over-The-Air (OTA), that the update server is secure, that the update file is transmitted via a secure connection, that it does not contain sensitive data (e.g. hardcoded credentials), and that it is signed by an authorised trust entity and encrypted using accepted encryption methods, and that the update package has its digital signature, signing certificate and signing certificate chain, verified by the device before the update process begins. Failing to build in OTA update capabilities will leave devices exposed to threats and vulnerabilities for the entirety of their lifetimes	IT Security Administration IT Security Architecture Identity and access management IT security maintenance	- ISO27001 A12. Operations security - NIST SP 800-53 - SI-7 Software, Firmware, And Information Integrity - NIST Framework for Improving Critical Infrastructure Cybersecurity - OWASP I9. Internet of Things Top Ten - U.S. Department of Homeland Security - Strategic Principles For Securing The Internet Of Things (IoT) - Article 29 Data Protection Working Party - Opinion 8/2014 on the on Recent Developments on the Internet of Things - U.S. Federal Communications Commission, Public Safety & Homeland Security Bureau - NOI Fifth Generation Wireless Network and Device Security U.S. Department of Commerce, National Telecommunications and Information Administration, Internet Policy Task Force & Digital Economy Leadership Team - Fostering The Advancement Of

	SECURITY MEASURES / GOOD PRACTICES	SECURITY DOMAIN	REFERENCES
	GP-TM-19: Offer an automatic firmware update mechanism. Devices should be configured to check for the existence of firmware updates at frequent intervals. Automatic firmware updates should be enabled by default. A device may offer an option to disable automatic firmware updates and require authentication for it.	IT Security Architecture	The Internet Of Things - Cloud Security Alliance (CSA) - Future-proofing the Connected World: 13 Steps to Developing Secure IoT Products - IoT Security Foundation (IoTSF) - GSM Association (GSMA) - IoT Security Guidelines - Atlantic Council (Brent Scowcroft Center On International Security) - Smart Homes and the Internet of Things - Online Trust Alliance (OTA) - IoT Trust Framework and Trust Framework Resource Guide - BITAG (Broadband Internet Technical Advisory Group) - Internet of Things (IoT) Security and Privacy Recommendations Technical Working Group Report - ARMOUR (Large-Scale Experiments of IoT Security Trust) - IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework (IIC:PUB:G4:V1.0:PB:20160926, 173 pages) - IETF (Internet Engineering Task Force) - IETF RFC 7452 Architectural Considerations in Smart Object Networking - IETF (Internet Engineering Task Force) - Best Current Practices for Securing Internet of Things (IoT) Devices - Internet Research Task force (IRTF) - State-of-the-Art and Challenges for the Internet of Things Security - BSI (Bundesamt für Sicherheit in der Informationstechnik) - Community Draft SYS 4.4 on General IoT Device (Entwurf SYS.4.4: Allgemeines IoT-Gerät) - BSI (Bundesamt für Sicherheit in der Informationstechnik) - Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP), Certification-ID: BSI-CC-PP-0073 - ISACA - Performing a Security Risk Assessment - AIOTI. Digitisation of Industry Policy Recommendations - International Telecommunication Union (ITU) - Unleashing the potential of the Internet of Things - HM Government - National cyber security strategy 2016-2021 - I am the cavalry - Five Star Automotive Cyber Safety Framework - AT&T Cybersecurity Insights - Exploring IoT Security Volume 2 - Symantec - An Internet of Things Reference Architecture - Symantec - Internet Security Threat Report (ISTR) - Microsoft - Cybersecurity Policy For The Internet Of Things - Infineon - Hardware Security for Smart Grid End Point Devices
	GP-TM-20: Backward compatibility of firmware updates. Automatic firmware updates should not change network protocol interfaces in any way that is incompatible with previous versions. Updates and patches should not modify user-configured preferences, security, and/or privacy settings without user notification. Users should have the ability to approve, authorise or reject updates.	IT Security Architecture	

Authentication	GP-TM-21: Design the authentication and authorisation schemes (unique per device) based on the system-level threat models. Devices should include mechanisms to reliably authenticate their backend services and supporting applications.	Identity and access management	- ISO27001 #A9. Access Control
			- NIST SP 800-30
			- NIST SP 800-53
			  - IA-5 Authenticator Management
			  - AC-7 Unsuccessful Logon Attempts

SECURITY MEASURES / GOOD PRACTICES	SECURITY DOMAIN	REFERENCES
GP-TM-22: Ensure default passwords and even default usernames are changed during the initial setup, and that weak, null or blank passwords are not allowed.	Identity and access management	- AC-14 Permitted Actions Without Identification Or Authentication - NIST Framework for Improving Critical Infrastructure Cybersecurity - OWASP I1, I2, I6. Internet of Things Top Ten - U.S. Federal Communications Commission, Public Safety & Homeland Security Bureau - FCC White Paper, Cybersecurity Risk Reduction - Cloud Security Alliance (CSA) - Identity and Access Management for the Internet of Things - Cloud Security Alliance (CSA) - Future-proofing the Connected World: 13 Steps to Developing Secure IoT Products - Cloud Security Alliance (CSA) - New Security Guidance for Early Adopters of the IoT - IoT Security Foundation (IoTSF) - GSM Association (GSMA) - IoT Security Guidelines - oneM2M - Standards for M2M and the Internet of Things - Online Trust Alliance (OTA) - IoT Trust Framework and Trust Framework Resource Guide - EuroSMART (the voice of the Smart Security Industry) - Internet Of Trust Security And Privacy In The Connected World - IETF (Internet Engineering Task Force) - IETF RFC 7452 Architectural Considerations in Smart Object Networking - World Wide Web Consortium (W3C) - WoT Current Practices - BSI (Bundesamt fur Sicherheit in der Informationstechnik) - Community Draft SYS 4.4 on General IoT Device (Entwurf SYS 4.4: Allgemeines IoT-Gerät) - ISACA - Performing a Security Risk Assessment - International Telecommunication Union (ITU) - Unleashing the potential of the Internet of Things - AT&T Cybersecurity Insights - Exploring IoT Security Volume 2 - Symantec - Internet Security Threat Report (ISTR) - Microsoft - Cybersecurity Policy For The Internet Of Things - Infineon - Hardware Security for Smart Grid End Point Devices
GP-TM-23: Authentication mechanisms must use strong passwords or personal identification numbers (PINs), and should consider using two-factor authentication (2FA) or multi-factor authentication (MFA) like Smartphones, Biometrics, etc., and certificates.	Identity and access management	
GP-TM-24: Authentication credentials including but not limited to user passwords shall be salted, hashed and/or encrypted.	Identity and access management	
GP-TM-25: Protect against 'brute force' and/or other abusive login attempts (such as automated login bots, etc.) by locking or disabling user and device support account(s) after a reasonable number of invalid log in attempts, or y making the user wait a certain amount of time to login again after a failed attempt. This protection should also consider keys stored in devices.	Identity and access management IT Security Administration	
GP-TM-26: Ensure password recovery or reset mechanism is robust and does not supply an attacker with information indicating a valid account. The same applies to key update and recovery mechanisms.	Identity and access management	

	SECURITY MEASURES / GOOD PRACTICES	SECURITY DOMAIN	REFERENCES
Authorisation	GP-TM-27: Limit permissions of the allowed actions for a given system (e.g., the information owner or the database administrator determines who can update a shared file accessed by a group of online users). Implement fine-grained authorisation mechanisms - such as Attribute-Based Access Control (ABAC) or Role-Based Access Control (RBAC)- for executing privileged actions, access to files and directories, applications, etc. Use the Principle of least privilege (POLP): applications must operate at the lowest privilege level possible.	Identity and access management	- ISO27001 #A9. Access Control - NIST SP 800-30 - NIST SP 800-53 - AC-6 Least Privilege - CA-6 Security Authorization - NIST Framework for Improving Critical Infrastructure Cybersecurity - OWASP I1, I2, I6. Internet of Things Top Ten - FTC - Internet of Things: Privacy & Security in a Connected World - IOT-A (Internet of Things Architecture) - Software Assurance Forum for Excellence in Code (SAFECode) - NPO - Call it the Internet of Connected Things: The IoT Security Conundrum - Cloud Security Alliance (CSA) - New Security Guidance for Early Adopters of the IoT - IoT Security Foundation (IoTSF) - GSM Association (GSMA) - IoT Security Guidelines - oneM2M - Standards for M2M and the Internet of Things - IETF (Internet Engineering Task Force) - IETF RFC 7452 Architectural Considerations in Smart Object Networking - IETF (Internet Engineering Task Force) - Best Current Practices for Securing Internet of Things (IoT) Devices - World Wide Web Consortium (W3C) - WoT Current Practices - BSI (Bundesamt für Sicherheit in der Informationstechnik) - Community Draft on Implementation Notes for the module SYS 4.4 on General IoT Device (Entwurf Umsetzungshinweise zum Baustein SYS.4.4 Allgemeines IoT-Gerät) - International Electrotechnical Commission (IEC) - IEC White Paper on "IoT 2020: Smart and secure IoT platform" - ISACA - Performing a Security Risk Assessment - International Telecommunication Union (ITU) - Unleashing the potential of the Internet of Things - Industrial Internet Consortium (IIC)
	GP-TM-28: Device firmware should be designed to isolate privileged code, processes and data from portions of the firmware that do not need access to them, and device hardware should provide isolation concepts to prevent unprivileged from accessing security sensitive code. in order to minimise the potential for compromised code to access those code and/or data.	IT Security Architecture	

	SECURITY MEASURES / GOOD PRACTICES	SECURITY DOMAIN	REFERENCES
Access Control - Physical and Environmental security	GP-TM-29: Data integrity and confidentiality must be enforced by access controls. When the subject requesting access has been authorised to access particular processes, it is necessary to enforce the defined security policy. The effectiveness and the strength of access control depend on the correctness of the access control decisions (e.g., how the security rules are configured) and the strength of access control enforcement (e.g., the design of software or hardware security).	Information System Security Governance & Risk Management Identity and access management	- ISO27001 #A9. Access Control, #A11. Physical and Environmental security - NIST SP 800-30 - NIST SP 800-53 - Physical And Environmental Protection Control Family (PE) - SA-18 Tamper Resistance And Detection - AC-1 Access Control Policy And Procedures - NIST Framework for Improving Critical Infrastructure Cybersecurity - OWASP Access control - OWASP I10. Internet of Things Top Ten - European Commission - Advancing the Internet of Things in Europe - IERC European Research Cluster on the Internet of Things - FTC - Internet of Things: Privacy & Security in a Connected World - oneM2M - Standards for M2M and the Internet of Things - International Electrotechnical Commission (IEC) - IEC White Paper on "IoT 2020: Smart and secure IoT platform" - Cloud Security Alliance (CSA) - Future-proofing the Connected World: 13 Steps to Developing Secure IoT Products - OTA IoT Trust Framework - IoT Security Foundation (IoTSF) - GSM Association (GSMA) - IoT Security Guidelines - Online Trust Alliance (OTA) - IoT Trust Framework and Trust Framework Resource Guide - Trusted Computing Group (TCG) - Guidance for Securing IoT Using TCG Technology Reference Document - BSI (Bundesamt für Sicherheit in der Informationstechnik) - Community Draft on Implementation Notes for the module SYS 4.4 on General IoT Device (Entwurf Umsetzungshinweise zum Baustein SYS.4.4 Allgemeines IoT-Gerät) - BSI (Bundesamt für Sicherheit in der Informationstechnik) - Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP), Certification-ID: BSI-CC-PP-0073 - International Electrotechnical Commission (IEC) - IEC White Paper on "IoT 2020: Smart and secure IoT platform" - International Telecommunication Union (ITU) - Unleashing the potential of the Internet of Things - International Telecommunication Union (ITU) - Unleashing the potential of the Internet of Things - Symantec - An Internet of Things Reference Architecture - Microsoft - Cybersecurity Policy For The Internet Of Things
	GP-TM-30: Ensure a context-based security and privacy that reflects different levels of importance (e.g. emergency crisis, home automation).	Information System Security Governance & Risk Management	
	GP-TM-31: Since some devices, gateways, etc. are required to be managed remotely rather than operated manually in the field, measures for tamper protection and detection are needed. Detection and reaction to hardware tampering should not rely on network connectivity. Hardware tampering means that an attacker has physical control of the device for some period of time. Broadly speaking, hardware tampering might occur at any of the different periods in the life cycle of a device.	Physical and environmental security	
	GP-TM-32: Ensure that the device cannot be easily disassembled and that the data storage medium is encrypted at rest and cannot be easily removed. There should be mechanisms to control device security settings, such as remotely locking or erasing contents of a device if the device has been stolen.	Physical and environmental security	
	GP-TM-33: Ensure that devices only feature the essential physical external ports (such as USB) necessary for them to function and that the test/debug modes are secure, so they cannot be used to maliciously access the devices. In general, lock down physical ports to only trusted connections.	Physical and environmental security	

	SECURITY MEASURES / GOOD PRACTICES	SECURITY DOMAIN	REFERENCES
Cryptography	GP-TM-34: Ensure a proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of data and information (including control messages), in transit and in rest. Ensure the proper selection of standard and strong encryption algorithms and strong keys, and disable insecure protocols. Verify the robustness of the implementation.	IT Security Architecture	- ISO27001 #A10. Cryptography - ISO 27031 7.4.3 - NIST SP 800-30 - NIST SP 800-53 - SC-13 Cryptographic Protection - NIST Framework for Improving Critical Infrastructure Cybersecurity - OWASP Guide to Cryptography - U.S. Federal Communications Commission, Public Safety & Homeland Security Bureau - IOT-A (Internet of Things Architecture) - Software Assurance Forum for Excellence in Code (SAFECode) - NPO - Call it the Internet of Connected Things: The IoT Security Conundrum - Cloud Security Alliance (CSA) - Future-proofing the Connected World: 13 Steps to Developing Secure IoT Products - IoT Security Foundation (IoTSF) - GSM Association (GSMA) - IoT Security Guidelines - oneM2M - Standards for M2M and the Internet of Things - BITAG (Broadband Internet Technical Advisory Group) - Internet of Things (IoT) Security and Privacy Recommendations Technical Working Group Report - EuroSMART (the voice of the Smart Security Industry) - Internet Of Trust Security And Privacy In The Connected World - IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework (IIC:PUB:G4:V1.0:PB:20160926) - IETF (Internet Engineering Task Force) - IETF RFC 7452 Architectural Considerations in Smart Object Networking - IETF (Internet Engineering Task Force) - Best Current Practices for Securing Internet of Things (IoT) Devices - Trusted Computing Group (TCG) - Guidance for Securing IoT Using TCG Technology Reference Document - Internet Research Task force (IRTF) - State-of-the-Art and Challenges for the Internet of Things Security - BSI (Bundesamt für Sicherheit in der Informationstechnik) - Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP), Certification-ID: BSI-CC-PP-0073 - ISACA - Performing a Security Risk Assessment - AIOTI, Digitisation of Industry Policy Recommendations - International Telecommunication Union (ITU) - Unleashing the potential of the Internet of Things - AT&T Cybersecurity Insights - Exploring IoT Security Volume 2 - Symantec - Internet Security Threat Report (ISTR) - Infineon - Hardware Security for Smart Grid End Point Devices
	GP-TM-35: Cryptographic keys must be securely managed. Encryption is only as robust as the ability for any encryption based system to keep the encryption key hidden. Cryptographic key management includes key generation, distribution, storage, and maintenance.	IT Security Architecture	
	GP-TM-36: Build devices to be compatible with lightweight encryption and security techniques (including entities secure identification, secure configuration, etc.) that can, on the one hand, be usable on resource-constrained devices, and, on the other hand, be scalable so to minimise the management effort and maximise their usability.	IT Security Architecture	
	GP-TM-37: Support scalable key management schemes. It has to be considered that tiny sensor nodes cannot provide all security features because they have lots of system limitations. Thus, the sensed data carried over infrastructure networks may not have strong encryption or security protection.	IT Security Architecture	

	SECURITY MEASURES / GOOD PRACTICES	SECURITY DOMAIN	REFERENCES
Secure and trusted communications	GP-TM-38: Guarantee the different security aspects -confidentiality (privacy), integrity, availability and authenticity- of the information in transit on the networks or stored in the IoT application or in the Cloud, using data encryption methods to minimise network threats such as replay, interception, packet sniffing, wiretapping, or eavesdropping.	IT Security Architecture	- ISO27001 #A10. Cryptography - NIST SP 800-30 - NIST SP 800-163 - NIST Framework for Improving Critical Infrastructure Cybersecurity - OWASP I4. Internet of Things Top Ten - FTC - Internet of Things: Privacy & Security in a Connected World - U.S. Department of Homeland Security - Strategic Principles For Securing The Internet Of Things (IoT) - Cloud Security Alliance (CSA) - Future-proofing the Connected World: 13 Steps to Developing Secure IoT Products - IoT Security Foundation (IoTSF) - GSM Association (GSMA) - IoT Security Guidelines - Online Trust Alliance (OTA) - IoT Trust Framework and Trust Framework Resource Guide - BITAG (Broadband Internet Technical Advisory Group) - Internet of Things (IoT) Security and Privacy Recommendations Technical Working Group Report - IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework (IIC:PUB:G4:V1.0:PB:20160926) - World Wide Web Consortium (W3C) - WoT Current Practices - International Electrotechnical Commission (IEC) - IEC White Paper on "IoT 2020: Smart and secure IoT platform" - OpenFog Consortium - The 8 Pillars of the OpenFog Reference Architecture - Trusted Computing Group (TCG) - Guidance for Securing IoT Using TCG Technology Reference Document - Internet Research Task force (IRTF) - State-of-the-Art and Challenges for the Internet of Things Security - International Telecommunication Union (ITU) - Unleashing the potential of the Internet of Things - AT&T Cybersecurity Insights - Exploring IoT Security Volume 2 - Symantec - An Internet of Things Reference Architecture - Symantec - Internet Security Threat Report (ISTR) - Infineon - Hardware Security for Smart Grid End Point Devices
	GP-TM-39: Ensure that communication security is provided using state-of-the-art, standardised security protocols, such as TLS for encryption.	IT Security Architecture	
	GP-TM-40: Ensure credentials are not exposed in internal or external network traffic	IT Security Architecture Identity and access management	
	GP-TM-41: Guarantee data authenticity to enable trustable exchanges (from data emission to data reception - both ways). Data is often stored, cached, and processed by several nodes; not just sent from point A to point B. For these reasons, data should always be signed whenever and wherever the data is captured and stored.	IT Security Architecture	
	GP-TM-42: Do not trust data received and always verify any interconnections. Discover, identify and verify/authenticate the devices connected to the network before trust can be established, and preserve their integrity for trustable solutions and services. For example, a device measures its own integrity as part of boot, but does not validate those measurements - when the device applies to join a network, part of joining involves sending an integrity report for remote validation. If validation fails, the end point is diverted to a remediation network for action.	IT Security Architecture Ecosystem Management	
	GP-TM-43: IoT devices should be restrictive rather than permissive in communicating: When possible, devices should not be reachable via inbound connections by default. IoT devices should not rely on the network firewall alone to restrict communication, as some communication between devices within the home may not traverse the firewall.	IT Security Architecture Ecosystem Management	

	SECURITY MEASURES / GOOD PRACTICES	SECURITY DOMAIN	REFERENCES
Secure Interfaces and network services	GP-TM-44: Make intentional connections. Prevent unauthorised connections to it or other devices the product is connected to, at all levels of the protocols. IoT devices must provide notice and/or request a user confirmation when initially pairing, onboarding, and/or connecting with other devices, platforms or services.	IT Security Architecture	
	GP-TM-45: Disable specific ports and/or network connections for selective connectivity. If necessary, provide users with guidelines to perform this process in the final implementation.	IT Security Architecture	
	GP-TM-46: Rate limiting – controlling the traffic sent or received by a network to reduce the risk of automated attacks.	IT Security Architecture	
	GP-TM-47: Risk Segmentation - Splitting network elements into separate components to help isolate security breaches and minimise overall risk. Networks can be divided into isolated subnetworks to boost performance and improve security.	Information System Security Governance & Risk Management	- ISO27001 #A12. Operations security - NIST SP 800-53 - SC-5 Denial Of Service Protection - NIST Framework for Improving Critical Infrastructure Cybersecurity - OWASP I1, I3, I6. Internet of Things Top Ten - FTC - Internet of Things: Privacy & Security in a Connected World - U.S. Federal Communications Commission, Public Safety & Homeland Security Bureau - NOI Fifth Generation Wireless Network and Device Security - Software Assurance Forum for Excellence in Code (SAFECode) - NPO - Call it the Internet of Connected Things: The IoT Security Conundrum - Cloud Security Alliance (CSA) - Future-proofing the Connected World: 13 Steps to Developing Secure IoT Products - IoT Security Foundation (IoTSF) - GSM Association (GSMA) - IoT Security Guidelines - Online Trust Alliance (OTA) - IoT Trust Framework and Trust Framework Resource Guide - BITAG (Broadband Internet Technical Advisory Group) - Internet of Things (IoT) Security and Privacy Recommendations Technical Working Group Report - IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework (IIC:PUB:G4:V1.0:PB:20160926) - IETF (Internet Engineering Task Force) - IETF RFC 7452 Architectural Considerations in Smart Object Networking - World Wide Web Consortium (W3C) - WoT Current Practices - International Electrotechnical Commission (IEC) - IEC White Paper on "IoT 2020: Smart and secure IoT platform" - Symantec - Internet Security Threat Report (ISTR)
	GP-TM-48: Protocols should be designed to ensure that, if a single device is compromised, it does not affect the whole set, since smart objects are often deployed as sets of identical or almost identical devices.	IT Security Architecture Ecosystem Management	
	GP-TM-49: Avoid provisioning the same secret key in an entire product family, since compromising a single device would be enough to expose the rest of the product family.	Ecosystem Management Identity and access management	
	GP-TM-50: Ensure only necessary ports are exposed and available.	IT Security Architecture	
	GP-TM-51: Implement a DDoS-resistant and Load-Balancing infrastructure to protect the services against DDoS attacks which can affect the device itself or other devices and/or users on the local network or other networks.	IT Security Architecture	

	SECURITY MEASURES / GOOD PRACTICES	SECURITY DOMAIN	REFERENCES
	GP-TM-52: Ensure web interfaces fully encrypt the user session, from the device to the backend services, and that they are not susceptible to XSS, CSRF, SQL injection, etc.	IT Security Architecture	
	GP-TM-53: Avoid security issues when designing error messages. An error message should give/display only the concise information the user needs – it must not expose sensitive information that can be exploited by an attacker, such as an error ID, the version of the web server, etc.	IT Security Administration	
Secure input and output handling	GP-TM-54: Data input validation (ensuring that data is safe prior to use) and output filtering. Security is a concern for decision triggers (malware or general defects). Other possibilities here might be indirect manipulation of input values to the trigger by tampering with or restricting the input values. Reliability is a concern for decision triggers (general defects). Decision triggers could be inconsistent, self-contradictory, and incomplete. Understanding how bad data propagates to affect decision triggers is paramount. Failure to execute decision triggers at time may have undesired consequences.	IT Security Architecture IT Security Administration	- ISO27001 #A12: Operations security - NIST SP 800-53 - SI-10 Information Input Validation - NIST SP 800-183 - 2.5 Primitive #5 (16,19&20): Decision Trigger - OWASP Secure Coding Practices - Input Validation - Software Assurance Forum for Excellence in Code (SAFECode) - NPO - Call it the Internet of Connected Things: The IoT Security Conundrum - IoT Security Foundation (IoTSF) - GSM Association (GSMA) - IoT Security Guidelines - International Electrotechnical Commission (IEC) - IEC White Paper on "IoT 2020: Smart and secure IoT platform" - ISACA - Performing a Security Risk Assessment - Symantec - An Internet of Things Reference Architecture

	SECURITY MEASURES / GOOD PRACTICES	SECURITY DOMAIN	REFERENCES
Logging	GP-TM-55: Implement a logging system that records events relating to user authentication, management of accounts and access rights, modifications to security rules, and the functioning of the system. The logs must also be preserved on durable storage and retrievable via an authenticated connection.	Detection	- ISO27001 #A12. Operations security - NIST SP 800-92 - NIST Framework for Improving Critical Infrastructure Cybersecurity - OWASP Logging Cheat Sheet - Software Assurance Forum for Excellence in Code (SAFECode) - NPO - Call it the Internet of Connected Things: The IoT Security Conundrum - Cloud Security Alliance (CSA) - Future-proofing the Connected World: 13 Steps to Developing Secure IoT Products - Cloud Security Alliance (CSA) - New Security Guidance for Early Adopters of the IoT - GSM Association (GSMA) - IoT Security Guidelines - IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework (IIC:PUB:G4:V1.0:PB:20160926) - Trusted Computing Group (TCG) - Guidance for Securing IoT Using TCG Technology Reference Document - BSI (Bundesamt für Sicherheit in der Informationstechnik) - Community Draft on Implementation Notes for the module SYS 4.4 on General IoT Device (Entwurf Umsetzungshinweise zum Baustein SYS.4.4 Allgemeines IoT-Gerät) - BSI (Bundesamt für Sicherheit in der Informationstechnik) - Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP), Certification-ID: BSI-CC-PP-0073 - ISACA - Performing a Security Risk Assessment - I am the cavalry - Five Star Automotive Cyber Safety Framework - Symantec - An Internet of Things Reference Architecture - Microsoft - Cybersecurity Policy For The Internet Of Things

Monitoring and Auditing	GP-TM-56: Implement regular monitoring to verify the device behaviour, to detect malware and to discover integrity errors.	Detection	- ISO27001 #A12. Operations security
			- ISO 27031 8.1.2
			- NIST SP 800-30
			- NIST SP 800-53
			  - AU-1 Audit And Accountability Policy And Procedures
			  - SI-4 Information System Monitoring
			  - CA-7 Continuous Monitoring
			- OWASP Error Handling, Auditing and Logging
			- FTC - Internet of Things: Privacy & Security in a Connected World
			- Software Assurance Forum for Excellence in Code (SAFECode) - NPO - Call it the Internet of Connected Things: The IoT Security Conundrum

	SECURITY MEASURES / GOOD PRACTICES	SECURITY DOMAIN	REFERENCES
	GP-TM-57: The auditing of security-relevant events and the monitoring and tracking of system abnormalities are key elements in the after-the-fact detection of, and recovery from, security breaches. Conduct periodic audits and reviews of security controls to ensure that the controls are effective. Perform penetration tests at least biannually.	Information System Security Governance & Risk Management IT security maintenance	- Cloud Security Alliance (CSA) - Future-proofing the Connected World: 13 Steps to Developing Secure IoT Products - Cloud Security Alliance (CSA) - New Security Guidance for Early Adopters of the IoT - GSM Association (GSMA) - IoT Security Guidelines - Online Trust Alliance (OTA) - IoT Trust Framework and Trust Framework Resource Guide - IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework (IIC:PUB:G4:V1.0:PB:20160926) - BSI (Bundesamt für Sicherheit in der Informationstechnik) - Community Draft on Implementation Notes for the module SYS 4.4 on General IoT Device (Entwurf Umsetzungshinweise zum Baustein SYS.4.4 Allgemeines IoT-Gerät) - ISACA - Performing a Security Risk Assessment - International Telecommunication Union (ITU) - Unleashing the potential of the Internet of Things - I am the cavalry - Five Star Automotive Cyber Safety Framework Symantec - An Internet of Things Reference Architecture - Symantec - Internet Security Threat Report (ISTR) - Microsoft - Cybersecurity Policy For The Internet Of Things - Infineon - Hardware Security for Smart Grid End Point Devices
End-of-life support	GP-OP-01: Develop an end-of-life strategy for IoT products. Security patches and updates will eventually be discontinued for some IoT devices. Therefore, developers should prepare and communicate a product sunset plan from the initial stages to ensure that manufacturers and consumers are aware of the risks posed to a device beyond its expected expiry date.	IT security maintenance	
	GP-OP-02: Disclose the duration and end-of-life security and patch support (beyond product warranty). Such disclosures should be aligned to the expected lifespan of the device and communicated to the consumer prior to purchase.	IT security maintenance	- U.S. Department of Homeland Security - Strategic Principles For Securing The Internet Of Things (IoT) - FTC - Internet of Things: Privacy & Security in a Connected World - Online Trust Alliance (OTA) - IoT Trust Framework and Trust Framework Resource Guide - BITAG (Broadband Internet Technical Advisory Group) - Internet of Things (IoT) Security and Privacy Recommendations Technical Working Group Report
	GP-OP-03: Monitor the performance and patch known vulnerabilities up until the "end-of-support|" period of of a product's lifecycle. Due to the limited life cycle of many IoT devices, critical, publicly known security or privacy bugs will pose a risk to consumers using outdated devices.	IT security maintenance	

	SECURITY MEASURES / GOOD PRACTICES	SECURITY DOMAIN	REFERENCES
Proven solutions	GP-OP-04: Use proven solutions, i.e. well known communications protocols and cryptographic algorithms, recognized by the scientific community, etc. Certain proprietary solutions, such as custom cryptographic algorithms, should be avoided. Purely proprietary approaches and standards limit interoperability and can severely hamper the potential of the Digital Single Market. Common open standards will help users access new innovative services, especially for SMEs, the public sector and the scientific community. In particular, the portability of applications and data between different providers is essential to avoid lock-in.	IT Security Architecture	- European Commission - ICT Standardisation Priorities for the Digital Single Market - European Commission - Advancing the Internet of Things in Europe - Software Assurance Forum for Excellence in Code (SAFECode) - NPO - Call it the Internet of Connected Things: The IoT Security Conundrum - IIC (Industrial Internet Consortium) - Industrial Internet of Things Volume G4: Security Framework (IIC:PUB:G4:V1.0:PB:20160926) - IETF (Internet Engineering Task Force) - Best Current Practices for Securing Internet of Things (IoT) Devices - OASIS (Organization for the Advancement of Structured Information Standards) - Technical Committees
Management of security vulnerabilities and/or incidents	GP-OP-05: Establish procedures for analysing and handling security incidents. For any incident there should be a response to: a) confirm the nature and extent of the incident; b) take control of the situation; c) contain the incident; and d) communicate with stakeholders Establish management procedures in order to ensure a quick, effective and orderly response to information security incidents.	IT security maintenance	- ISO27001 #A16. Information security incident management - ISO 27031 9.2 and 7.3 - NIST SP 800-30 - NIST SP 800-53 - Incident Response Control Family (IR) - OWASP Top 10 Considerations For Incident Response - U.S. Department of Health and Human Services Food and Drug Administration (FDA) Center for Devices and Radiological Health - Postmarket Management of Cybersecurity in Medical Devices Guidance for Industry and Food and Drug Administration Staff - U.S. Department of Homeland Security - STRATEGIC PRINCIPLES FOR SECURING THE INTERNET of THINGS (IoT) - Online Trust Alliance (OTA) - IoT Trust Framework and Trust Framework Resource Guide - BITAG (Broadband Internet Technical Advisory Group) - Internet of Things (IoT) Security and Privacy Recommendations Technical Working Group Report - IETF (Internet Engineering Task Force) - Best Current Practices for Securing Internet of Things (IoT) Devices - Internet Research Task force (IRTF) - State-of-the-Art and Challenges for the Internet of Things Security
	GP-OP-06: Coordinated disclosure of vulnerabilities, including associated security practices to address identified vulnerabilities. A coordinated disclosure policy should involve developers, manufacturers, and service providers, and include information regarding any vulnerabilities reported to a computer security incident response team (CSIRT).	IT Security Architecture IT security maintenance	
	GP-OP-07: Participate in information sharing platforms to report vulnerabilities and receive timely and critical information about current cyber threats and vulnerabilities from public and private partners. Information sharing is a critical tool in ensuring stakeholders are aware of threats as they arise.	IT security maintenance Computer security incident management	
	GP-OP-08: Create a publicly disclosed mechanism for vulnerability reports. Bug Bounty programs, for example, rely on crowdsourcing methods to identify vulnerabilities that companies' own internal security teams may not catch.	IT security maintenance Computer security incident management	

	SECURITY MEASURES / GOOD PRACTICES	SECURITY DOMAIN	REFERENCES
Human Resource Security Training and Awareness	GP-OP-09: Ensure the personnel practices promote privacy and security - train employees in good privacy and security practices for the secure usage of the systems, recognizing that technological expertise does not necessarily equate to security expertise.	Information System Security Governance & Risk Management	- ISO27001 #A7. Human Resource Security - NIST SP 800-30 - NIST SP 800-50 - NIST SP 800-53 - Awareness And Training Control Family (AT) - NIST Framework for Improving Critical Infrastructure Cybersecurity - FTC - Internet of Things: Privacy & Security in a Connected World - U.S. Federal Communications Commission, Public Safety & Homeland Security Bureau - FCC White Paper, Cybersecurity Risk Reduction
	GP-OP-10: Document and monitor the privacy and security training activities	Information System Security Governance & Risk Management	
	GP-OP-11: Ensure that cybersecurity roles and responsibilities for all workforce are established and introduce personnel assignments in accordance with the specifics of the projects and security engineering needs.	Information System Security Governance & Risk Management	

Third-Party relationships	GP-OP-12: Data processed by a third-party (i.e., if the organisation utilises a cloud email provider), must be protected by a data processing agreement with the third-party. With the transference of data, the responsibility of protecting that data also should be transferred and compliance verified.	Information System Security Governance & Risk Management	- ISO27001 #A18. Compliance
			- NIST SP 800-53
			  - AC-20 Use Of External Information Systems
			  - PS-7 Third-Party Personnel Security
			- NIST Framework for Improving Critical Infrastructure Cybersecurity
			- OWASP Top 10 Privacy Risks Project - P7 Sharing of data with third party
			- OWASP I5. Internet of Things Top Ten
			- Online Trust Alliance (OTA) - IoT Trust Framework and Trust Framework Resource Guide
			- Atlantic Council (Brent Scowcroft Center On International Security) - Smart Homes and the Internet of Things
			- EY - Cybersecurity and the Internet of Things

	GP-OP-13: Only share consumers' personal data with third parties with consumers' affirmative consent, unless required and limited for the use of product features or service operation. Require that third-party service providers are held to the same polices including holding such data in confidence and notification requirements of any data loss/breach incident and/or unauthorised access.	Information System Security Governance & Risk Management	
	GP-OP-14: For IoT hardware manufacturers and IoT software developers it is necessary to adopt cyber supply chain risk management policies and to communicate cyber security requirements to its suppliers and partners.	Information System Security Governance & Risk Management	

Annex B: Security measures and threats mapping

	SECURITY MEASURES / GOOD PRACTICES	THREAT GROUPS
Security by design	GP-PS-01: Consider the security of the whole IoT system in a consistent and holistic approach during its whole lifecycle across all levels of device/application design and development, integrating security throughout the development, manufacture, and deployment	• Nefarious Activity /Abuse
	GP-PS-02: Ensure the ability to integrate different security policies and techniques.	• Nefarious Activity / Abuse
	GP-PS-03: Security must consider the risk posed to human safety	• Nefarious Activity / Abuse
	GP-PS-04: Designing for power conservation should not compromise security	• Nefarious Activity / Abuse
	GP-PS-05: Design architecture by compartments to encapsulate elements in case of attacks.	• Nefarious Activity / Abuse
	GP-PS-06: For IoT hardware manufacturers and IoT software developers it is necessary to implement test plans to verify whether the product performs as it is expected. Penetration tests help to identify malformed input handling, authentication bypass attempts and overall security posture.	• Nefarious Activity / Abuse
	GP-PS-07: For IoT software developers it is important to conduct code review during implementation as it helps to reduce bugs in a final version of a product.	• Nefarious Activity / Abuse
Privacy by design	GP-PS-08: Make privacy an integral part of the system	• Nefarious Activity / Abuse • Damage loss (IT assets)
	GP-PS-09: Perform privacy impact assessments before any new applications are launched	• Nefarious Activity / Abuse • Damage loss (IT assets)
Asset Management	GP-PS-10: Establish and maintain asset management procedures and configuration controls for key network and information systems.	• Nefarious Activity / Abuse • Damage loss (IT assets) • Eavesdropping / Interception / Hijacking • Outages
Risks and Threats Identification and Assessment	GP-PS-11: Identify significant risks using a defence-in-depth approach	• Nefarious Activity /Abuse • Eavesdropping / Interception / Hijacking • Failures / Malfunctions
	GP-PS-12: Identify the intended use and environment of a given IoT device	• Nefarious Activity • Physical attacks • Disasters • Outages
Hardware security	GP-TM-01: Employ a hardware-based immutable root of trust.	
	GP-TM-02: Use hardware that incorporates security features to strengthen the protection and integrity of the device - specialized security chips / coprocessors that integrate security at the transistor level, embedded in the processor, providing, among other things, a trusted storage of device identity and authentication means, protection of keys at rest and in use, and preventing unprivileged from accessing to security sensitive code. Protection against local and physical attacks can be covered via functional security.	• Physical attacks • Disasters • Outages

	SECURITY MEASURES / GOOD PRACTICES	THREAT GROUPS
Trust and Integrity Management	GP-TM-03: The boot process initializes the main hardware components, and starts the operating system. Trust must be established in the boot environment before any trust in any other software or executable program can be claimed.	• Failures / Malfunctions • Nefarious Activity / Abuse • Outages
	GP-TM-04: Sign code cryptographically to ensure it has not been tampered after being signed as safe for the device, and implement run-time protection and secure execution monitoring to be sure malicious attacks do not overwrite code after it is loaded.	• Nefarious Activity / Abuse • Eavesdropping / Interception / Hijacking
	GP-TM-05: Control the installation of software on operational systems, to prevent unauthenticated software and files being loaded onto it.	• Outages • Nefarious Activity / Abuse • Eavesdropping / Interception / Hijacking
	GP-TM-06: Restore Secure State - Enable a system to return to a state that is known to be secure, after a security breach occurs or if an upgrade is not successful.	• Outages • Nefarious Activity / Abuse • Eavesdropping / Interception / Hijacking
	GP-TM-07: Use protocols and mechanisms able to represent and manage trust and trust relationships	• Nefarious Activity / Abuse • Eavesdropping / Interception / Hijacking
Strong default security and privacy	GP-TM-08: Enable security by default. Any applicable security features should be enabled by default, and any unused or insecure functionalities should be disabled by default	• Outages • Nefarious Activity / Abuse • Failures / Malfunctions
	GP-TM-09: Establish hard to crack device individual default passwords	• Outages • Nefarious Activity / Abuse • Failures / Malfunctions
Data protection and compliance	GP-TM-10: Personal data must be collected and processed fairly and lawfully. The fairness principle specifically requires that personal data should never be collected and processed without the user's consent.	• Damage / loss (IT Assets) • Nefarious Activity / Abuse
	GP-TM-11: Make sure that personal data is used for the specified purposes for which they were collected, and that any further processing of personal data is compatible and that the data subjects are well informed.	• Damage / loss (IT Assets) • Nefarious Activity / Abuse
	GP-TM-12: Minimize the data collected and retained.	• Damage / loss (IT Assets)
	GP-TM-13: IoT stakeholders must be compliant with the EU General Data Protection Regulation (GDPR).	• Damage / loss (IT Assets) • Nefarious Activity / Abuse
	GP-TM-14: Users must be able to exercise their rights to information, access, erasure, rectification, data portability, restriction of processing, objection to processing, and their right not to be evaluated on the basis of automated processing.	• Damage / loss (IT Assets) • Nefarious Activity / Abuse
System safety and reliability	GP-TM-15: Design with system and operational disruption in mind, preventing the system from causing unacceptable risk of injury or physical damage	• Outages • Failures / Malfunctions • Disasters
	GP-TM-16: Mechanisms for self-diagnosis and self-repair/healing to recover from failure, malfunction or a compromised state.	• Outages • Failures / Malfunctions

	SECURITY MEASURES / GOOD PRACTICES	THREAT GROUPS
Secure Software / Firmware updates	GP-TM-17: Ensure standalone operation - essential features should continue to work with a loss of communications and chronicle negative impacts from compromised devices or cloud-based systems.	• Outages • Failures / Malfunctions
	GP-TM-18: Ensure that the device software/firmware, its configuration and its applications have the ability to update Over-The-Air (OTA), that the update server is secure, that the update file is transmitted via a secure connection, that it does not contain sensitive data (e.g. hardcoded credentials), and that it is signed by an authorised trust entity and encrypted using accepted encryption methods, and that the update package has its digital signature, signing certificate and signing certificate chain, verified by the device before the update process begins.	• Outages • Failures / Malfunctions • Nefarious Activity / Abuse • Eavesdropping / Interception / Hijacking
	GP-TM-19: Offer an automatic firmware update mechanism.	• Outages • Failures / Malfunctions
	GP-TM-20: Backward compatibility of firmware updates. Automatic firmware updates should not modify user-configured preferences, security, and/or privacy settings without user notification.	• Outages • Failures / Malfunctions
Authentication	GP-TM-21: Design the authentication and authorization schemes (unique per device) based on the system-level threat models.	• Failures / Malfunctions • Nefarious Activity / Abuse • Eavesdropping / Interception / Hijacking
	GP-TM-22: Ensure default passwords and even default usernames are changed during the initial setup, and that weak, null or blank passwords are not allowed.	• Failures / Malfunctions • Nefarious Activity / Abuse • Eavesdropping / Interception / Hijacking
	GP-TM-23: Authentication mechanisms must use strong passwords or personal identification numbers (PINs), and should consider using two-factor authentication (2FA) or multi-factor authentication (MFA) like Smartphones, Biometrics, etc., and certificates.	• Failures / Malfunctions • Nefarious Activity / Abuse • Eavesdropping / Interception / Hijacking
	GP-TM-24: Authentication credentials including but not limited to user passwords shall be salted, hashed and/or encrypted.	• Failures / Malfunctions • Nefarious Activity / Abuse • Eavesdropping / Interception / Hijacking
	GP-TM-25: Protect against 'brute force' and/or other abusive login attempts. This protection should also consider keys stored in devices.	• Failures / Malfunctions • Nefarious Activity / Abuse • Eavesdropping / Interception / Hijacking
	GP-TM-26: Ensure password recovery or reset mechanism is robust and does not supply an attacker with information indicating a valid account. The same applies to key update and recovery mechanisms.	• Failures / Malfunctions • Nefarious Activity / Abuse • Eavesdropping / Interception / Hijacking
Authorization	GP-TM-27: Limit the permissions of actions allowed for a given system by Implementing fine-grained authorisation mechanisms and using the Principle of least privilege (POLP): applications must operate at the lowest privilege level possible.	• Failures / Malfunctions • Nefarious Activity / Abuse • Eavesdropping / Interception / Hijacking
	GP-TM-28: Device firmware should be designed to isolate privileged code and data from portions of the firmware that do not need access to them, and device hardware should provide isolation concepts to prevent unprivileged from accessing security sensitive code.	• Failures / Malfunctions • Nefarious Activity / Abuse • Eavesdropping / Interception / Hijacking

	SECURITY MEASURES / GOOD PRACTICES	THREAT GROUPS
Access Control - Physical and Environmental security	GP-TM-29: Data integrity and confidentiality must be enforced by access controls. When the subject requesting access has been authorised to access particular processes, it is necessary to enforce the defined security policy.	• Physical Attacks • Failures / Malfunctions • Nefarious Activity / Abuse • Eavesdropping / Interception / Hijacking
	GP-TM-30: Ensure a context-based security and privacy that reflects different levels of importance.	• Failures / Malfunctions • Nefarious Activity / Abuse • Eavesdropping / Interception / Hijacking • Damage / Loss (IT Assets)
	GP-TM-31: Measures for tamper protection and detection. Detection and reaction to hardware tampering should not rely on network connectivity.	• Physical attacks • Nefarious Activity / Abuse
	GP-TM-32: Ensure that the device cannot be easily disassembled and that the data storage medium is encrypted at rest and cannot be easily removed.	• Physical attacks • Nefarious Activity / Abuse
	GP-TM-33: Ensure that devices only feature the essential physical external ports (such as USB) necessary for them to function and that the test/debug modes are secure, so they cannot be used to maliciously access the devices. In general, lock down physical ports to only trusted connections.	• Physical attacks • Eavesdropping / Interception / Hijacking • Failures / Malfunctions
Cryptography	GP-TM-34: Ensure a proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of data and information (including control messages), in transit and in rest. Ensure the proper selection of standard and strong encryption algorithms and strong keys, and disable insecure protocols. Verify the robustness of the implementation.	• Nefarious Activity / Abuse • Eavesdropping / Interception / Hijacking
	GP-TM-35: Cryptographic keys must be securely managed.	• Nefarious Activity / Abuse • Eavesdropping / Interception / Hijacking
	GP-TM-36: Build devices to be compatible with lightweight encryption and security techniques.	• Nefarious Activity / Abuse • Eavesdropping / Interception / Hijacking
	GP-TM-37: Support scalable key management schemes.	• Nefarious Activity / Abuse • Eavesdropping / Interception / Hijacking • Failures / Malfunctions
Secure and trusted communications	GP-TM-38: Guarantee the different security aspects -confidentiality (privacy), integrity, availability and authenticity- of the information in transit on the networks or stored in the IoT application or in the Cloud.	• Nefarious Activity / Abuse • Eavesdropping / Interception / Hijacking • Failures / Malfunctions
	GP-TM-39: Ensure that communication security is provided using state-of-the-art, standardised security protocols, such as TLS for encryption.	• Eavesdropping / Interception / Hijacking • Damage / Loss (IT Assets)
	GP-TM-40: Ensure credentials are not exposed in internal or external network traffic.	• Eavesdropping / Interception / Hijacking • Damage / Loss (IT Assets)
	GP-TM-41: Guarantee data authenticity to enable reliable exchanges from data emission to data reception. Data should always be signed whenever and wherever it is captured and stored.	• Nefarious Activity / Abuse • Eavesdropping / Interception / Hijacking

	SECURITY MEASURES / GOOD PRACTICES	THREAT GROUPS
	GP-TM-42: Do not trust data received and always verify any interconnections. Discover, identify and verify/authenticate the devices connected to the network before trust can be established, and preserve their integrity for reliable solutions and services.	• Nefarious Activity / Abuse • Eavesdropping / Interception / Hijacking • Failures / Malfunctions / Outages
	GP-TM-43: IoT devices should be restrictive rather than permissive in communicating.	• Nefarious Activity / Abuse • Eavesdropping / Interception / Hijacking
	GP-TM-44: Make intentional connections. Prevent unauthorised connections to it or other devices the product is connected to, at all levels of the protocols.	• Nefarious Activity / Abuse • Eavesdropping / Interception / Hijacking
	GP-TM-45: Disable specific ports and/or network connections for selective connectivity.	• Nefarious Activity / Abuse • Eavesdropping / Interception / Hijacking
	GP-TM-46: Rate limiting – controlling the traffic sent or received by a network to reduce the risk of automated attacks.	• Nefarious Activity / Abuse • Eavesdropping / Interception / Hijacking
	GP-TM-47: Risk Segmentation. Splitting network elements into separate components to help isolate security breaches and minimise the overall risk.	• Eavesdropping / Interception / Hijacking
	GP-TM-48: Protocols should be designed to ensure that, if a single device is compromised, it does not affect the whole set.	• Eavesdropping / Interception / Hijacking
	GP-TM-49: Avoid provisioning the same secret key in an entire product family, since compromising a single device would be enough to expose the rest of the product family.	• Eavesdropping / Interception / Hijacking
Secure interfaces and network services	GP-TM-50: Ensure only necessary ports are exposed and available.	• Eavesdropping / Interception / Hijacking • Failures / Malfunctions
	GP-TM-51: Implement a DDoS-resistant and Load-Balancing infrastructure.	• Nefarious Activity / Abuse
	GP-TM-52: Ensure web interfaces fully encrypt the user session, from the device to the backend services, and that they are not susceptible to XSS, CSRF, SQL injection, etc.	• Nefarious Activity / Abuse
	GP-TM-53: Avoid security issues when designing error messages.	• Nefarious Activity / Abuse
Secure input and output handling	GP-TM-54: Data input validation (ensuring that data is safe prior to use) and output filtering.	• Nefarious Activity / Abuse • Failures / Malfunctions
Logging	GP-TM-55: Implement a logging system that records events relating to user authentication, management of accounts and access rights, modifications to security rules, and the functioning of the system.	• Damage / Loss (IT Assets)
Monitoring and Auditing	GP-TM-56: Implement regular monitoring to verify the device behaviour, to detect malware and to discover integrity errors.	• Damage / Loss (IT Assets)
	GP-TM-57: Conduct periodic audits and reviews of security controls to ensure that the controls are effective. Perform penetration tests at least biannually.	• Damage / Loss (IT Assets) • Nefarious Activity / Abuse
End-of-life support	GP-OP-01: Develop an end-of-life strategy for IoT products.	• Failures / Malfunctions
	GP-OP-02: Disclose the duration and end-of-life security and patch support (beyond product warranty).	• Failures / Malfunctions

	SECURITY MEASURES / GOOD PRACTICES	THREAT GROUPS
Proven solutions	GP-OP-03: Monitor the performance and patch known vulnerabilities for as long as possible during a product's lifecycle.	• Damage / Loss (IT Assets) • Nefarious Activity / Abuse • Failures / Malfunctions
	GP-OP-04: Use proven solutions, i.e. well known communications protocols and cryptographic algorithms, recognized by the scientific community, etc. Certain proprietary solutions, such as custom cryptographic algorithms, should be avoided	• Damage / Loss (IT Assets) • Nefarious Activity / Abuse
Management of security vulnerabilities and/or incidents	GP-OP-05: Establish procedures for analysing and handling security incidents.	• Failures / Malfunctions • Damage / Loss (IT Assets)
	GP-OP-06: Coordinated disclosure of vulnerabilities.	• Failures / Malfunctions • Damage / Loss (IT Assets) • Nefarious Activity / Abuse • Eavesdropping / Interception / Hijacking • Outages
	GP-OP-07: Participate in information sharing platforms to report vulnerabilities and receive timely and critical information about current cyber threats and vulnerabilities from public and private partners.	• Damage / Loss (IT Assets)
	GP-OP-08: Create a publicly disclosed mechanism for vulnerability reports, e.g. Bug Bounty programs.	• Damage / Loss (IT Assets)
Human Resource Security Training and Awareness	GP-OP-09: Ensure the personnel practices promote privacy and security – train employees in good privacy and security practices.	• Nefarious Activity / Abuse
	GP-OP-10: Document and monitor the privacy and security training activities.	• Nefarious Activity / Abuse
	GP-OP-11: Ensure that cybersecurity roles and responsibilities for all workforce are established and introduce personnel assignments in accordance with the specifics of the projects and security engineering needs.	• Nefarious Activity / Abuse
Third-Party relationships	GP-OP-12: Data processed by a third-party must be protected by a data processing agreement.	• Failures / Malfunctions
	GP-OP-13: Only share consumers' personal data with third parties with consumers' affirmative consent, unless required and limited for the use of product features or service operation.	• Failures / Malfunctions • Damage / Loss (IT Assets)
	GP-OP-14: For IoT hardware manufacturers and IoT software developers it is necessary to adopt cyber supply chain risk management policies and to communicate cyber security requirements to its suppliers and partners.	• Failures / Malfunctions • Damage / Loss (IT Assets) • Nefarious Activity / Abuse • Eavesdropping / Interception / Hijacking • Outages

Annex C: Security standards and references reviewed

This annex lists all the security standards, good practices guides and resources and their corresponding references that have been analysed to develop all of the security measures/good practices listed in chapter 4 and detailed in Annex A. The following table lists said resources, including the ones provided and/or pointed out by the experts interviewed.

AUTHOR	TITLE	REFERENCE
	1. EU Initiatives	
DG CONNECT commissioned study, authored by IDC Italia S.r.L and TXT e-solutions S.p.A.	Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination	https://ec.europa.eu/digital-single-market/en/news/definition-research-and-innovation-policy-leveraging-cloud-computing-and-iot-combination
	Digitising European Industry Reaping the full benefits of a Digital Single Market (COM(2016) 180 final)	https://ec.europa.eu/digital-single-market/en/digitising-european-industry http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1447773803386&uri=CELEX:52015DC0192
	Building A European Data Economy	http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41205 http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41247
European Commission	ICT Standardisation Priorities for the Digital Single Market	https://ec.europa.eu/digital-single-market/en/news/communication-ict-standardisation-priorities-digital-single-market http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=15265
	Advancing the Internet of Things in Europe	http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016SC0110
	H2020	https://ec.europa.eu/programmes/horizon2020/
	EU cybersecurity initiatives	http://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf
Article 29 Data Protection Working Party	Opinion 8/2014 on the on Recent Developments on the Internet of Things	http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf
IERC European Research Cluster on the Internet of Things	IoT Governance, Privacy and Security Issues - IERC Position Paper	http://www.internet-of-things-research.eu/pdf/IERC_Position_Paper_IoT_Governance_Privacy_Security_Final.pdf
	AIOTI WG04: Report on Policy Issues	https://aioti-space.org/wp-content/uploads/2017/03/AIOTIWG04Report2015-Policy-Issues.pdf
EC Alliance for Internet of Things Innovation (AIOTI)	AIOTI WG03: SmartM2M; IoT Standards landscape and future evolutions (October 2016 with the contribution of ETSI)	https://aioti-space.org/wp-content/uploads/2017/03/tr_103375v010101p-Standards-landscape-and-future-evolutions.pdf

AUTHOR	TITLE	REFERENCE
	AIOTI WG03: High Level Architecture (September 2016)	https://aioti-space.org/wp-content/uploads/2017/03/AIOTI-WG3-IoT-High-Level-Architecture-Release_2_1.pdf
	AIOTI Digitisation of Industry Policy Recommendations	https://aioti-space.org/wp-content/uploads/2017/03/AIOTI-Digitisation-of-Ind-policy-doc-Nov-2016.pdf
	AIOTI WG07 Report on Wearables	https://aioti-space.org/wp-content/uploads/2017/03/AIOTIWG07Report2015-Wearables.pdf
	AIOTI WG09 Report on Smart Mobility	https://aioti-space.org/wp-content/uploads/2017/03/AIOTIWG09Report2015-Smart-Mobility.pdf
BEREC (Body of European Regulators for Electronic Communications)	BEREC Report on Enabling the Internet of Things - BoR (16) 39	http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5755-berec-report-on-enabling-the-internet-of-things
ENISA	Cyber Security and Resilience of smart cars	https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars
	Security and Resilience of Smart Home Environments	https://www.enisa.europa.eu/publications/security-resilience-good-practices
	Securing Smart Airports	https://www.enisa.europa.eu/publications/securing-smart-airports
	Cyber security and resilience for Smart Hospitals	https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals
	IoT and Smart Infrastructure efforts	https://www.enisa.europa.eu/iot/
	Ad-hoc & sensor networking for m2m communications - Threat Landscape and good practices guide	https://www.enisa.europa.eu/publications/m2m-communications-threat-landscape
	Threat Landscape and Good Practice Guide for Software Defined Networks/5G	https://www.enisa.europa.eu/publications/sdn-threat-landscape
	ENISA Programming Document	https://www.enisa.europa.eu/publications/corporate/enisa-programming-document-2017-2019
	Communication network dependencies for ICS/SCADA Systems	https://www.enisa.europa.eu/publications/ics-scada-dependencies
2. US Government Initiatives		
National Institute of Standards and Technology (NIST)	NIST.SP.800-27	http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-27.pdf
	NIST.SP.800-30	http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
	NIST.SP.800-50	http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf
	NIST.SP.800-53	http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-53.pdf
	NIST.SP.800-92	http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf

AUTHOR	TITLE	REFERENCE
	NIST.SP.800-160	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf
	NIST SP 800-183 - Network of 'Things'	http://dx.doi.org/10.6028/NIST.SP.800-183
	Framework for Improving Critical Infrastructure Cybersecurity	https://www.nist.gov/document-3766
	NISTIR 7628 Revision 1 - Guidelines for Smart Grid Cyber Security	http://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf
	CPS PWG Cyber-Physical Systems (CPS) Framework	https://pages.nist.gov/cpspwg/
	Securing the Internet of Things	https://www.dhs.gov/securingtheIoT
U.S. Department of Homeland Security (DHS)	Strategic Principles For Securing The Internet Of Things (IoT)	https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL_v2-dg11.pdf
The President's National Security Telecommunications Advisory Committee	NSTAC Report to the President on the Internet of Things	http://www.dhs.gov/sites/default/files/publications/IoT Final Draft Report 11-2014.pdf
U.S. Commission On Enhancing National Cybersecurity	Report On Securing And Growing The Digital Economy	https://www.nist.gov/document/cybersecurity-commission-report-final-postpdf
U.S. Department Of Commerce, National Telecommunications And Information Administration, Internet Policy Task Force & Digital Economy Leadership Team	Fostering The Advancement Of The Internet Of Things	https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf
U.S. Federal Communications Commission, Public Safety & Homeland Security Bureau	FCC White Paper, Cybersecurity Risk Reduction	https://apps.fcc.gov/edocs_public/attachmatch/DOC-343096A1.pdf
	NOI Fifth Generation Wireless Network and Device Security	http://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db1216/DA-16-1282A1.pdf
U.S. Department of Health and Human Services Food and Drug Administration (FDA) Center for Devices and Radiological Health	Postmarket Management of Cybersecurity in Medical Devices Guidance for Industry and Food and Drug Administration Staff	http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm482022.pdf
U.S. Federal Communications Commission, Public Safety & Homeland Security Bureau	Internet of Things, Privacy and Security in a Connected World, FTC Staff report	https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

AUTHOR	TITLE	REFERENCE
	Careful Connections: Building Security in the Internet of Things	https://www.ftc.gov/system/files/documents/plain-language/pdf0199-carefulconnections-buildingsecurityinternetofthings.pdf
United States Government Accountability Office	Internet Of Things Enhanced Assessments and Guidance Are Needed to Address Security Risks in DOD	https://www.gao.gov/assets/690/686203.pdf
National Telecommunications and Information Administration (NTIA)	IoT Security Upgradability and Patching - Existing Standards, Tools and Initiatives Working Group (WG1) Catalog of Existing IoT Security Standards Version 0.01	https://www.ntia.doc.gov/files/ntia/publications/iotsecuritystandardscatalog.pdf
	3. EU-funded projects	
FI-WARE (Future Internet Core Platform)	FI-WARE (Future Internet Core Platform)	http://cordis.europa.eu/project/rcn/99929_en.html https://www.fiware.org/
IOT-A (Internet of Things Architecture)	IOT-A (Internet of Things Architecture)	http://cordis.europa.eu/project/rcn/95713_en.html http://www.meet-iot.eu/iot-a-deliverables.html
Agile-IoT (Adaptive Gateways for diverse muLtiple Environments)	Agile-IoT (Adaptive Gateways for diverse muLtiple Environments)	http://cordis.europa.eu/project/rcn/199853_en.html http://agile-iot.eu/
Eye-O-T (Cyber security system with a high IoT network visibility and fast vulnerability detection for Smart Homes)	Eye-O-T (Cyber security system with a high IoT network visibility and fast vulnerability detection for Smart Homes)	http://cordis.europa.eu/project/rcn/205793_en.html
SCR (Disruptive Cybersecurity SaaS for SMEs and freelance developers)	SCR (Disruptive Cybersecurity SaaS for SMEs and freelance developers)	http://cordis.europa.eu/project/rcn/205788_en.html
TAMPRES (TAMper Resistant Sensor node)	TAMPRES (TAMper Resistant Sensor node)	http://cordis.europa.eu/project/rcn/95511_en.html http://www.tampres.eu/
BUTLER (uBiquitous, secUre inTernet-of-things with Location and contExt-awaReness)	BUTLER (uBiquitous, secUre inTernet-of-things with Location and contExt-awaReness)	http://cordis.europa.eu/project/rcn/101349_en.html
ALMANAC (Reliable Smart Secure Internet Of Things For Smart Cities)	ALMANAC (Reliable Smart Secure Internet Of Things For Smart Cities)	http://cordis.europa.eu/project/rcn/109709_en.html http://www.almanac-project.eu/news.php
RERUM (REliable, Resilient and secUre IoT for sMart city applications)	RERUM (REliable, Resilient and secUre IoT for sMart city applications)	http://cordis.europa.eu/project/rcn/109710_en.html https://ict-rerum.eu/
INSTET (Integral Security Trust Element for the Internet of Things)	INSTET (Integral Security Trust Element for the Internet of Things)	http://cordis.europa.eu/project/rcn/207692_en.html

AUTHOR	TITLE	REFERENCE
BASTION (Leveraging Binary Analysis to Secure the Internet of Things)	BASTION (Leveraging Binary Analysis to Secure the Internet of Things)	http://cordis.europa.eu/project/rcn/193687_en.html
ANASTACIA	ANASTACIA (Advanced Networked Agents for Security and Trust Assessment in CPS/IOT Architectures)	http://cordis.europa.eu/project/rcn/207199_en.html http://www.anastacia-h2020.eu
ARMOUR (Large-Scale Experiments of IoT Security Trust)	ARMOUR (Large-Scale Experiments of IoT Security Trust)	http://cordis.europa.eu/project/rcn/199076_en.html http://www.armour-project.eu/
AdvIOT (Advanced Methods for Analyzing and Improving the Reliability and Security of Novel Environmental-friendly Wireless Devices for Internet of Things)	AdvIOT (Advanced Methods for Analyzing and Improving the Reliability and Security of Novel Environmental-friendly Wireless Devices for Internet of Things)	http://cordis.europa.eu/project/rcn/109385_en.html http://www.adviot.eu/
4. International Organizations/Alliances		
Open Web Application Security Project (OWASP)	OWASP Internet of Things Project	https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project
	OWASP (Draft) IoT Security Guidance	https://www.owasp.org/index.php/IoT_Security_Guidance
	IoT Top Ten 2014 Top Ten	https://www.owasp.org/images/7/71/Internet_of_Things_Top_Ten_2014-OWASP.pdf
Open Geospatial Consortium (OGC) Standard Working Group (SWG) on SensorThings	OGC SensorThings API (former SWE for IoT)	https://github.com/opengeospatial/sensorthings http://www.ogcnetwork.net/IoT http://docs.opengeospatial.org/is/15-078r6/15-078r6.html https://portal.opengeospatial.org/files/15-078r6
International Telecommunication Union (ITU) Global Standards Initiative on Internet of Things (IoT-GSI) – concluded 07/2015 and superseded by Study Group 20 on IoT & its applications incl. smart cities & communities	ITU-T Y.4000/Y.2060 Overview of the Internet of Things	http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060 http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx http://www.itu.int/en/ITU-T/studygroups/2013-2016/20/Pages/default.aspx
	Update of IoT and SC&C Standards Roadmap	http://www.itu.int/en/ITU-T/jca/iot/Documents/deliverables/Free-download-IoT-roadmap.doc
Joint Coordination Activity on Internet of Things and Smart Cities and Communities (JCA-IoT and SC&C)	Unleashing the potential of the Internet of Things	https://www.itu.int/en/publications/Documents/tsb/2016-InternetOfThings/index.html
	ITU-T SG20	http://www.itu.int/en/ITU-T/studygroups/2013-2016/20/Pages/default.aspx
	Call it the Internet of Connected Things: The IoT Security Conundrum	http://www.safecode.org/call-it-the-internet-of-connected-things-the-iot-security-conundrum/

AUTHOR	TITLE	REFERENCE
Software Assurance Forum for Excellence in Code (SAFECode) - NPO		http://www.safecode.org/wp-content/uploads/2014/09/SAFECode_Dev_Practices0211.pdf
Cloud Security Alliance (CSA)	Future-proofing the Connected World: 13 Steps to Developing Secure IoT Products	https://cloudsecurityalliance.org/download/future-proofing-the-connected-world/
	Identity and Access Management for the Internet of Things	https://cloudsecurityalliance.org/download/identity-and-access-management-for-the-iot/
	New Security Guidance for Early Adopters of the IoT	https://cloudsecurityalliance.org/download/new-security-guidance-for-early-adopters-of-the-iot/
IoT Security Foundation (IoTSF)	IoT Security Compliance Framework	https://iotsecurityfoundation.org/wp-content/uploads/2016/12/IoT-Security-Compliance-Framework.pdf
	Connected Consumer Best Practice Guidelines	https://iotsecurityfoundation.org/wp-content/uploads/2016/12/Connected-Consumer-Products.pdf
	Vulnerability Disclosure Best Practice Guidelines	https://iotsecurityfoundation.org/wp-content/uploads/2017/01/Vulnerability-Disclosure.pdf
	Establishing Principles for IoT Security	https://iotsecurityfoundation.org/wp-content/uploads/2015/09/IoTSF-Establishing-Principles-for-IoT-Security-Download.pdf
European Telecommunications Standards Institute (ETSI) Specialist Task Force 505: IoT Standards landscaping and IoT European Large Scale Pilots (LSP) gap analysis	Supporting the IoT	http://www.etsi.org/technologies-clusters/technologies/internet-of-things
	ETSI TR 103 375 SmartM2M; IoT Standards landscape and future evolutions	http://www.etsi.org/deliver/etsi_tr/103300_103399/103375/01.01.01_60/tr_103375v010101p.pdf
	ETSI TR 103 376 SmartM2M; IoT LSP use cases and standards gaps	http://www.etsi.org/deliver/etsi_tr/103300_103399/103376/01.01.01_60/tr_103376v010101p.pdf
	ETSI TR 103 118 Machine-to-Machine communications (M2M) Smart Energy Infrastructures security	http://www.etsi.org/deliver/etsi_tr/103100_103199/103118/01.01.01_60/tr_103118v010101p.pdf
	ETSI TR 103 167 Machine-to-Machine Communications (M2M)	http://www.etsi.org/deliver/etsi_tr/103100_103199/103167/01.01.01_60/tr_103167v010101p.pdf
	ETSI TS 103 267 SmartM2M	http://www.etsi.org/deliver/etsi_ts/103200_103299/103267/01.01.01_60/ts_103267v010101p.pdf
GSM Association (GSMA)	IoT Security Guidelines - Overview Document	http://www.gsma.com/connectedliving/wp-content/uploads/2016/11/CLP.11-v1.1.pdf
	IoT Security Guidelines for Service Ecosystems	http://www.gsma.com/connectedliving/wp-content/uploads/2016/11/CLP.12-v1.1.pdf

AUTHOR	TITLE	REFERENCE
	IoT Security Guidelines for Endpoint Ecosystems	http://www.gsma.com/connectedliving/wp-content/uploads/2016/11/CLP.13-v1.1.pdf
	IoT Security Guidelines for Network Operators	http://www.gsma.com/connectedliving/wp-content/uploads/2016/11/CLP.14-v1.1.pdf
	IoT Security Self-Assessment Process	https://www.gsma.com/iot/wp-content/uploads/2016/09/cl_iot_security_self_assessment_checklist__processes_05_17-1.zip
	GSMA Embedded SIM Remote Provisioning Architecture	http://www.gsma.com/connectedliving/wp-content/uploads/2014/01/1.-GSMA-Embedded-SIM-Remote-Provisioning-Architecture-Version-1.1.pdf
	GSMA Remote Provisioning Architecture for Embedded UICC Technical Specification	http://www.gsma.com/newsroom/wp-content/uploads/SGP.02_v3.1.pdf
	GSMA SAS Standard for Subscription Manager Roles	http://www.gsma.com/aboutus/wp-content/uploads/2015/01/FS08-SAS_SM-Standard-v2_0.pdf
	GSMA SAS Methodology for Subscription Manager Roles	http://www.gsma.com/connectedliving/wp-content/uploads/2014/10/SGP-09-GSMA-SAS-Methodology-for-Subscription-Manager-Roles.pdf
	GSMA Remote Provisioning Architecture for Embedded UICC Test Specification	http://www.gsma.com/newsroom/wp-content/uploads/SGP11_Remote_Provisioning_Architecture_for_Embedded_UICC_Test_Specification_v2_0.pdf
	GSMA IoT Security Guidelines	http://www.gsma.com/iot/gsma-iot-security-guidelines-complete-document-set/ https://www.gsma.com/iot/future-iot-networks/iot-security-guidelines/
Institute of Electrical and Electronics Engineers (IEEE)	IEEE Internet of Things	http://iot.ieee.org/
	IEEE Standards Association - IoT Ecosystem Study	http://standards.ieee.org/innovate/iot/study.html
	Internet Of Things Related Standards	http://standards.ieee.org/innovate/iot/stds.html
	How to Build a Safer Internet of Things	http://spectrum.ieee.org/telecom/security/how-to-build-a-safer-internet-of-things
	Standard for an Architectural Framework for the Internet of Things (IoT)	https://standards.ieee.org/develop/project/2413.html
Online Trust Alliance (OTA)	OTA IoT Trust Framework and Trust Framework Resource Guide	http://otalliance.actonsoftware.com/acton/attachment/6361/f-008d/1/-/-/-/-/IoT Trust Framework.pdf http://otalliance.actonsoftware.com/acton/attachment/6361/f-008e/1/-/-/-/-/IoT Framework Resource Guide.pdf
	IoT Security & Privacy Trust Framework v2.5	https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf
	oneM2M Release 2 specifications	http://www.onem2m.org/technical/published-documents

AUTHOR	TITLE	REFERENCE
oneM2M - Standards for M2M and the Internet of Things	Technical Specification	http://www.onem2m.org/images/files/deliverables/Release2/TR-0008-Security-V2_0_0.pdf
	Technical Report - TR-0008	http://www.onem2m.org/images/files/deliverables/Release2/TR-0012-End-to-End-Security_and_Group_Authentication_V2_0_0.pdf
	Technical Report - TR-0012	http://www.onem2m.org/images/files/deliverables/Release2/TS-0003_Security_Solutions-v2_4_1.pdf
	Technical Report - TR-0016	http://www.onem2m.org/images/files/deliverables/Release2/TR-0016-Authorization_Architecture_and_Access_Control_Policy-V2_0_0.pdf
	Technical Report - TR-0019	http://www.onem2m.org/images/files/deliverables/Release2/TR-0019-Dynamic_Authorization-V2_0_0.pdf
Atlantic Council (Brent Scowcroft Center On International Security)	Smart Homes and the Internet of Things (issue brief)	http://www.atlanticcouncil.org/publications/issue-briefs/smart-homes-and-the-internet-of-things
BITAG (Broadband Internet Technical Advisory Group)	Internet of Things (IoT) Security and Privacy Recommendations Technical Working Group Report	https://www.bitag.org/report-internet-of-things-security-privacy-recommendations.php
EuroSMART (the voice of the Smart Security Industry)	Internet Of Trust Security And Privacy In The Connected World	http://www.eurosmart.com/news-publications/99-policy-papers/245-eurosmart-internet-of-trust-security-and-privacy-in-the-connected-world.html
ICIT (Institute for Critical Infrastructure Technology)	Rise of the Machines: The Dyn Attack Was Just a Practice Run	http://icitech.org/icit-publication-the-rise-of-the-machines-the-dyn-attack-was-just-a-practice-run/
IIC (Industrial Internet Consortium)	Industrial Internet of Things Volume G4 Security Framework (IIC:PUB:G4:V1.0:PB:20160926)	http://www.iiconsortium.org/IISF.htm
IoT-A (IoT Alliance)	Internet of Things Security Guideline IoT Reference Architecture	http://www.iot.org.au/s/IoTAA-Security-Guideline-V10-8242.pdf
Internet Research Task force (IRTF)	IETF RFC 7452 Architectural Considerations in Smart Object Networking	https://tools.ietf.org/html/rfc7452
	Best Current Practices for Securing Internet of Things (IoT) Devices	https://tools.ietf.org/pdf/draft-moore-iot-security-bcp-00.pdf
Internet Research Task force (IRTF)	State-of-the-Art and Challenges for the Internet of Things Security	https://tools.ietf.org/pdf/draft-irtf-t2trg-iot-seccons-04.pdf
	Secure IoT Bootstrapping: A Survey	https://tools.ietf.org/pdf/draft-sarikaya-t2trg-sbootstrapping-03.pdf
Thing to Thing Research Group (T2TRG)	Survey on Thing Secure Bootstrapping	https://tools.ietf.org/pdf/draft-liu-t2trg-bootstrapping-survey-00.pdf
	IoT architecture based on Virtual thing environment for security	https://tools.ietf.org/pdf/draft-yang-t2trg-virtualthing-00.pdf
	The Open Trust Protocol (OTrP)	https://www.ietf.org/id/draft-pei-opentrustprotocol-04.txt

AUTHOR	TITLE	REFERENCE
Internet Engineering Task Force (IETF)	State-of-the-Art and Challenges for the Internet of Things Security	https://tools.ietf.org/html/draft-irtf-t2trg-iot-seccons-04
	Best Current Practices for Securing Internet of Things (IoT) Devices	https://datatracker.ietf.org/doc/draft-moore-iot-security-bcp/
	The Internet Engineering Task Force (IETF®)56	https://www.ietf.org/proceedings/56/
	RFC 7925	https://tools.ietf.org/html/rfc7925
	Datagram Transport Layer Security Version 1.2	https://tools.ietf.org/html/rfc6347
	The Constrained Application Protocol (CoAP)	https://tools.ietf.org/html/rfc7252
IAB (Internet Architecture Board)	IAB Workshop on IoT Software Updates	https://www.iab.org/activities/workshops/iotsu/
World Wide Web Consortium (W3C)	Web of Things (WoT) Architecture	http://w3c.github.io/wot/architecture/wot-architecture.html
	WoT Current Practices	http://w3c.github.io/wot/current-practices/wot-practices.html
Trusted Computing Group (TCG)	Guidance for Securing IoT Using TCG Technology Reference Document	https://trustedcomputinggroup.org/guidance-securing-iot-using-tcg-technology-reference-document/
OpenFog Consortium	OpenFog Reference Architecture for Fog Computing	https://www.openfogconsortium.org/wp-content/uploads/OpenFog-Reference-Architecture-Executive-Summary.pdf
	The 8 Pillars of the OpenFog Reference Architecture	https://www.openfogconsortium.org/wp-content/uploads/OpenFog-Pillars-10-page-summary.pdf
OASIS (Organization for the Advancement of Structured Information Standards)	Technical Committees	https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=mqtt https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=amqp https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=obix
Open Mobile Alliance for a Connected World (OMA)	OMA Device Management Security	http://www.openmobilealliance.org/release/DM/V1_3-20160524-A/OMA-TS-DM_Security-V1_3-20160524-A.pdf
	OMA LightweightM2M V1.0	http://www.openmobilealliance.org/release/LightweightM2M/V1_0-20170208-A/
BSI (Bundesamt für Sicherheit in der Informationstechnik)	Community Draft SYS 4.4 on General IoT Device (Entwurf SYS.4.4: Allgemeines IoT-Gerät)	https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-Grundschutz-Modernisierung/BS_IoT.html?nn=7712584
BMWi (Bundesministerium für Wirtschaft und Energie)	Community Draft on Implementation Notes for the module SYS 4.4 on General IoT Device (Entwurf Umsetzungshinweise zum Baustein SYS.4.4 Allgemeines IoT-Gerät)	https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-Grundschutz-Modernisierung/UH_IoT.html?nn=7712584

AUTHOR	TITLE	REFERENCE
	Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP), Certification-ID: BSI-CC-PP-0073	https://www.commoncriteriaportal.org/files/ppfiles/pp0073b_pdf.pdf
IP for Smart Objects (IPSO) Alliance	IPSO Security, Privacy & Identity (SPI) - Working Group Charter	http://www.ipso-alliance.org/wp-content/uploads/2015/12/IPSO_SPI-Charter.pdf
	Enabling IoT Devices' Hardware and Software Interoperability (IPSO Alliance Technical Overview)	http://www.ipso-alliance.org/wp-content/uploads/2016/11/2016-11-08_IPSO_Overview.pdf
Open Connectivity Foundation (formerly OIC-Open Interconnect Consortium)	OIC Security Specification v1.1.1	https://openconnectivity.org/specs/OIC_Security_Specification_v1.1.1.pdf
	IEC White Paper on "IoT 2020: Smart and secure IoT platform"	http://www.iec.ch/whitepaper/pdf/iecWP-IoT2020-LR.pdf
International Electrotechnical Commission (IEC)	IEC/TR 62443-2-3, "Security for industrial automation and control systems - Part 2-3: Patch management in the IACS environment."	https://webstore.iec.ch/publication/22811
	5. Other references	
	ISO 27001	https://www.iso.org/standard/54534.html
	ISO 27002	https://www.iso.org/standard/54533.html
	ISO 27031	https://www.iso.org/standard/44374.html
International Organization for Standardization (ISO)	ISO/IEC JTC 1 SC 27 and SC41	https://www.iso.org/committee/45306.html https://www.iso.org/committee/6483279.html
	ISO/IEC CD 30141	https://www.iso.org/standard/65695.html
	ISO/IEC 15408 series	https://www.iso.org/standard/50341.html
	Internet of Things Reference Architecture (IoT RA)	http://isotc.iso.org/livelink/livelink/open/jtc1wg10 https://www.w3.org/WoT/IG/wiki/images/9/9a/10N0536_CD_text_of_ISO_IEC_30141.pdf
ISACA	Performing a Security Risk Assessment	https://www.isaca.org/journal/archives/2010/volume-1/pages/performing-a-security-risk-assessment1.aspx
	IoT Journal Vol.3	https://www.isaca.org/Journal/archives/2017/Volume-3/Pages/default.aspx
Symantec	An Internet of Things Reference Architecture	https://www.symantec.com/content/dam/symantec/docs/white-papers/iot-security-reference-architecture-en.pdf

AUTHOR	TITLE	REFERENCE
	Internet Security Threat Report (ISTR) Volume 22	https://www.symantec.com/security-center/threat-report https://resource.elq.symantec.com/LP=3980?cid=70138000001BjppAAC&mc=202671&ot=wp&tt=sw&inid=symc_threat-report_regular_to_leadgen_form_LP-3980_ISTR22-report-main
CableLabs	Data-Over-Cable Service Interface Specifications DOCSIS® 3.1 Security Specification	https://apps.cablelabs.com/specification/CM-SP-SECv3.1
RISE SICS	How to secure the Internet of Things?	https://www.sics.se/sites/default/files/pub/lund-hannestschofenig_final.pdf
HM Government	National cyber security strategy 2016-2021	https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf
AT&T Cybersecurity Insights	Exploring IoT Security Volume 2	https://www.business.att.com/cybersecurity/docs/exploringiotsecurity.pdf
I am the cavalry	Five Star Automotive Cyber Safety Framework	https://www.iamthecavalry.org/wp-content/uploads/2014/08/Five-Star-Automotive-Cyber-Safety-February-2015.pdf
Microsoft - Cybersecurity Policy For The Internet Of Things	Cybersecurity Policy For The Internet Of Things	https://mscorpmedia.azureedge.net/mscorpmedia/2017/05/IoT_WhitePaper_5_15_17.pdf
Infineon	Hardware Security for Smart Grid End Point Devices	https://www.nrel.gov/esif/assets/pdfs/hardware_security_smart_grid.pdf
International Society of Automation (ISA)	Industrial Automation and Control System Security	http://isa99.isa.org/ISA99%20Wiki/Home.aspx
	IEC 62443: Industrial Network And System Security	https://www.isa.org/pdfs/autowest/phinneydone/
Object Management Group	DDS-Security	http://www.omg.org/spec/DDS-SECURITY/1.0/
Thread Group	Thread 1.1 Specification	http://threadgroup.org/ThreadSpec
Cloud Standards Customer Council (CSCC)	Cloud Customer Architecture for IoT	http://www.cloud-council.org/deliverables/cloud-customer-architecture-for-iot.htm
Industrie 4.0	The Internet Of Things – What Is It?	https://industrie4.0.gtai.de/INDUSTRIE40/Navigation/EN/Topics/The-internet-of-things/internet-of-things-what-is-it.html
	Embedded Systems And Networks	https://industrie4.0.gtai.de/INDUSTRIE40/Navigation/EN/Topics/The-internet-of-things/embedded-systems-and-networks.html
	Digital Infrastructure	https://industrie4.0.gtai.de/INDUSTRIE40/Navigation/EN/Topics/Smart-service-world/digital-infrastructure.html
	Disruptive Business Models	https://industrie4.0.gtai.de/INDUSTRIE40/Navigation/EN/Topics/Smart-service-world/disruptive-business-models.html
	Industrie 4.0 – What Is It?	https://industrie4.0.gtai.de/INDUSTRIE40/Navigation/EN/Topics/Industrie-40/what-is-it.html
North American Electric Reliability Corp.	State of Reliability 2017	http://www.nerc.com/pa/rapa/pa/performance%20analysis%20dl/sor_2017_master_20170613.pdf

AUTHOR	TITLE	REFERENCE
Broadband Forum	User Services Platform (TR-369)	https://broadbandforum.github.io/usp/
OAuth	OAuth 2.0	https://oauth.net/
OPC Foundation	Unified Architecture	https://opcfoundation.org/about/opc-technologies/opc-ua/
Bruce Schneier	Schneier on Security	https://www.schneier.com/blog/archives/2017/02/security_and_pr.html
Smart Grid Interoperability Panel (SGIP)	Case studies and use cases	http://www.sgip.org/case-studies-and-use-cases/
Underwriters Laboratories (UL)	The Internet of Things (IoT)	http://industries.ul.com/blog/the-internet-of-things-iot
	UL Cybersecurity Assurance Program	http://industries.ul.com/cybersecurity
3rd Generation Partnership Project (3GPP)	LTE to 5G: Cellular and Broadband Innovation - Internet of Things poised for massive adoption with new Cellular IoT capabilities in 3GPP Release 13	http://www.3gpp.org/technologies/presentations-white-papers
The Digital Standard	The Digital Standard	http://thedigitalstandard.org/
Internet of Things Consortium	Internet of Things Consortium	http://iofthings.org/
Other	Philips pushes lightbulb firmware update that locks out third-party bulbs	http://boingboing.net/2015/12/14/philips-pushes-lightbulb-firmw.html
	Industrial Internet Consortium Develops an IoT Security Framework	https://securityintelligence.com/news/industrial-internet-consortium-develops-iot-security-framework/
	IoT Security Resources	http://blog.mobilephonesecurity.org/2016/11/iot-security-resources.html

Annex D: Description of indicative IoT security incidents

SECURITY INCIDENT	DATE	DESCRIPTION
Puerto Rican Smart Meters hacked	2009	At some point in 2009, the Puerto Rican Electric Power Authority (PREPA) suffered a series of power theft incidents related to its smart meter deployment. The attack required physical access to the smart meters, and it is believed that former employees of the meter manufacturer were altering the smart meters to reduce power bills[81].
Foscam IP baby-cam hijacked	August 10, 2013	On April 11, 2013, a vulnerability in Foscam wireless cameras was disclosed by security researchers in a presentation titled "To watch or to be watched: Turning your surveillance camera against you". Later, on August 10, an attacker gained control of one of those cameras in Houston, Texas, which was being used as a baby-cam. The attacker was able to see, hear and speak through the camera[82].
Target data breach	November 15 - December 15, 2013	The intrusion into Target's systems was traced back to network credentials stolen from a third-party IoT HVAC vendor. It is believed that Target allowed that HVAC vendor remote access to its network in order to report fluctuations in store temperature which might have affected how long a customer stayed within a given store. Nevertheless, it remains a mystery why the point of sale system was not segmented from the rest of the Target network[83]. The intrusion took place on November 15, 2013, and one month later, the data breach had already resulted in the theft of 40 million credit and debit card accounts[84].
BMW's Connected Drive vulnerable (demonstration)	January 2015	A security vulnerability in BMW's Connected Drive system allowed researchers to unlock the vehicles affected without the car keys. The attack took advantage of a feature that allows drivers who have been locked out of their vehicles to request the remote unlocking of their car from a BMW assistance line. The researchers were able to impersonate BMW servers and send, over the public cellular network, remote unlocking instructions to vehicles[85]. The software patch for the 2.2 million cars equipped with Connected Drive adds HTTPS encryption to the connection from BMW to the car and ensures that the car only accepts connections from a server with the correct security certificate[86].
Jeep car remotely hijacked (demonstration)	July 21, 2015	Charlie Miller and Chris Valasek developed a zero-day exploit that targets Jeep Cherokees, giving an attacker, who may be miles away, complete control -via the Internet- of thousands of vulnerable vehicles. The attack is performed by sending commands through the Jeep's entertainment system to its dashboard functions, steering, brakes, and transmission[87].

[81] See https://www.metering.com/puerto-rico-smart-meters-believed-to-have-been-hacked-and-such-hacks-likely-to-spread/
[82] See https://www.forbes.com/sites/kashmirhill/2013/08/13/how-a-creep-hacked-a-baby-monitor-to-say-lewd-things-to-a-2-year-old/
[83] See https://www.mocana.com/blog/2014/02/05/iot-hack-connected-target-breach
[84] See http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/
[85] AJ Trainor, Amalia Safer, Lily Houghton, «BMW ConnectedDrive Vulnerability». See https://www.cs.bu.edu/~goldbe/teaching/HW55815/presos/bmw.pdf
[86] See https://www.mocana.com/blog/2014/02/05/iot-hack-connected-target-breach
[87] See https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

SECURITY INCIDENT	DATE	DESCRIPTION
TrackingPoint's smart sniper rifle hack (demonstration)	July 29, 2015	Security researchers Runa Sandvik and Michael Auger have developed a set of techniques that could allow an attacker to exploit vulnerabilities in the software of a US$13,000 TrackingPoint self-aiming rifle via its Wi-Fi connection. The attacker could then compromise the scope's targeting system, preventing the gun from firing or even causing it to miss the intended target, hitting another one[88].
VTech Toymaker data breach	November 8, 2015	A cyber-attack on digital toymaker VTech Holdings exposed the data of 6.4 million children and 4.9 million adults. The personal information stolen was not encrypted, and it included names, email addresses, passwords, secret questions and answers for password retrieval, IP addresses, postal addresses, download histories, chat logs, and children's names, photos, genders and birth dates[89].
Mirai - DDoS on OVH hosting provider	September 19, 2016	Mirai gathered a botnet made up of more than one million hacked IoT devices, mostly DVRs and CCTV cameras, which were infected through their Telnet port. The French hosting company OVH is believed to be the first to have suffered a DDoS attack coming from the Mirai botnet, which was reported to have peaked at 1 Tbps, one of the largest recorded in history in terms of volume[90].
Mirai - DDoS on "Krebs on Security" website	September 20, 2016	Just a day after the attack against OVH, the Mirai botnet conducts a DDoS attack on "Krebs on Security" website that surpassed 620 Gbps of traffic, making it also one of the largest recorded in history in terms of volume[90].
Hajime	October 15, 2016	Hajime is a "vigilante" spreading IoT worm that, like Mirai, takes advantage of devices with default usernames and passwords to gain control over them, via their Telnet ports. Its purpose is believed to be fighting the Mirai botnet for control over IoT products – once a device is infected, Hajime blocks access to ports 23 (Telnet), 7547, 5555, and 5358, which are common entry points for the rival Mirai worm and other threats[91]. At the moment, the Hajime worm is not doing anything malign – it just displays the following message: "Just a white hat, securing some systems"[92].
Mirai - DDoS on Dyn DNS provider	October 21, 2016	Some of Mirai's targets were cloud-related services, such as DNS provider Dyn, which suffered a DDoS attack that affected several high-profile websites, including Amazon, Netflix, PayPal and Spotify. Unconfirmed reports say the peak of the attack reached around 1.2 Tbps[93].
DDoS on building blocks' central heating system	November 3, 2016	In Finland, a DDoS Attack took down the heating systems of at least two housing blocks in the city of Lappeenranta, leaving their residents without heating in sub-zero temperatures for more than a week[94].

[88] See https://www.wired.com/2015/07/hackers-can-disable-sniper-rifleor-change-target/
[89] See http://www.cnbc.com/2015/12/02/vtech-hack-data-of-64m-kids-exposed.html
[90] See https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf
[91] See https://blog.radware.com/security/2017/04/hajime-futureproof-botnet/
[92] See https://www.symantec.com/connect/blogs/hajime-worm-battles-mirai-control-internet-things
[93] See https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/
[94] See http://thehackernews.com/2016/11/heating-system-hacked.html

SECURITY INCIDENT	DATE	DESCRIPTION
Mirai - DDoS on Deutsche Telekom network	November 27, 2016	Mirai botnet targets Deutsche Telekom routers, affecting more than 900,000 customers[95].
Cloudpets' DB held for ransom	December 25, 2016 - January 8, 2017	Cloudpets is a company that sells Internet-connected teddy bears, allowing kids to communicate with their far-away parents. Cloudpets customers' data were left for two weeks in a publicly available database without password or firewall protection. More than 820,000 customer credentials were exposed, as well as two million message recordings. In addition, the database was also held for ransom[96].
Romantik Seehotel Jägerwirt	January 25, 2017	The Romantik Seehotel Jägerwirt, a 4-star hotel in the Austrian Alps, had its digital key system breached and held for ransom. The attackers managed to take down the entire key system – the guests could no longer get into their hotel rooms and new key cards could not be programmed. The hotel has admitted they had to pay a ransom worth thousands of Bitcoin to the cybercriminals, who restored the key system and the computers as soon as they received the payment. The attackers left a backdoor in the system to exploit it in the near future, but when they tried again, the hotel had already bolstered its security[97].
Cloudpets and "Meine Freundin Cayla" - insecure Bluetooth	February 17 - 27, 2017	Apart from Cloudpets' customer database being completely insecure, it turns out Cloudpets' teddy bears were themselves insecure too. CloudPets' toys did not use any standard Bluetooth security features, such as pairing encryption with their owner's smartphone app, so anyone within range (10 meters with a normal smartphone) could just connect to it and send and receive commands and data – e.g. uploading a message to the toy, or silently triggering the toy's recording functionality and later downloading the audio the toy has recorded. In other words, the teddy bears could be turned into remote surveillance devices, used to harass toddlers like some insecure baby monitors have in the past, such as the Foscam IP baby-cam case[98]. Just one week before, the German government banned the Internet-connected "Meine Freundin Cayla" doll for the same reasons that concern Cloudpets' toys – it had vulnerabilities that could be exploited by an attacker to remotely spy on children[99].
BrickerBot	March 20, 2017	BrickerBot is a bot that permanently incapacitates –Permanent DoS (PDoS)– poorly secured IoT devices, leaving them in a "bricked" state before they can be conscripted into Internet-crippling denial-of-service armies. The latest version BrickerBot.3 appeared April 20, one month after BrickerBot.1 first surfaced[100,101].

[95] See https://www.engadget.com/2016/11/29/mirai-botnet-targets-deutsche-telekom-routers-in-global-cyberatt/
[96] See https://motherboard.vice.com/en_us/article/internet-of-things-teddy-bear-leaked-2-million-parent-and-kids-message-recordings
[97] See https://www.thelocal.at/20170128/hotel-ransomed-by-hackers-as-guests-locked-in-rooms
[98] See https://motherboard.vice.com/en_us/article/how-this-internet-of-things-teddy-bear-can-be-remotely-turned-into-a-spy-device
[99] See https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/DE/2017/14012017_cayla.html
[100] See https://arstechnica.com/security/2017/04/brickerbot-the-permanent-denial-of-service-botnet-is-back-with-a-vengeance/
[101] See https://ics-cert.us-cert.gov/alerts/ICS-ALERT-17-102-01A

ENISA

European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office

1 Vasilissis Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

TP-05-17-148-EN-N

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-236-3
DOI: 10.2824/03228

Cybersecurity

Implementatierichtlijn

Objecten – RWS

Uitgegeven door	PRIA / CIV-IRN Security Center
Steller	Turabi Yildirim
Datum	02 december 2013
Status	Definitief
Vertrouwelijkheid	RWS Ongeclassificeerd
Informatieklasse	RWS-O
Versie	1.01

Inhoudsopgave

1 Inleiding 3

1.1 Baseline Informatiebeveiliging RWS 3

1.2 Cybersecurity Implementatierichtlijn Objecten - RWS 3

1.3 Instructie voor toepassing 6

1.4 Structuur 7

2 Generieke beheersdoelen en beheersmaatregelen 8

3 Specifieke maatregelpakketten 22

3.1 Maatregelen Fysieke toegangsbeveiliging IA-gerelateerde ruimten 23

3.2 Maatregelen Logische toegang 25

3.3 Maatregelen Beveiligingsincidenten en incident Response Plan 27

3.4 Maatregelen Netwerkkoppelingen 29

3.5 Maatregelen bescherming tegen malware, hardening en patching 31

3.6 Maatregelen Logging en Monitoring 33

3.7 Maatregelen Bewustwording en Training 35

3.8 Maatregelen gecontroleerd wijzigen 39

3.9 Maatregelen beheer en onderhoud 41

3.10 Maatregelen Back-ups 45

Bijlage A: Wachtwoord Richtlijn 47

Bijlage B: Factsheet Wachtwoorden 49

1 Inleiding

Cybersecurity is er op gericht om uitval, verstoring en misbruik van ICT-systemen te voorkomen en daarmee bij te dragen aan de beschikbaarheid, de integriteit, de vertrouwelijkheid en de controleerbaarheid van de informatievoorziening (IV) en de Industriele Automatisering (IA) van RWS.

1.1 Baseline Informatiebeveiliging RWS

De Baseline Informatiebeveiliging Rijksdienst (BIR) schrijft het basisniveau voor informatiebeveiliging bij de Rijksoverheid voor. De BIR biedt één normenkader voor de beveiliging van de Informatievoorziening (IV) van het Rijk. Dit maakt het mogelijk om veilig samen te werken en onderling gegevens uit te wisselen. De BIR zorgt voor één heldere set afspraken zodat een bedrijfsonderdeel weet dat de gegevens die verstuurd worden naar een ander onderdeel van de rijksdienst op het juiste beveiligingsniveau (vertrouwelijkheid, integriteit en beschikbaarheid) worden behandeld.

In het beveiligingsbeleid van IenM wordt de Baseline Informatiebeveiliging Rijksdienst (BIR) gehanteerd als het te volgen Tactisch Normen Kader voor de beveiliging van de IV. De BIR is daarmee ook kaderstellend voor RWS. De BIR hoofdstukken en paragrafen worden integraal aangehouden voor de vertaalslag en invulling van de beveiliging van de IV van RWS. De Baseline Informatiebeveiliging RWS (BIR RWS) is het resultaat van de vertaalslag en invulling van de BIR voor de beveiliging van de IV van RWS.

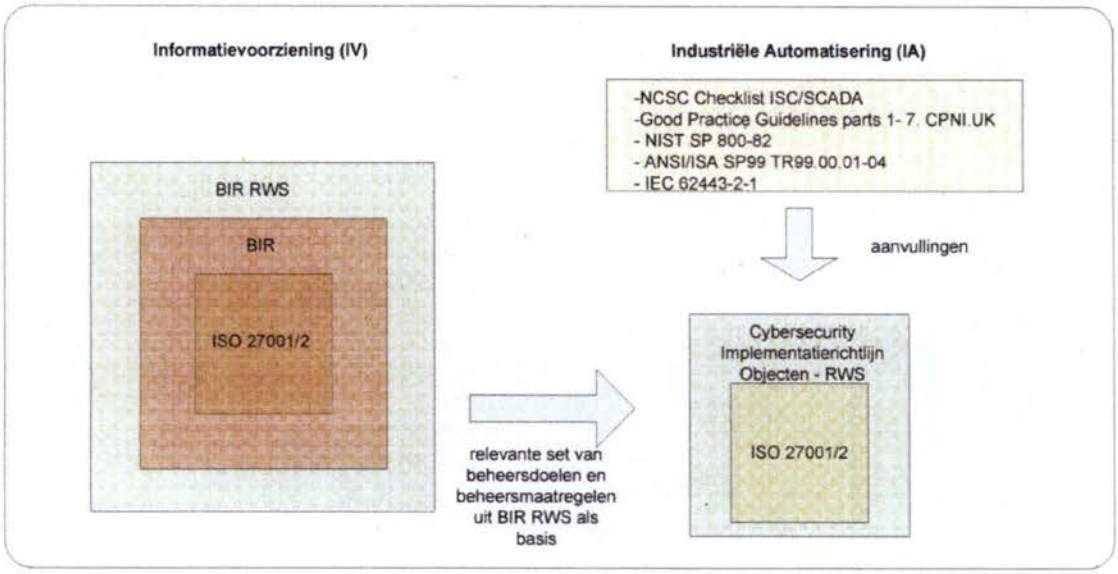
1.2 Cybersecurity Implementatierichtlijn Objecten - RWS

RWS heeft veel systemen en omgevingen die los staan van de centrale kantooromgeving. Dit zijn veelal operationele systemen voor het bedienen van objecten, het communiceren met vaarweggebruikers of het modelleren van waterkwaliteit en -kwantiteit in verschillende stroomgebieden. Deze systemen hebben vaak een ander dreigingprofiel dan de IV in de kantooromgeving en staan daar vaak ook los van zoals de Industriële Automatisering (IA) met veel ICS/SCADA-toepassingen.

Hiernaast heeft RWS ook op grote schaal te maken met uitbesteding van werk en het voeren van regie op de uitbestede taken aan marktpartijen. Bij deze samenwerking en uitvoering van werkzaamheden door marktpartijen speelt (IA) en inzet van ICS/SCADA-systemen een grote rol. De BIR (RWS) is voor de IA omgeving en de ICS/SCADA toepassingen niet volledig dekkend en op onderdelen te algemeen van aard waardoor bedrijfsrisico's blijven bestaan voor RWS.

Het Beveiligingsbeleid van IenM geeft aan dat de dienstonderdelen daar waar nodig aanvullingen dienen te plegen op de BIR om de beveiligingsrisico's in het eigen werkveld te mitigeren. De uitvoeringstaken van RWS waarbij de inzet nodig is van IA en vele ICS/SCADA-systemen, zijn van dien aard dat extra eisen en maatregelen naast de BIR (RWS) noodzakelijk zijn.

Afhankelijk van het domein, het karakter van de samenwerking, de uitbesteding van taken en de operationele behoefte neemt RWS binnen de kaders van het beveiligingsbeleid van IenM de ruimte om afgeleide implementatierichtlijnen uit de BIR RWS te ontwikkelen en van toepassing te verklaren zoals de Cybersecurity Implementatierichtlijn Objecten - RWS. Schematisch ziet dit er als volgt uit:

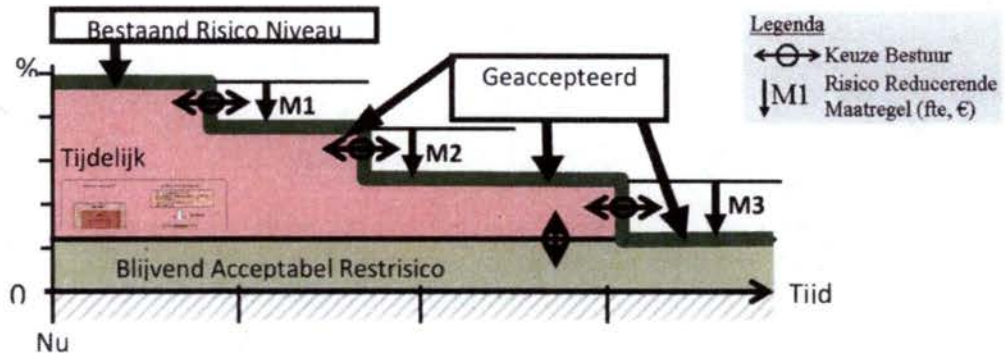


De Cybersecurity Implementatierichtlijn Objecten - RWS is een vertaalslag en specifieke invulling van de relevante beheersdoelen en beheersmaatregelen uit de BIR RWS en de NCSC Checklist beveiliging ICS/SCADA systemen voor de beveiliging van objecten RWS. Waar nodig zijn aanvullingen gedaan uit good practices voor de beveiliging van IA, ICT en ICS/SCADA-systemen. De formulering van de beheersdoelen en beheersmaatregelen heeft meer een operationeel karakter en is daardoor geschikt voor zowel RWS interne doelgroepen zoals objectbeheerders en projecten als voor gebruik bij inkooptrajecten, contracten, vraagspecificaties en uitvoering van werk door marktpartijen.

Tevens is in de Cybersecurity Implementatierichtlijn Objecten - RWS rekening gehouden met de risico mitigatiestrategie van RWS. Op basis van interne en externe onderzoeksrapporten en de hieruit voortvloeiende aanbevelingen is er voor gekozen om te starten met een set van top 10 maatregelpakketten. Bij implementatie van deze maatregelen zal RWS de belangrijkste kwetsbaarheden die kunnen leiden tot een onacceptabel risico voor RWS op het vlak van functionaliteit, veiligheid en imagoschade gaan beheersen. Primair hebben de maatregelen het doel om misbruik, uitval en fouten binnen de IV en IA te voorkomen.

Verder is in de richtlijn gezocht naar een balans tussen de meer generieke beheersdoelen en beheersmaatregelen uit de BIR RWS en de meer specifieke beheersdoelen en beheersmaatregelen op basis van de risico's en de risicogestuurde aanpak binnen RWS voor het werkveld van de IA.

Mitigatiestrategie – Sturing op top 10 maatregelpakketten



1.3 Instructie voor toepassing

RWS streeft naar een passend niveau van beveiliging voor de objecten en de Infrastructuur waar de objecten onderdeel van uitmaken. Daarbij wordt aan een object een specifieke cyber-classificatie toegekend (zie voor deze cyber-classificatie per object de meest recente versie van de Infraclassificatie[1]). Deze cyber-classificatie correspondeert met een zgn. cybersecurity-weerstandsniveau, conform onderstaande tabel.

Classificatie object in Infraclassificatie	Cybersecurity weerstandsniveau
A	4
B	3
C	2
D	1
E	1

Voor een object met een weerstandsniveau 4 wordt een zwaarder maatregelenpakket geïmplementeerd dan voor een object met een weerstandsniveau 3. In dit document is een implementatierichtlijn opgenomen per weerstandsniveau.

Cybersecurity weerstandsvermogen in Ketens: Elke keten is zo sterk als de zwakste schakel. Indien de bediening of het beheer van object A wordt gedaan vanuit een initieel lager geclassificeerd object B, wordt de classificatie van dat object B verhoogd tot het cybersecurity weerstandsniveau van object A.

Als een RWS object nog niet voorzien is van een cyber-classificatie dient er contact gezocht te worden met de afdeling Security Center van RWS-CIV-IRN voor advies en correcte indeling qua cybersecurity weerstandsniveau.

In het geval dat er helemaal geen object uit de infraclassificatie lijst objecten voorkomt in de scope van de overeengekomen dienstverlening dan dient voor de beveiliging van de ICT-, ICS/SCADA-, DVM-systemen en datanetwerkcomponenten binnen de Infrastructuur RWS het Cybersecurity weerstandniveau van 1 te worden aangehouden.

Voorbeeld

Uitgaande van een specifieke tunnel met cyber-classificatie B (volgens Infraclassificatie) dienen alle generieke beheersdoelen uitgewerkt te worden in het beveiligingsplan van Opdrachtnemer. Voor de tunnel dienen de generieke beheersdoelen met als uitgangspunt cybersecurity weerstandsniveau 3 in bovenstaand tabel aangevuld te worden met specifieke maatregelen uit de maatregelpakketten die te vinden zijn in hoofdstuk 3 van dit document. Bij mogelijke overlap tussen de generieke beheersdoelen en de specifieke aanvullende maatregelen uit de maatregelpakketten dienen de specifieke maatregelen voorrang te hebben. Met de invulling van de specifieke maatregelen wordt tevens de bovenliggende generieke beheersdoel en of beheersmaatregel ingevuld.

[1] Momenteel op te vragen bij PRIA of CIV-IRN/Security Center

1.4 Structuur

Hoofdstuk 2 beschrijft de relevante set van beheersdoelen en beheersmaatregelen die afgeleid zijn uit de BIR (RWS). Dit zijn de meer generieke geformuleerde beheersdoelen en beheersmaatregelen in de vaste hoofdstuk- en paragraaf indeling van de BIR (RWS). Binnen de hoofdstuk structuur van de BIR RWS zijn tevens de relevante beheersdoelen en beheersmaatregelen uit de NCSC Checklist beveiliging ICS/SCADA systemen geïntegreerd. Indien noodzakelijk wordt vanuit de generieke beheersdoel doorverwezen naar de specifieke maatregelpakketten waar een verdieping plaatsvindt in de maatregelenset en dit is weer afhankelijk van het risico en het cybersecurity weerstandsniveau dat gehaald moet worden.

Hoofdstuk 3 beschrijft de specifieke maatregelpakketten. De specifieke maatregelpakketten zijn een aanvulling en verdieping op de generieke beheersdoelen en beheersmaatregelen uit hoofdstuk 2. De maatregelpakketten zijn gerelateerd aan de risico's en de risico mitigatiestrategie die RWS hanteert. In de specifieke maatregelpakketten wordt tevens een link gemaakt met de infraclassificatie objecten van RWS. Afhankelijk van de infraclassificatie en de daaruit volgende cybersecurity weerstandsniveau van het object wordt een vaste set van maatregelen voorgeschreven. Bij de samenstelling van de specifieke maatregelpakketten is gebruik gemaakt van de NCSC Checklist beveiliging ICS/SCADA systemen en overige good practices voor de beveiliging van IA en ICS/SCADA systemen.

In bijlage A en B zijn de wachtwoord richtlijn en de Factsheet Wachtwoorden opgenomen.

2 Generieke beheersdoelen en beheersmaatregelen

Het Beveiligingsbeleid van IenM geeft aan dat de dienstonderdelen daar waar nodig aanvullingen dienen te plegen op de BIR om de beveiligingsrisico's in het eigen werkveld zoals de IA te mitigeren.

De BIR (RWS) is vanwege de interne gerichte formulering van beheersdoelen en beheersmaatregelen die veelal gelinkt worden aan de interne rolhouders en organisatorische inbedding niet zonder meer geschikt voor toepassing in projecten en in uitbestedingstrajecten. Een vertaalslag is nodig van de BIR (RWS) beheersdoelen en beheersmaatregelen naar een meer pragmatische en operationele toepassing.

De Cybersecurity Implementatierichtlijn Objecten - RWS is dan ook niet meer dan een vertaalslag en specifieke invulling van de relevante beheersdoelen en beheersmaatregelen uit de BIR RWS en de "NCSC Checklist beveiliging ICS/SCADA systemen" voor de beveiliging van objecten. Waar nodig zijn aanvullingen gedaan uit good practices voor de beveiliging van IA, ICT en ICS/SCADA-systemen. De formulering van de beheersdoelen en beheersmaatregelen zijn generiek van aard en daardoor geschikt voor zowel RWS interne doelgroepen zoals objectbeheerders en projecten als voor gebruik bij inkooptrajecten, contracten, vraagspecificaties en uitvoering van werk door marktpartijen. Indien nodig wordt verwezen naar aanvullende beheersdoelen en beheersmaatregelen die in hoofdstuk 3 staan beschreven. Op basis van de risico mitigatiestrategie en de infraclassificatie objecten kunnen aanvullende specifieke maatregelen nodig zijn om invulling te geven aan de generiek geformuleerde beheersdoelen en beheersmaatregelen in dit hoofdstuk.

BIR-(RWS) indeling		**Generieke beheersdoelen en beheersmaatregelen**
B-1 A5.1.1	**Hoofdeis Cybersecuritybeleid**	Opdrachtnemer conformeert zich aan het Cybersecuritybeleid van Opdrachtgever door invulling te geven aan de Cybersecurity beheersdoelen en maatregelen zoals beschreven in de overeenkomst en de specifieke aanvullende beheersdoelen en maatregelen die zijn beschreven in de Cybersecurity Implementatierichtlijn Objecten - RWS.
	Invulling	Middels beheersmaatregelen uit Cybersecurity Implementatierichtlijn Objecten - RWS.
B-2	**Code voor Informatie-beveiliging**	Voor de invulling van de beheersdoelen dient Opdrachtnemer beheersmaatregelen te implementeren die volgen uit de Cybersecurity Implementatierichtlijn Objecten - RWS van Opdrachtgever. Indien de Cybersecurity Implementatierichtlijn Objecten - RWS van Opdrachtgever niet voorziet in specifieke beheersmaatregelen voor de invulling van de beheersdoelen van Opdrachtgever dan dient de Code voor Informatiebeveiliging - NEN-ISO/IEC 27002-2005 (of de meest recente versie hiervan) aangehouden te worden voor de te nemen beheersmaatregelen in relatie tot het beheersdoel van Opdrachtgever.
	Invulling	Middels Cybersecurity Implementatierichtlijn Objecten - RWS of de beheersmaatregelen uit NEN-ISO/IEC-27002
B-3	**Gelaagde beveiliging**	Bij de keuze van de beheersmaatregelen voor de beveiliging van de infrastructuur en systemen en met name voor de ICS/SCADA toepassingen dient het principe van gelaagde beveiliging gevolgd te worden die meerdere lagen van beveiliging bewerkstelligt binnen het ontwerp en inrichting op proces-, netwerk-, systeem- en applicatieniveau.
NCSC T/O-4	Invulling	Middels beheersmaatregelen uit NEN-ISO/IEC-27002
B-4 A5.1.2	**Evaluatie en actualisatie van Cybersecuritybeleid**	Opdrachtgever behoudt te allen tijde het recht om wijzigingen in de beheersdoelen aan te brengen als gevolg van de periodieke evaluatie van het Cybersecuritybeleid of naar aanleiding van (dreigende) incidenten. In dergelijke gevallen dient de Opdrachtnemer direct passende beheersmaatregelen te treffen.
	Invulling	Middels beheersmaatregelen uit NEN-ISO/IEC-27002 par. 5.1.2, 13.1 en 13.2
B-5	**Belegging**	De Opdrachtnemer dient voor Cybersecurity de verantwoordelijkheden binnen de eigen organisatie te beleggen.

A6.1	**verantwoordelijk-heden**	
	Invulling	Middels beheersmaatregelen uit NEN-ISO/IEC-27002 par. 6.1.1 en 6.1.3
B-6 A6.1	**Borging beheersdoelen en certificering**	Opdrachtnemer dient de Cybersecurity beheersdoelen van Opdrachtgever te borgen in zijn processen/(kwaliteits)managementsysteem en kan ervoor kiezen om zich te laten certificeren conform NEN-ISO/IEC-27001. Indien voor certificering conform de NEN-ISO/IEC-27001 wordt gekozen dienen de beheersdoelen van Opdrachtgever onderdeel uit te maken van de scope van certificering.
NCSC O-1	Invulling	
B-7 A6.2.3	**Onderaanneming**	Opdrachtnemer dient alle relevante Cybersecurity beheersdoelen en maatregelen aan alle onderaannemers middels een overeenkomst op te leggen en toe te zien op naleving.
	Invulling	Middels beheersmaatregelen uit NEN-ISO/IEC-27002 par. 6.2.3
B-8	**Risicomanagement**	Opdrachtnemer dient op basis van risicoanalyses en risicoafwegingen voor de Cybersecurity beheersdoelen van Opdrachtgever beheersmaatregelen te treffen.
NCSC O-2	Invulling	Conform NEN-ISO/IEC-27005
B-9 A7.1.1	**Inventarisatie Configuration Items en opname in Configuration Management Database**	Opdrachtnemer dient over een geborgde procedure te beschikken voor de inventarisatie en registratie van alle Configuration Items (CI's) met bijbehorende settings/configuraties in een Configuration Management Database (CMDB) die actueel wordt gehouden en draagt zorg dat deze informatie beschikbaar is voor andere beheerprocessen.
NCSC T/O-10	Invulling	Middels ITIL Configuration Management
B-10 A7	**Beveiliging bedrijfsmiddelen**	Opdrachtnemer dient maatregelen te nemen om de ICT- ICS/SCADA- DVM-systemen en datanetwerken te beschermen tegen verlies, vernietiging en vervalsing.
	Invulling	
B-11	**Aanvaardbaar gebruik**	Door Opdrachtgever beschikbaar gestelde toegangsmiddelen (tokens, pasjes) tot ICT, ICS/SCADA en

A7.1.3	**toegangsmiddelen**	ondersteunende systemen en –netwerken dienen alleen gebruikt te worden voor het doel waarvoor ze ontworpen zijn waarbij de beveiligingsmaatregelen niet omzeild mogen worden.
	Invulling	Middels beheersmaatregelen uit NEN-ISO/IEC-27002 par. 7.1.3
B-12 A7.2.1	**Classificatie en beveiliging informatie**	Opdrachtnemer dient de door Opdrachtgever aangegeven classificatie en bijbehorende beveiligingsmaatregelen aan te houden voor de beveiliging van informatie.
	Invulling	Middels beheersmaatregelen uit NEN-ISO/IEC-27002 par. 7.2
B-13 A8	**Bewustwording en scholing**	Opdrachtnemer dient voor bewustwording en scholing middels de beheersmaatregelen uit de Cybersecurity Implementatierichtlijn Objecten - RWS te bewerkstelligen dat werknemers en ingehuurd personeel bewust worden gemaakt en geschikte training en regelmatige bijscholing krijgen met betrekking tot het beveiligingsbeleid en procedures, voor zover relevant voor hun functie.
NCSC O-5	Invulling	Middels beheersmaatregelen uit hoofdstuk "Maatregelen bewustwording en training" uit de Cybersecurity Implementatierichtlijn Objecten - RWS en beheersmaatregelen uit de NEN-ISO/IEC-27002 par. 8.2.2
B-14 A8.1.2	**Gescreend personeel**	Opdrachtnemer dient werkzaamheden door gescreend personeel te laten uitvoeren. De Opdrachtnemer dient te verzorgen dat al het onderhoudspersoneel voorafgaand aan operationele inzet een geheimhoudingsverklaring heeft ondertekend en over een VOG bezit die gerelateerd is aan de beoogde werkzaamheden. Opdrachtnemer houdt hier een actuele administratie van bij. Hangende de aanvraag van een VOG kan worden volstaan met een eigen verklaring van betreffende medewerker gedurende een periode van maximaal zes weken welke niet verlengd kan worden.
	Invulling	Middels beheersmaatregelen uit hoofdstuk "Maatregelen beheer en onderhoud uit Cybersecurity Implementatierichtlijn Objecten - RWS
B-15 A9.1.1	**Fysieke beveiliging**	De fysieke beveiliging van het object dient conform het "Handboek Security Rijkswaterstaat" te worden vormgegeven.
NCSC T/O-9	Invulling	Middels beheersmaatregelen uit het "Handboek Security Rijkswaterstaat".
B-16 A9.1.2	**Fysieke toegangsbeveiliging**	De fysieke toegangsbeveiliging IA - ruimten binnen het object dient conform de beheersmaatregelen uit de Cybersecurity Implementatierichtlijn Objecten - RWS hoofdstuk " Maatregelen Fysieke toegangsbeveiliging IA-gerelateerde ruimten" ingevuld te worden.

NCSC T/O-9	Invulling	Middels beheersmaatregelen uit hoofdstuk " Maatregelen Fysieke toegangsbeveiliging IA-gerelateerde ruimten" van de Cybersecurity Implementatierichtlijn Objecten - RWS
B-17 A9.2.1	**Plaatsing en bescherming van RWS bedrijfsmiddelen**	Opdrachtnemer dient zorg te dragen dat bedrijfsmiddelen, ICT-, ICS/SCADA-, DVM-systemen en datanetwerkcomponenten zo worden geplaatst en beschermd dat risico's van schade en storing van buitenaf en de gelegenheid voor onbevoegde toegang worden verminderd.
NCSC T/O-9	Invulling	Middels beheersmaatregelen uit NEN-ISO/IEC-27002 par. 9.2.1
B-18 A9.2.3	**Voedings- en telecommunicatie-kabels**	Voedings- en telecommunicatiekabels die voor dataverkeer of ondersteunende informatiediensten worden gebruikt, dienen tegen aftapping of beschadiging te zijn beschermd.
	Invulling	Middels beheersmaatregelen uit NEN-ISO/IEC-27002 par. 9.2.3
B-19 A10.1.1 NCSC T/O-10	**Documentatie bediening en beheer**	ICS/SCADA, beveiliging, ICT-systemen en –netwerken dienen een gedocumenteerde beheer- en bedienprocedure, onderhoud en support level te hebben.
	Invulling	Middels beheersmaatregelen uit NEN-ISO/IEC-27002 hoofdstuk 10
B-20 A10.1.2	**Geborgde wijzigings-procedure**	Opdrachtnemer dient conform hoofdstuk "Maatregelen gecontroleerd wijzigen" uit de Cybersecurity Implementatierichtlijn Objecten - RWS over een geborgde wijzigingsprocedure te beschikken voor het doorvoeren van wijzigingen aan ICS/SCADA en ondersteunende ICT systemen, beveiliging- en netwerkomgeving. Wijzigingen dienen eerst in de testomgeving beproefd te worden.
NCSC T/O-10	Invulling	Middels beheersmaatregelen uit hoofdstuk "Maatregelen gecontroleerd wijzigen" van de Cybersecurity Implementatierichtlijn Objecten - RWS en ITIL Changemanagement proces
B-21 A10.4.1	**Hardening**	ICS/SCADA, beveiliging en ondersteunende ICT-systemen en –netwerkelementen dienen middels beheersmaatregelen uit hoofdstuk "Bescherming tegen malware, hardening en patching" van de Cybersecurity Implementatierichtlijn Objecten - RWS te zijn gehardend door: • niet noodzakelijke netwerkservices uit te zetten • verwijderen van bekende kwetsbaarheden • alle poorten die niet nodig zijn te deactiveren/blokkeren • alle default "access points" te verwijderen • optimaal gebruik te maken van de security opties van leveranciers

	Invulling	Middels beheersmaatregelen uit hoofdstuk "Bescherming tegen malware, hardening en patching" van de Cyberscecurity Implementatierichtlijn Objecten - RWS.
B-22 A10.4.1	**Bescherming tegen malware**	Er dient een geborgde procedure en voorzieningen conform hoofdstuk "Bescherming tegen malware, hardening en patching" van de Cybersecurity Implementatierichtlijn - RWS te bestaan voor detectie en preventie tegen malware. Tevens dient Opdrachtnemer voor controle vooraf van in te zetten beheer- en onderhoudsapparatuur over een geborgde procedure en voorzieningen te beschikken voor detectie, preventie en verwijdering van malware.
	Invulling	Middels beheersmaatregelen uit hoofdstuk "Bescherming tegen malware, hardening en patching" van de Cybersecurity Implementatierichtlijn Objecten - RWS.
B-23 A10.5.1	**Back-ups en bewaartermijnen**	De integriteit en beschikbaarheid van de ICS/SCADA systemen, programmatuur en besturingssystemen dient conform hoofdstuk "Back-ups" van de Cybersecurity Implementatierichtlijn Objecten - RWS gewaarborgd te worden door het maken van back-ups om herstel na een incident of calamiteit mogelijk te maken.
	Invulling	Middels beheersmaatregelen uit hoofdstuk "Back-ups" van de Cybersecurity Implementatierichtlijn Objecten - RWS.
B-24 A10.5.1	**Back-up en recovery procedure**	Er dient conform hoofdstuk "Maatregelen Back-ups" van de Cybersecurity Implementatierichtlijn Objecten - RWS een geborgd proces te bestaan voor het jaarlijks controleren en testen van de recovery procedure en de leesbaarheid en bruikbaarheid van de ingezette media voor back-ups.
		Middels beheersmaatregelen uit hoofdstuk "Maatregelen Back-ups" van de Cybersecurity Implementatierichtlijn Objecten - RWS.
B-25 A10.7.4	**Beveiliging documentatie**	Documentatie van ICS/SCADA, beveiliging, ICT-systemen en –netwerkelementen dient beschermd te worden tegen onbevoegde toegang.
	Invulling	Middels beheersmaatregelen uit NEN-ISO/IEC-27002 par. 10.7.4
B-26 A10.10.1	**Activiteiten in audit-logbestanden**	De activiteiten van gebruikers, beheerders, uitzonderingen en informatiebeveiligingsgebeurtenissen dienen conform de beheersmaatregelen uit hoofdstuk "Maatregelen Logging en Monitoring" van de Cybersecurity Implementatierichtlijn Objecten - RWS te worden vastgelegd in audit-logbestanden waarbij een logregel minimaal de volgende gegevens bevat: • de gebeurtenis zelf

BIR 10.10		• een tot een natuurlijk persoon herleidbare gebruikersnaam of (systeem)-ID • de gebeurtenis • waar mogelijk de identiteit van het werkstation of de locatie • het object waarop de handeling werd uitgevoerd • het resultaat van de handeling • de datum en het tijdstip van de gebeurtenis
NCSC T/O-8		Middels beheersmaatregelen uit hoofdstuk "Maatregelen Logging en Monitoring" van de Cybersecurity Implementatierichtlijn Objecten - RWS.
B-27	**Geen gevoelige gegevens in logregels**	In een logregel worden in geen geval gevoelige gegevens opgenomen. Dit betreft onder meer gegevens waarmee de beveiliging doorbroken kan worden zoals wachtwoorden, inbelnummers, e.d.
		Middels beheersmaatregelen uit NEN-ISO/IEC-27002 par. 10.10.1
B-28 A10.10.1	**Bewaartermijn audit logbestanden**	Opdrachtnemer dient van de systemen met logvoorzieningen de audit logbestanden een maand te bewaren.
NCSC T/O-8		
B-29 A10.10.3	**Beveiliging logbestanden**	De Opdrachtnemer dient zorg te dragen voor de beveiliging van logbestanden van ICS/SCADA, beveiliging en ondersteunende ICT-systemen en -netwerkelementen.
NCSC T/O-8		Middels beheersmaatregelen uit NEN-ISO/IEC-27002 par. 10.10.3
B-30 A10.10.3	**Levering logfiles**	Logfiles van ICS/SCADA, beveiliging en ondersteunende ICT-systemen en- netwerkelementen dienen op verzoek aan Opdrachtgever in CSV-formaat opgeleverd te worden.
NCSC T/O-8		
B-31 A11.1.1	**Toegang geautoriseerden fysiek en logisch**	Opdrachtnemer dient conform hoofdstuk "Maatregelen Logische toegang" van de Cybersecurity Implementatierichtlijn Objecten - RWS zorg te dragen dat de fysieke toegang tot het object en ruimten waar zich informatie, software en andere bedrijfsmiddelen (o.a. apparatuur) bevinden, alsmede de logische toegang tot systemen, uitsluitend toegestaan is voor personen die hiertoe door Opdrachtgever en/of Opdrachtnemer

		geautoriseerd zijn.
NCSC T/O-9	Invulling	Middels beheersmaatregelen uit hoofdstuk "Maatregelen Logische toegang" van de Cybersecurity Implementatierichtlijn Objecten - RWS.
B-32 A11.2.1	**Registratie fysieke toegang**	Opdrachtnemer dient zorg te dragen voor een procedure en registratie die de lokale fysieke toegang van alle medewerkers inclusief onderaannemers tot technische ruimten regelt en dat de registratie up-to-date blijft, hetzij geautomatiseerd hetzij op papier. *Toelichting: Opdrachtnemer is, binnen de overeengekomen beheertaken, verantwoordelijk voor het onderhouden van een registratie van alle aan medewerkers - zowel van Opdrachtnemer als onderaannemers - toegekende autorisaties en toegangsmiddelen.*
	Invulling	Middels beheersmaatregelen uit NEN-ISO/IEC-27002 par. 9.1.2 en 11.2
B-33 A11.3.1	**Wachtwoord richtlijn**	Opdrachtnemer dient zorg te dragen dat op ICS/SCADA en ondersteunende ICT systemen en –netwerken standaard/default accounts en/of wachtwoorden uitgeschakeld zijn en gehandeld wordt conform de beheersmaatregelen uit hoofdstuk "Wachtwoord Richtlijn" van de Cybersecurity Implementatierichtlijn Objecten - RWS van Opdrachtgever.
NCSC T/O-3	Invulling	Middels beheersmaatregelen uit hoofdstuk "Wachtwoord Richtlijn" van Cybersecurity Implementatierichtlijn Objecten - RWS.
B-34 A11.4.1	**Koppeling apparatuur**	Opdrachtnemer dient over een geborgde procedure te beschikken voor het veilig koppelen van mobiele apparatuur van derden of removable media aan locale ICS/SCADA netwerken of het RWS netwerk.
NCSC T/O-6 en 7	Invulling	Middels beheersmaatregelen uit NEN-ISO/IEC-27002 par. 11.7.1
B-35 A11.4.5	**Geen directe verbinding met kantoornetwerken**	Opdrachtnemer dient zorg te dragen dat ICS/SCADA en de ondersteunende systemen en besloten (lokale) datanetwerken geen directe verbindingen hebben met kantoornetwerken.
NCSC T/O-2	Invulling	Middels beheersmaatregelen uit NEN-ISO/IEC-27002 par. 11.4.5
B-36	**Minimalisatie**	Opdrachtnemer dient conform hoofdstuk "Maatregelen Netwerkkoppelingen" van de Cybersecurity Implementatierichtlijn Objecten - RWS zorg te dragen dat het aantal netwerkkoppelingen tussen ICS/SCADA

	netwerkkoppelingen	systemen en andere netwerken beperkt blijft tot alleen de functioneel noodzakelijke
NCSC T/O-2	Invulling	Middels beheersmaatregelen uit hoofdstuk "Maatregelen Netwerkkoppelingen" van Cybersecurity Implementatierichtlijn Objecten - RWS.
B-37	**Verboden en geautoriseerde verbindingen**	Opdrachtnemer dient zorg te dragen dat er geen Internet, draadloze (WiFi en GPRS/UMTS etc.) of inbelvoorzieningen verbonden worden met de besloten (lokale) objectnetwerken en/of hierop aangesloten systemen. Uitgezonderd zijn de netwerkverbindingen van het object met de centrale netwerkvoorzieningen van RWS en de door RWS-CIV toegestane verbindingen.
NCSC T/O-2	Invulling	
B-38	**Remote access**	Opdrachtnemer dient conform hoofdstuk "Maatregelen Logische toegang" van Cybersecurity Implementatierichtlijn Objecten - RWS zorg te dragen dat Remote Access voor bediening en beheer tot ICT, ICS/SCADA en (ondersteunende) systemen en objectnetwerken altijd verloopt via de centrale, beveiligde en gemonitorde voorzieningen van RWS met inzet van two-factor authenticatie. De aanvraag verloopt via Opdrachtgever en conform de "Procedure Toegang derden RWS".
	Invulling	Middels beheersmaatregelen uit hoofdstuk "Maatregelen Logische toegang" van Cybersecurity Implementatierichtlijn Objecten - RWS en "Procedure Toegang derden RWS".
B-39	**Actuele documentatie netwerkkoppelingen**	Opdrachtnemer dient over een geborgde procedure te beschikken die: • alle wijzigingen aan het objectnetwerk bijhoudt; • de lokale objectnetwerktopologie actueel houdt; • een zodanig detailniveau heeft dat alle netwerkkoppelingen en objectnetwerkcomponenten met alle relevante informatie beschikbaar is in een CMDB.
TF 1 en 3; NCSC T/O-2	Invulling	
B-40 A11.4.6	**Compartimentering infrastructuur**	ICS/SCADA systemen dienen gebruik te maken van een eigen gecompartimenteerde infrastructuur die van de Kantoorautomatisering is afgescheiden. De scheiding kan fysiek of logisch zijn.
NCSC T/O-1	Invulling	Middels beheersmaatregelen uit NEN-ISO/IEC-27002 par. 11.4.5

B-41	**Segmentering van verkeersstromen**	Binnen de locale object dataverkeersnetwerken voor ICS/SCADA systemen dient segmentering voor de datastromen voor productie, beheer en OTA toegepast te worden.
B-42	**Gebruik beveiligde communicatie protocollen**	Wanneer configuratie van ICS/SCADA-systemen op afstand plaatsvindt, dient dit altijd over beveiligde verbindingen plaats te vinden. Inzet van onveilige communicatieprotocollen zoals FTP, Telnet, VNC en RDP dient vermeden te worden. Indien dit niet haalbaar is, mogen deze enkel gemotiveerd worden ingezet wanneer een additioneel encryptiekanaal wordt toegepast (zoals SSL, TLS of IPSEC).
B-43	**Beveiligde netwerkkoppelingen en netwerkaansluit-voorwaarden RWS**	Opdrachtnemer dient zorg te dragen dat alle netwerkkoppelingen tot het RWS netwerk en de lokale objectnetwerken strikt en uitsluitend plaats vinden via de centrale beveiligde voorzieningen en conform de NNV-aansluitvoorwaarden van RWS.
	Invulling	Conform "NNV aansluitvoorwaarden"
B-44 A11.5.2	**IAA proces**	De toegang tot gegevens, de verwerking of de uitwisseling van gegevens met derden, ICS/SCADA en ondersteunende systemen en -netwerken dient plaats te vinden na een succesvol identificatie, authenticatie en autorisatie proces.
	Invulling	
B-45 A11.2.3 & BIR 11.2.3	**Versleutelde uitwisseling en opslag van IAA gegevens**	Identificatie, authenticatie en autorisatiegegevens worden in versleutelde vorm uitgewisseld en in versleutelde vorm opgeslagen.
	Invulling	
B-46 A11.6.1	**Verboden toegang tenzij expliciet toegestaan**	Alle toegang tot informatie, systemen, ICS/SCADA en de ondersteunende systemen en -netwerken dient geweigerd te worden tenzij het expliciet is toegestaan.

NICC	Invulling	
B-47	**Lokale logische toegang**	Opdrachtnemer dient voor de lokale logische toegang tot ICT-, ICS/SCADA-systemen en lokale tunnelnetwerken over een geborgde procedure en up-to-date registratie te beschikken van uitgegeven accounts met bijbehorende rechten.
	Invulling	Middels beheersmaatregelen uit hoofdstuk "Maatregelen Logische toegang" van Cybersecurity Implementatierichtlijn Objecten - RWS.
B-48	**Raamwerk beveiliging webapplicaties**	Bij inzet van webapplicaties voor bediening en beheer dient het "Raamwerk beveiliging Webapplicaties" van het National Cyber Security Centrum voor de invulling van beveiliging gevolgd te worden.
	Invulling	Middels "Raamwerk beveiliging Webapplicaties" van het National Cyber Security Centrum.
B-49 A12.1.1	**Validatie controles**	Toepassingen dienen te voorzien in validatie controles om eventueel corrumperen van informatie door verwerkingsfouten of opzettelijke handelingen traceerbaar te maken.
	Invulling	Middels beheersmaatregelen uit de NEN-ISO/IEC-27002 par. 12.2
B-50	**WIB vendor requirements**	Voor leveranciers van ICS/SCADA systemen dient Opdrachtnemer waar mogelijk de vendor requirements te hanteren van de Werkgroep voor Instrument Beoordeling (WIB).
A12.5.5	Invulling	Middels beheersmaatregelen uit de NEN-ISO/IEC-27002 par. 12.5.5 en WIB vendor requirements versie 2.0 oktober 2010.
B-51 A12.6.1	**Respons proces op technische kwetsbaarheden**	De Opdrachtnemer dient een proces te hebben waarmee tijdig gereageerd kan worden op technische kwetsbaarheden van de in gebruik zijnde ICS/SCADA en ondersteunende ICT-systemen en netwerken en Opdrachtnemer maakt dit aantoonbaar aan Opdrachtgever.
	Invulling	Middels beheersmaatregelen uit de NEN-ISO/IEC-27002 par. 12.6
B-52 A12.6.1	**Beveiligingsupdates en patches**	Opdrachtnemer dient zorg te dragen dat ICT systemen die gekoppeld worden aan ICS/SCADA, beveiliging- en netwerkomgeving en de ICS/SCADA systemen zelf, voorzien zijn van alle recente beveiligingsupdates en patches.
NCSC T/O-5	Invulling	Middels beheersmaatregelen uit de NEN-ISO/IEC-27002 par. 12.4.1

B-53	**Risicoanalyse en implementatieadvies kritieke patches**	Opdrachtnemer dient conform hoofdstuk "Maatregelen bescherming tegen malware, hardening en patching" van Cybersecurity Implementatierichtlijn Objecten - RWS over een geborgde procedure te beschikken die er voor zorgt dat voor kritieke patches binnen 48 uur na melding, gerekend vanaf eerstvolgend werkdag een risicoanalyse wordt uitgevoerd en voorzien is van een implementatieadvies. Voor niet kritieke patches is de doorlooptijd voor uitvoering van risicoanalyse en implementatieadvies maximaal twee maanden. De patches worden na instemming met het implementatieadvies door Opdrachtgever conform het advies door Opdrachtnemer geïmplementeerd.
NCSC T/O-5	Invulling	Middels beheersmaatregelen uit hoofdstuk "Maatregelen bescherming tegen malware, hardening en patchting" van Cybersecurity Implementatierichtlijn Objecten - RWS.
B-54 A13.1.1	**Procedure incidenten informatiebeveiliging**	Opdrachtnemer dient conform implementatierichtlijn "Maatregelen Beveiligingsincidenten en Incident Response" een geborgde procedure te hebben voor het melden en oplossen van informatiebeveiligingsincidenten.
	Invulling	Middels implementatierichtlijn "Maatregelen Beveiligingsincidenten en Incident Response"
B-55 A13.1.2	**Rapportage incidenten informatiebeveiliging**	Opdrachtnemer dient aan Opdrachtgever maandelijks een rapportage te verstrekken van alle beveiligingsincidenten, en van alle maatregelen die ter zake getroffen zijn.
	Invulling	Middels beheersmaatregelen uit NEN-ISO/IEC-27002 par. 13.1
B-56 A13.2.3	**Bewijsmateriaal verzamelen en bewaren**	In voorkomende gevallen dient Opdrachtnemer zijn medewerking te verlenen bij een juridische vervolgprocedure voor het verzamelen en bewaren van bewijsmateriaal.
		Middels beheersmaatregelen uit NEN-ISO/IEC-27002 hoofdstuk 13.2.3
B-57 A4.1.3	**Continuïteit en herstel bedrijfsprocessen en -activiteiten**	Opdrachtnemer dient maatregelen te nemen om onderbreking van dienstverlening voor Opdrachtgever tegen te gaan en continuïteitsplannen te ontwikkelen voor de kritieke dienstverleningsprocessen waarmee deze beschermd worden tegen de gevolgen van omvangrijke storingen in informatiesystemen en herstel bewerkstelligd wordt.
	Invulling	Middels beheersmaatregelen uit de NEN-ISO/IEC-27002 hoofdstuk 14
B-58	**Testen**	Opdrachtnemer dient jaarlijks de ontwikkelde continuïteitsplannen te testen om te bewerkstelligen dat ze

A14.1.5	**continuïteitsplannen**	actueel en doeltreffend blijven.
	Invulling	Middels beheersmaatregelen uit de NEN-ISO/IEC-27002 paragraaf 14.1.5.
B-59 A15	**Vigerende wet- en regelgeving en geheimhouding**	Opdrachtnemer dient te bewerkstelligen dat informatie en persoonsgegevens overeenkomstig relevante wetgeving, voorschriften en indien van toepassing contractuele bepalingen, worden beveiligd en geheimhouding in acht wordt genomen.
	Invulling	Middels beheersmaatregelen uit NEN-ISO/IEC-27002 hoofdstuk 15
B-60 A15	**Wet bescherming persoonsgegevens**	De Opdrachtnemer dient zorg te dragen voor rechtmatige verwerking en omgang met persoonsgegevens, camerabeelden en andere tot natuurlijke personen herleidbare gegevens.
	Invulling	Conform Wet bescherming persoonsgegevens
B-61 A15	**Beveiligingswerkplan en onderhoud beheersmaatregelen**	De Opdrachtnemer draagt zorg voor een up-to-date beveiligingswerkplan die op verzoek aan Opdrachtgever beschikbaar wordt gesteld en verder dienen de getroffen beheersmaatregelen voor beveiliging beheert en onderhouden te worden conform de "Cybersecurity Implementatierichtlijn Objecten - RWS hoofdstuk Maatregelen Beheer en onderhoud" van Opdrachtgever. *Toelichting: Beveiligingseisen moeten de totale keten van ontwikkeling, aanschaf, beheer, onderhoud en vervanging, etc. afdekken en het toepassen van de eisen moet in elke fase gewaarborgd zijn.*
NCSC O-3 en 4	Invulling	Middels beheersmaatregelen uit hoofdstuk "Maatregelen Beheer en Onderhoud" van Cybersecurity Implementatierichtlijn Objecten – RWS en middels beheersmaatregelen uit NEN-ISO/IEC-27002 hoofdstuk 15
B-62 A15	**Audit rapportage over getroffen maatregelen**	Opdrachtnemer dient jaarlijks een audit uit te voeren op de opzet, bestaan en werking van de getroffen Cybersecurity beheersmaatregelen en rapporteert hierover aan Opdrachtgever.
NCSC-O-5	Invulling	Middels beheersmaatregelen uit NEN-ISO/IEC-27002 paragraaf 15.3
B-63	**Wbp bewerkers-overeenkomst**	Voor de verwerking en opslag van persoonsgegevens en videobeelden, dient Opdrachtnemer met Opdrachtgever een bewerkerovereenkomst af te sluiten.

A15		
BIR 6.1.2	Invulling	Conform sjabloon Opdrachtgever "RWS bewerkersovereenkomst"
B-64 A15	**Spionage**	Opdrachtnemer dient op basis van risicoanalyse maatregelen te treffen om offertes, contracten, netwerkschema's, constructie, en bouwtekeningen te beveiligen tegen spionage in de breedste zin. *Toelichting intern: nieuwe regelgeving waarop door Veiligheid en Justitie recentelijk binnen RWS een technische kwetsbaarheid onderzoek voor heeft plaatsgevonden.*
	Invulling	Conform richtlijn Opdrachtgever

3 Specifieke maatregelpakketten

De specifieke maatregelpakketten zijn een aanvulling en verdieping op de generieke beheersdoelen en beheersmaatregelen uit hoofdstuk 2. De maatregelpakketten zijn gerelateerd aan de risico's en de risico mitigatiestrategie die RWS volgt om tot beheersing van kwetsbaarheden te komen. In de specifieke maatregelpakketten wordt tevens een link gemaakt met de infraclassificatie objecten van RWS.

RWS streeft naar een passend niveau van beveiliging voor de objecten. Daarbij wordt aan een objecttype een zgn. Cybersecurity weerstandsniveau toegekend dat correspondeert met het te beschermen belang van het object. Voor een object met een weerstandsniveau 4 wordt een zwaarder maatregelenpakket geïmplementeerd dan voor een object met een weerstandsniveau 3.

In de tabel hieronder wordt het Cybersecurity weerstandsniveau weergegeven dat nagestreefd moet worden voor de beveiliging van de verschillende objecten.

Cyber classificatie object in Infraclassificatie	**Cybersecurity weerstandsniveau**
A	4
B	3
C	2
D	1
E	1

Afhankelijk van de infraclassificatie en het daaruit volgende cybersecurity weerstandsniveau van het object wordt een vaste set van maatregelen voorgeschreven. Bij de samenstelling van de specifieke maatregelpakketten is gebruik gemaakt van de NCSC Checklist beveiliging ICS/SCADA systemen en overige good practices voor de beveiliging van IA en ICS/SCADA systemen.

Bij mogelijke overlap tussen de generieke beheersdoelen en de specifieke aanvullende maatregelen uit de maatregelpakketten dienen de specifieke aanvullende maatregelen voorrang te hebben. Met de invulling van de specifieke maatregelen wordt tevens het bovenliggende generieke beheersdoel en/of beheersmaatregel uit hoofdstuk 2 ingevuld.

3.1 Maatregelen Fysieke toegangsbeveiliging IA-gerelateerde ruimten

Cybersecurity Weerstandsniveau	**4**	**3**	**2**	**1**
VRKI-referentie	4	3	2	1
Toegangsbeheer	Rijkspas VG-IA	Rijkspas Kantoor	Sleutel	Sleutel
Toegangsproces	Lokaal geldende regels en processen			
Organisatorisch	O2	O2	O1	O1
Bouwkundig	B3	B2	B1	B1
Compartimentering	C/M3	C/M2	C/M1	C/M1
Inbraak-installatie	E3	E2	E1	E1
Alarmering	AL3	AL2	AL1	AL0
Alarm opvolging	R3	R2	R1	R0

N.B.:

1. Naast bovengenoemde weerstandsniveaus 1 t/m 4 zijn door de DG en politieke top specifieke maatregelenpakketten te definiëren. Hierbij valt bijvoorbeeld te denken aan bomvrije ruimten, kogelvrij glas of 24-uur on-site bewaking.
2. Voor richtlijnen voor de integrale fysieke beveiliging wordt verwezen naar het Handboek Security RWS (GPO).
3. Gemotiveerd afwijken van de hier genoemde implementatierichtlijnen kan, bijv. als dat efficiënter is in de integrale aanpak, als maar wel aan de bovenliggende weerstandseisen wordt voldaan.

Toelichting tabellen

Toegangsbeheer

Rijkspas VG-IA Toegang middels Rijkspas Vitale Gebieden (vanuit IA-perspectief) installatienormen (Grade 3)

Rijkspas Kantoor Toegang middels Rijkspas Kantoor installatienormen

Sleutel Toegang middels een fysieke sleutel (voor normering zie Bouwkundige maatregelen/sluitwerk)

Toegangsproces

Uitgangspunt is dat alleen toegang wordt verleend aan personen (internen / externen incl. bezoekers) die in de IA-gerelateerde ruimten moeten zijn vanwege het verrichten van werkzaamheden of het houden van toezicht.

Organisatorische maatregelen

O1 Standaard maatregelen + voorlichting over preventie + uitleg over het systeem.

O2 Als O1 + specifieke maatregelen opnemen in beveiligingsplan.

Bouwkundige maatregelen

B0 Het aanwezige hang- en sluitwerk handhaven.

B1 Hang- en sluitwerk met een inbraakwerendheid van 3 minuten volgens BRL3104 of klasse 2 NEN5096.

B2 Idem met inbraakwerendheid van 5 minuten. Alternatief: rolluiken, traliewerk, inbraakwerende beglazing.

B3 Idem met inbraakwerendheid van 10 minuten. Alternatief: rolluiken, traliewerk, inbraakwerende beglazing.

Compartimentering / Meeneem beperkende maatregelen

C/M1 Inbraakwerende kast/safe volgens VGW kwalificaties. Of M1 door verankeren, verplaatsen. Of bouwkundig compartiment C1. Alles met inbraakvertraging van 3 minuten.

C/M2 Inbraakwerende kast/safe volgens VGW kwalificaties. Of M2 door slagvaste vitrines, rolluiken e.d. Of bouwkundig compartiment C2. Alles met inbraakvertraging van 5 minuten.

C/M3 Inbraakwerende kast/safe volgens VGW kwalificaties. Of M3 door mistgenerator. Of bouwkundig compartiment C3. Alles met inbraakvertraging van 10 minuten.

Elektronische maatregelen

Ed Alleen voor woningen in risicoklasse 1. De (domestic) alarminstallatie met mogelijke doormelding naar (mobiele) telefoon. Grade 2 /NCP 2

E1 Inbraakalarminstallatie. Grade 2 /NCP 2

E2 Inbraakalarminstallatie met ruimtelijk werkende anti-masking detectoren. Grade 2 / NCP 2

E3 Inbraakalarminstallatie met anti-masking detectoren. Componenten Grade 3 /NCP 3

Alarmering

AL0 Optische en/of akoestische alarmgever en/ of alarmtransmissie naar (mobiele) telefoon

AL1 Alarmtransmissiesysteem niveau AL1 volgens NEN EN 50136-1-1 naar een PAC.

AL2 Alarmtransmissiesysteem niveau AL2 volgens NEN EN 50136-1-2 naar een PAC.

AL3 AL2 aangevuld met back-up melding (AL1) via andere transmissieweg (GPRS) naar de PAC.

Reactie (alarmopvolging)

R0 Alarmopvolging door sleutelhouder na melding naar (mobiele) telefoon.

R1 Alarmopvolging door PAC naar de sleutelhouder(s).

R2 Alarmopvolging door PAC naar een erkende Particuliere Bewakingsdienst.

R3 Als R2 + Politie (prioriteit 1) Technische alarmverificatie verplicht.

3.2 Maatregelen Logische toegang

Niveau	Mens	Procedures & Organisatie	Techniek
4	LTM 1	LTPO 1 t/m 5, 8, 9 en 10	LTT 1 t/m 3
3	LTM 1	LTPO 1 t/m 5, 7, 9	LTT 1 t/m 3
2	LTM 1	LTPO 1 t/m 6 en 9	LTT 1 t/m 3
1	LTM 1	LTPO 1 t/m 6 en 9	LTT 1 t/m 3

Mens	LTM1	Voor bewustwording, gedragsregels en training van bedienaars, beheerders en overig ondersteunend personeel zowel van RWS als die van Opdrachtnemer wordt verwezen naar de maatregelenset "bewustwording en training".
Procedures & Organisatie	LTPO1	Er dient een geborgde procedure te bestaan die de fysieke en logische toegang regelt en een actuele registratie wordt bijgehouden van alle medewerkers inclusief die van onderaannemers voor toegang tot ruimten en informatiesystemen. Tevens dient er voor de lokale logische toegang tot ICT-, ICS/SCADA-systemen en lokale datanetwerken een geborgde procedure en een up-to-date registratie te bestaan van uitgegeven accounts en autorisaties.
	LTPO2	Er dient erop toe te worden gezien dat: • de toegang voor de bestuurders tot ICS/SCADA en overige ondersteunende ICT-systemen uitsluitend op basis van het 'need to have' principe plaatsvindt; • de toewijzing en het gebruik van privileges van administrators en systeembeheerders beperkt dienen te blijven tot het noodzakelijke; • fysieke toegang tot objecten en ruimten waar zich informatie, software en andere bedrijfsmiddelen (o.a. apparatuur) bevinden, alsmede de logische toegang tot systemen, uitsluitend toegestaan wordt voor personen die hiertoe geautoriseerd zijn; • bij misbruik van accounts en autorisaties dienen disciplinaire maatregelen te worden genomen.
	LTPO3	De toegangsrechten van alle medewerkers (bedienaars, beheerders en overig ondersteunend personeel) dient jaarlijks beoordeelt en geactualiseerd te worden in een formeel proces.
	LTPO4	De lokale logische toegang voor medewerkers tot de RWS infrastructuur, ICT, ICS/SCADA systemen en de centrale en locale objectnetwerken dient bij de hiertoe verantwoordelijk gestelde en gemandateerde lijnmanager aangevraagd en goedgekeurd te worden.
	LTPO5	De (remote) toegang tot ICT, ICS/SCADA en (ondersteunende) systemen en –objectnetwerken dient altijd en uitsluitend via de centrale, beveiligde en gemonitorde voorzieningen van RWS te verlopen. Hierbij dient gebruik

		te worden gemaakt van de PDC-items van RWS-CIV.
	LTPO6	De logische toegang dient afhankelijk van de classificatie van het object als volgt te worden ingevuld: • Lokaal bediening en beheer – minimaal een user-id en wachtwoord combinatie met navolging van de wachtwoordrichtlijn • Remote toegang voor bediening en beheer - 'two factor' authenticatie en uitsluitend via de centrale beveiligde voorzieningen van RWS-CIV.
	LTPO7	De logische toegang dient afhankelijk van de classificatie van het object als volgt te worden ingevuld: • Lokaal bediening en beheer – 'two-factor' authenticatie ('bezit' plus 'kennis') met navolging van de wachtwoordrichtlijn • Remote toegang voor bediening en beheer - 'two factor' authenticatie en uitsluitend via de centrale beveiligde voorzieningen van RWS-CIV.
	LTPO8	De logische toegang dient afhankelijk van de classificatie van het object als volgt te worden ingevuld: • Lokaal bediening en beheer – Rijkspas Vitaal ('bezit' plus 'kennis') met navolging van de wachtwoordrichtlijn (indien technisch nog niet mogelijk dan minimaal op basis van user-id en wachtwoord combinatie) • Remote toegang voor bediening en beheer - 'two factor' authenticatie en uitsluitend via de centrale beveiligde voorzieningen van RWS/CIV.
	LTPO9	Er dient een geborgde procedure te bestaan die de toewijzing en verspreiding van authenticatiemiddelen aan bedienaars, beheerders en overig ondersteunend personeel regelt alsmede het innemen daarvan bij functiewisseling of vertrek (in-, door- en uitstroming). In deze procedure dient ook de voorgeschreven handelingen bij verlies, diefstal dan wel beschadiging te worden opgenomen.
	LTPO10	De toegang voor onderhoud op afstand door een leverancier wordt alleen voor de geschatte duur van dat onderhoud opengesteld op basis van een wijzigingsverzoek of storingsmelding. De toegang wordt bewaakt en teruggezet bij afmelding van de call.
Techniek	LTT1	De logische toegang tot informatiesystemen en netwerk dient plaats te vinden na het succesvol doorlopen van het identificatie, authenticatie en autorisatieproces (IAA), waarbij de IAA- gegevens voor zover haalbaar in versleutelde vorm worden uitgewisseld en opgeslagen.
	LTT2	De toegang tot ICS/SCADA en overige ondersteunende ICT-systemen is geblokkeerd, tenzij het expliciet is toegestaan.
	LTT3	Voor bedienaars en beheerders en systemen worden unieke ID's gehanteerd zodat uitgevoerde handelingen terug te leiden zijn tot een persoon of systeem.

3.3 Maatregelen Beveiligingsincidenten en incident Response Plan

Niveau	Mens	Procedures & Organisatie	Techniek
4	BIRM1	BIRPO1 t/m 8	BIRPT1
3	BIRM1	BIRPO1 t/m 8	BIRPT1
2	BIRM1	BIRPO1 t/m 3, 5, 6 en 7	BIRPT1
1	BIRM1	BIRPO1 t/m 3, 5 en 6	BIRPT1

Mens	BIRPM1	Voor bewustwording, gedragsregels en training van bedienaars, beheerders en overig ondersteunend personeel zowel van RWS als die van Opdrachtnemer wordt verwezen naar de maatregelenset "bewustwording en training".
Procedures & Organisatie	BIRPO1	Er dient een geborgde procedure te bestaan die regelt dat bedienaars, beheerders en overig ondersteunend personeel zowel van RWS als die van externe partijen beveiligingsincidenten en zwakke plekken in de beveiliging zo snel mogelijk melden bij de daartoe ingerichte meldpunten. Van bedienaars, beheerders en overig ondersteunend personeel zowel van RWS als die van externe partijen moet worden geëist dat zij alle beveiligingsincidenten, verdachte of zwakke plekken in systemen of diensten registreren en rapporteren aan de Objectverantwoordelijke/-beheerder.
	BIRPO2	Er is een Incident Manager benoemd en bijbehorende verantwoordelijkheden voor Cybersecurity zijn vastgesteld.
	BIRPO3	Er is bestaat een geborgde procedure voor de reactie op en eventuele escalatie van beveiligingsincidenten. De incidenten worden vastgelegd, gerapporteerd, gerouteerd, geanalyseerd, gekwantificeerd en afgewikkeld in relatie tot het betrouwbaarheidsniveau en de ernst van de storing. Welke rolhouders aanspreekbaar zijn inzake storingen, beveiligingsincidenten en zwakke plekken. De verantwoordelijkheden en incidentenprocedure moet gecommuniceerd worden naar de bedienaars, beheerders en overig ondersteunend personeel zowel van RWS als die van externe partijen.
	BIRPO4	De Opdrachtnemer draagt zorg voor aansluiting en borging van het eigen incidentmanagementproces op die van RWS-CIV.
	BIRPO5	Er dient een geborgde procedure te bestaan voor de maandelijkse rapportage en evaluatie van alle beveiligingsincidenten, dreigingen en maatregelen die ter zake zijn getroffen.
	BIRPO6	Voor het afhandelen van urgente en niet-standaard beveiligingsincidenten (bijv. bij computervirusinfecties en aanvallen via publieke netwerken zoals internet) wordt de Incidentmanager van RWS-CIV ingeschakeld.

	BIRPO7	Er dient een geborgde procedure te bestaan voor incidentrespons en continuïteit van de ICT en ICS/SCADA dienstverlening ingeval van incidenten en calamiteiten. De volgende informatie van ICS/SCADA en overige ondersteunende ICT-systemen dient actueel en beschikbaar te zijn voor herstel na een calamiteit: -type en merk ICS/SCADA middel -Formaat -Locatie -Back-up en licenties -Software en hardware configuratie -Vervangingsinstructie/procedure
	BIRPO8	Jaarlijks dienen de ontwikkelde incident responseplannen beproefd te worden aan de hand van een actueel oefenplan om te bewerkstelligen dat ze doeltreffend blijven. Onderdeel van incidentresponse is het testen van de noodbediening.
Techniek	BIRPT1	De ingebouwde beveiligingsfuncties, controlemechanismen en waarschuwingen die systemen genereren dienen geactiveerd en benut te worden voor registratie en rapportage van beveiligingsincidenten.

3.4 Maatregelen Netwerkkoppelingen

Niveau	Mens	Procedures & Organisatie	Techniek
4	NKM 1	NKPO 1 t/m 9	NKT 1 t/m 3
3	NKM 1	NKPO 1 t/m 9	NKT 1 t/m 3
2	NKM 1	NKPO 1, 2, 4, 5, 6, 7 en 9	NKT 1 t/m 3
1	NKM 1	NKPO 1, 2, 4, 6, 7 en 9	NKT 1 t/m 3

Mens	NKM1	Voor bewustwording, gedragsregels en training van bedienaars, beheerders en overig ondersteunend personeel zowel van RWS als die van Opdrachtnemer wordt verwezen naar de maatregelenset "bewustwording en training".
Procedures & Organisatie	NKPO1	Opdrachtnemer draagt zorg voor en ziet erop toe dat alle netwerkkoppelingen met het lokale objectnetwerk strikt en uitsluitend plaatsvinden via de beveiligde centrale netwerkvoorzieningen en koppelpunten van RWS (zoals vastgelegd in de PDC Netwerken van RWS-CIV) en dat de overige generieke centrale netwerkdiensten evenals overige ondersteunende ICT worden afgestemd en afgenomen van de RWS dienst Centrale Informatievoorziening (CIV). Rechtstreekse toegang tot ICS/SCADA-systemen vanuit een publiek netwerk - waaronder het gebruik van internet en e-mail - is verboden.
	NKPO2	Opdrachtnemer draagt zorg voor en ziet erop toe dat bij netwerkkoppelingen tussen het object en de centrale netwerken van RWS (NNV/VicNet) de aansluitvoorwaarden van NNV/VicNet in acht worden genomen. Voor remote logische toegang van personeel tot de aan het object gekoppelde systemen moet de procedure "Toegang Derden" van RWS-CIV worden gevolgd waarbij de Objectverantwoordelijke/-beheer de aanvraag verzorgt.
	NKPO3	Opdrachtnemer draagt zorg voor en ziet erop toe dat bij renovatie en nieuwbouw van lokale objectdatanetwerken afstemming plaatsvindt met de RWS-CIV voor beoordeling en aansluiting van de lokale objectdatanetwerken aan de centrale netwerken, netwerkvoorzieningen, de RWS Netwerkarchitectuur inclusief security en de IA-kaderstelling.
	NKPO4	Opdrachtnemer dient zorg te dragen dat het aantal data netwerkkoppelingen tussen ICS/SCADA systemen en andere datanetwerken beperkt blijft tot alleen de functioneel noodzakelijke, waarbij de koppeling een passende vorm van beveiliging kent en geen onacceptabele risico's oplevert voor het object en de centrale netwerkdienstverlening. Voor elke koppeling is een risicoanalyse en afweging gemaakt.
	NKPO5	Opdrachtnemer draagt zorg voor een geborgde procedure die: • alle wijzigingen aan het objectdatanetwerk bijhoudt; • de lokale objectdatanetwerktopologie actueel houdt;

		• een zodanig detailniveau heeft dat alle netwerkkoppelingen en objectdatanetwerkcomponenten met alle relevante informatie beschikbaar is in een Configuration Management Database (CMDB).
	NKPO6	Opdrachtnemer draagt zorg voor en ziet erop toe dat het lokale objectdatanetwerk gehardend is door niet noodzakelijke netwerkservices uit te zetten (voor hardening zie 'Maatregelen bescherming tegen malware, hardening en patching').
	NKPO7	Het koppelen van mobiele apparatuur van derden of removable media aan lokale ICS/SCADA systemen, lokale objectdatanetwerken of het RWS datanetwerk dient plaats te vinden na autorisatie van de hiertoe aangewezen en gemandateerde functionaris aan de kant van Opdrachtnemer.
	NKPO8	Opdrachtnemer draagt zorg voor de beschikbaarheid van de actuele configuratiegegevens van de lokale objectnetwerken door middel van een Configuration Management Database (CMDB).
	NKPO9	Opdrachtnemer draagt zorg voor een geborgde procedure die aanhaakt en opvolging geeft aan geregistreerde datanetwerkincidentmeldingen vanuit RWS-CIV.
Techniek	NKT1	Wanneer configuratie van ICS/SCADA-systemen op afstand plaatsvindt, dient dit altijd over beveiligde verbindingen plaats te vinden. Het gebruik van onveilige communicatieprotocollen zoals FTP, Telnet, VNC en RDP dient vermeden te worden. Indien dit niet haalbaar is, mogen deze enkel gemotiveerd worden ingezet wanneer een additioneel encryptiekanaal wordt toegepast (zoals SSL, TLS of IPSEC).
	NKT2	ICS/SCADA en de ondersteunende systemen en besloten (lokale) objectnetwerken mogen geen directe verbindingen hebben met kantoornetwerken.
	NKT3	De besloten (lokale) objectdatanetwerken mogen geen directe internet verbindingen hebben. Dit geldt ook voor draadloze verbindingen (WiFi en GPRS/UMTS, bluetooth etc.) of inbelvoorzieningen.

3.5 Maatregelen bescherming tegen malware, hardening en patching

Niveau	Mens	Procedures & Organisatie	Techniek
4	MHPM 1	MHPPO 1 t/m 11	MHPT 1 t/m 2
3	MHPM 1	MHPPO 1 t/m 11	MHPT 1 t/m 2
2	MHPM 1	MHPPO 1 t/m 5, 7, en 11	MHPT 1 t/m 2
1	MHPM 1	MHPPO 1 t/m 5, 7, en 11	MHPT 1 t/m 2

Mens	MHPM1	Voor bewustwording, gedragsregels en training van bedienaars, beheerders en overig ondersteunend personeel zowel van RWS als die van Opdrachtnemer wordt verwezen naar de maatregelenset "bewustwording en training".
Procedures & Organisatie	MHPPO1	Opdrachtnemer dient over een geborgde procedure en voorzieningen te beschikken voor detectie van en preventie tegen malware waarbij de anti-malware software en signature updates dagelijks dienen plaats te vinden.
	MHPPO2	Opdrachtnemer dient over een geborgde procedure te beschikken voor het (laten) hardenen van ICS/SCADA en overige ondersteunde ICT-systemen en datanetwerkelementen door: • niet noodzakelijke datanetwerkservices uit te zetten; • het verwijderen (patchen) van bekende kwetsbaarheden; • alle poorten die niet nodig zijn te deactiveren/blokkeren; • alle default "access points" te verwijderen; • De default accounts uit te schakelen conform het wachtwoord policy; • Indien beschikbaar gebruik te maken van de security opties van leveranciers.
	MHPPO3	Opdrachtnemer draagt zorg voor en ziet erop toe dat removable apparatuur en ICT systemen die gekoppeld worden aan de ICS/SCADA en ondersteunende ICT-systemen en netwerkomgeving waar mogelijk zijn voorzien van alle recente beveiligingsupdates en patches.
	MHPPO4	Opdrachtnemer dient over een geborgde procedure te beschikken waarmee tijdig gereageerd kan worden op technische kwetsbaarheden van de in gebruik zijnde ICS/SCADA en ondersteunende ICT-systemen en netwerken.
	MHPPO5	Opdrachtnemer dient over een geborgde procedure te beschikken voor patching waarin taken, bevoegdheden en verantwoordelijkheden van de betrokken rolhouders zijn beschreven inclusief de van toepassing zijn doorlooptijden.
	MHPPO6	Bij patches en anti-virusupdates, die vanaf Internet worden gedownload, wordt gecontroleerd dat met de juiste Internetsite contact is gelegd en/of wordt het gebruik van digitale

		handtekeningen geverifieerd met gebruik van een betrouwbare certificate authority.
	MHPPO7	Opdrachtnemer dient over een geborgde procedure te beschikken die er voor zorgt dat voor kritieke patches binnen 48 uur na melding, gerekend vanaf eerstvolgend werkdag een risicoanalyse wordt uitgevoerd en voorzien is van een implementatieadvies. Voor niet kritieke patches is de doorlooptijd voor uitvoering van risicoanalyse en implementatieadvies maximaal twee maanden. De patches worden na instemming met het implementatieadvies door Opdrachtgever conform het advies door Opdrachtnemer geïmplementeerd.
	MHPPO8	Indien patches om bepaalde redenen bewust niet worden doorgevoerd, dient deze afweging schriftelijk te worden vastgelegd voorzien van een risicoafweging.
	MHPPO9	Opdrachtnemer dient te beschikken over een herstelplan na een besmetting met malware, waaronder alle nodige voorzieningen voor back-up, kopieën van gegevens en programmatuur evenals herstelmaatregelen.
	MHPPO10	Indien haalbaar dienen zowel intern ontworpen als ingekochte systemen en applicaties jaarlijks op fouten in code, malware of generieke beveiligingskwetsbaarheden te worden getest.
	MHPPO11	Opdrachtnemer draagt zorg voor en ziet erop toe dat gegevensdragers, beheer- en onderhoudsapparatuur altijd vooraf op virussen gecontroleerd worden voordat deze worden gekoppeld aan ICS/SCADA of overige ondersteunende ICT-systemen en lokale objectdatanetwerken.
Techniek	MHPT1	Indien mogelijk dienen ICS/SCADA-systemen zodanig (her)geconfigureerd te worden dat auto-run van USB-tokens, USB harde schijven, mounted network shares of andere removable media niet wordt toegestaan.
	MHPT2	Antimalware voorzieningen moeten in afstemming met RWS-CIV ingezet worden.

3.6 Maatregelen Logging en Monitoring

Niveau	Mens	Procedures & Organisatie	Techniek
4	LMM1	LMPO1 t/m 5	LMT1 t/m 5
3	LMM1	LMPO1 t/m 5	LMT1 t/m 5
2	LMM1	LMPO1 t/m 4	LMT1 t/m 4
1	LMM1	LMPO1 t/m 4	LMT1 t/m 4

Mens	LMM1	Voor bewustwording, gedragsregels en training van bedienaars, beheerders en overig ondersteunend personeel zowel van RWS als die van Opdrachtnemer wordt verwezen naar de maatregelenset "bewustwording en training".
Procedures & Organisatie	LMPO1	De handelingen van medewerkers, beheerders, meldingen vanuit systemen en eventlogs dienen te worden vastgelegd in audit-logbestanden waarbij een logregel minimaal de volgende gegevens bevat: • de gebeurtenis zelf; • een tot een natuurlijk persoon herleidbare gebruikersnaam of een (systeem)-ID • het object waarop de handeling werd uitgevoerd • het resultaat van de handeling • de datum en het tijdstip van de gebeurtenis • optioneel de identiteit van het werkstation of de locatie • een doorlopende en unieke nummering per logregel
	LMPO2	Opdrachtnemer draagt zorg voor en ziet er op toe dat: • de loggegevens in een apart bestand worden weggeschreven en opgeslagen die alleen toegankelijk is voor speciaal hiertoe geautoriseerd personeel; • de logbestanden van ICS/SCADA, beveiliging en ondersteunende ICT-systemen en -netwerkelementen beschermd worden voor verlies of wijziging; • van systemen met logvoorzieningen de logbestanden een maand bewaard worden; • loggegevens die gebruikt zijn voor incidentonderzoeken conform de bewaartermijnen die de (feiten)onderzoekers aangeven langer worden bewaard.
	LMPO3	Voor de levering van logbestanden aan derden dient de RWS Objectverantwoordelijke/-beheerder expliciet toestemming te verlenen.
	LMPO4	Opdrachtnemer draagt zorg voor een geborgde procedure die opvolging geeft aan meldingen uit de centrale logging en monitoringsvoorzieningen en proces vanuit RWS-CIV.
	LMPO5	Opdrachtnemer heeft de afhankelijkheid van de geautomatiseerde gegevensoverdrachten tussen het ICS/SCADA en gekoppelde ICT-componenten in kaart gebracht. Een geborgde procedure is aanwezig voor het bewaken dat alle benodigde gegevens op tijd worden overgedragen en dat hierin geen fouten ontstaan.

Techniek	LMT1	Logfiles van ICS/SCADA, beveiliging en ondersteunende ICT-systemen en- netwerkelementen dienen in CSV-formaat opgeleverd te kunnen worden.
	LMT2	In een logregel worden in geen geval gevoelige gegevens opgenomen. Dit betreft onder meer gegevens waarmee de beveiliging doorbroken kan worden zoals wachtwoorden, inbelnummers, e.d.
	LMT3	Het overschrijven of verwijderen van logregels- en bestanden wordt gelogd in een nieuw aangelegde log.
	LMT4	De loginstellingen en -bestanden worden zodanig beschermd dat deze niet gewijzigd of gewist kunnen worden door ongeautoriseerden.
	LMT5	Voor kritieke ICS/SCADA en overige ondersteunende ICT-systemen moet in afstemming met en op verzoek van Opdrachtgever beveiligingsspecifieke logsystemen worden ingezet.

3.7 Maatregelen Bewustwording en Training

Niveau	Medewerker	Manager
4	BTME1 t/m 22	BTMA1 t/m 6
3	BTME1 t/m 22	BTMA1 t/m 6
2	BTME1 t/m 22	BTMA1, 2, 3, 5 en 6
1	BTME1 t/m 22	BTMA1, 2, 5 en 6

Medewerker	BTME1	Bedienaars, beheerders en overig ondersteunend personeel zijn verplicht om de door het management aangegeven en beschikbaar gestelde periodieke Cybersecurity cursussen, trainingen, E-Learning modulen te volgen en hiernaar te handelen.
	BTME2	Iedere medewerker is zich bewust van de voor hem/haar van toepassing zijnde taken, bevoegdheden en verantwoordelijkheden voor beveiliging en weet dat gebruikers- en systeemactiviteiten worden gelogd.
	BTME3	Bedienaars, beheerders en overig ondersteunend personeel nemen de Cybersecurity beveiligingsinstructies strikt in acht en zijn verantwoordelijk voor hun aandeel in de beveiliging van het object.
	BTME4	Bedienaars, beheerders en overig ondersteunend personeel doen aan sociale controle, spreken elkaar aan op ontoelaatbaar en risicovol gedrag en bespreken geconstateerde onregelmatigheden in het periodieke werkoverleg met het eigen management/Objectbeheerder.
	BTME5	Bij het constateren van een beveiligingsincident dienen bedienaars, beheerders en overig ondersteunend personeel dit direct als een beveiligingsincident te melden bij de verantwoordelijke objecteigenaar/ -beheerder. Er is sprake van een beveiligingsincident bij het manifest worden van een (dreigend of reeds opgetreden) beveiligingsrisico als gevolg van een (mogelijke) overtreding van het beveiligingsbeleid of onregelmatigheid. Voorbeelden van beveiligingsincidenten zijn: - verlies van dienst, apparatuur of voorzieningen; - systeemstoringen of overbelasting; - menselijke fouten die leiden tot functionele verstoring of uitval van systemen; - inbreuk op fysieke en logische beveiligingsvoorzieningen van het object; - inbreuk op de bediening en beheer; - ongeautoriseerde systeemwijzingen;

		- niet-naleving van beleid of gedragsregels; - virusmeldingen; - verlies of diefstal van bedrijfsmiddelen; - oneigenlijk gebruik van bevoegdheden; - vandalisme, moedwillige beschadiging.
	BTME6	Afwijkend systeemgedrag kan een aanwijzing zijn voor een aanval op de beveiliging of voor een daadwerkelijk beveiligingslek en behoort daarom altijd direct te worden gerapporteerd als een beveiligingsincident en gemeld aan de Objectverantwoordelijke/-beheerder.
	BTME7	Bedienaars, beheerders en overig ondersteunend personeel moeten bij het constateren van eventuele onregelmatigheden dan wel onveilige situaties die handelingen verrichten of maatregelen treffen die verdere uitbreiding van het incident kunnen voorkomen dan wel de schade beperken.
	BTME8	Bedienaars, beheerders en overig ondersteunend personeel gaan zorgvuldig om met de verstrekte persoonsgebonden fysieke toegangmiddelen voor het object en de (systeem, bedien, technische) ruimten hierbinnen en delen deze niet met collega's.
	BTME9	Bedienaars, beheerders en overig ondersteunend personeel creëren geen eigen netwerkkoppelingen op het object en melden dit als een beveiligingsincident als er een zelf aangelegde netwerkkoppeling wordt geconstateerd.
	BTME10	Bedienaars, beheerders en overig ondersteunend personeel nemen de wachtwoordrichtlijn voor de logische toegang tot ICS/SCADA en overige ondersteunende ICT-systemen in acht.
	BTME11	Bedienaars, beheerders en overig ondersteunend personeel koppelen geen mobiele apparatuur of removable media aan de ICS/SCADA, overige ondersteunende ICT-systemen en object netwerken. Uitgezonderd zijn de beheerders die dit alleen na autorisatie van de hiertoe gemandateerde functionaris en uitgevoerde actuele viruscontrole van apparatuur/media mogen doen.
	BTME12	Voor bedienaars, beheerders en overig ondersteunend personeel is toegang tot internet en het gebruik van email vanaf ICS/SCADA en overige daaraan ondersteunende ICT-systemen strikt verboden.
	BTME13	Bedienaars, beheerders en overig ondersteunend personeel mogen de beschikbaar gestelde toegangsmiddelen (tokens, pasjes) tot ICS/SCADA en ondersteunende systemen en –netwerken alleen gebruiken voor het doel waarvoor ze ontworpen zijn. Hierbij mogen de getroffen beveiligingsmaatregelen niet omzeild worden.
	BTME14	Bedienaars, beheerders en overig ondersteunend personeel houden hun accountgegevens strikt geheim; zij gebruiken hun account en uitgegeven autorisaties alleen zelf en staan niet toe dat anderen onder hun account kunnen inloggen. Handelingen zijn altijd te herleiden naar

		de voor dat account geautoriseerde persoon.
	BTME15	Bedienaars, beheerders en overig ondersteunend personeel dienen op ICS/SCADA en de overige ondersteunende ICT systemen en –netwerken de standaard/default/fabrieks accounts en/of wachtwoorden bij ingebruikname te wijzigen conform de wachtwoordrichtlijn van RWS.
	BTME16	Bij het constateren van onregelmatigheden in de logische toegang tot ICS/SCADA en overige ondersteunende ICT-systemen dient iedere medewerker dit onverwijld als een beveiligingsincident te melden bij de Objectverantwoordelijke/-beheerder.
	BTME17	Ongeautoriseerd aan- of afkoppelen van removable apparatuur of usb-sticks aan het netwerk of ICS/SCADA systemen is strikt verboden.
	BTME18	Alleen geautoriseerde medewerkers/beheerders mogen systemen die voorzien zijn van de laatste security updates, patches en actuele viruscontroleprogrammatuur koppelen aan objectdatanetwerken of ICS/SCADA systemen.
	BTME19	Gegevensdragers worden altijd vooraf op virussen gecontroleerd voordat deze worden gekoppeld aan ICS/SCADA of overige ondersteunende ICT-systemen en netwerken.
	BTME20	Incidenten die zich voordoen binnen het wijzigingsproces en afwijkingen van het wijzigingsproces moeten worden gemeld bij de Objectverantwoordelijke/ -beheerder.
	BTME21	Onregelmatigheden, incidenten en storingen binnen het back-up en recovery proces moeten worden gemeld bij de Objectverantwoordelijke/ -beheerder.
	BTME22	Bedienaars, beheerders en overig ondersteunend personeel zorgen ervoor dat onbeheerde ICS/SCADA-systemen en overige ICT-apparatuur – zo mogelijk - wordt gelocked.
Manager	BTMA1	Er dient bewerkstelligd te worden dat bedienaars, beheerders en overig ondersteunend personeel continu bewust worden gemaakt en geschikte training en regelmatige bijscholing krijgen met betrekking tot het beveiligingsbeleid en procedures, voor zover relevant voor hun functie.
	BTMA2	Opdrachtnemer draagt zorg voor en ziet erop toe dat bedienaars, beheerders en overig ondersteunend personeel: • de periodieke Cybersecurity cursussen, trainingen en E-Learningmodulen volgen en een actuele administratie hiervan aanwezig is; • de beschikking hebben over actuele (technische) beheerdocumentatie, gebruikers- en/of installatiehandleidingen voor de ICS/SCADA en overige ondersteunende ICT-systemen en bedrijfsmiddelen; • dat werkzaamheden door gescreend personeel uitgevoerd worden en dat geheimhouding is overeengekomen voor ingehuurd personeel, objectverantwoordelijke/-beheerder bepaalt in welke situaties dit aan de orde is en de vorm waarin; • ingehuurd personeel een geheimhoudingsverklaring heeft ondertekend; • dat bedienaars, beheerders en overig ondersteunend personeel van zowel RWS als die van externe partijen alle

		bedrijfsmiddelen, ICS/SCADA en overige ondersteunende ICT-systeemdocumentatie van RWS die ze in hun bezit hebben retourneren bij beëindiging van hun dienstverband, contract of overeenkomst; • dat de toegangsrechten van alle bedienaars, beheerders en overig ondersteunend personeel van zowel RWS als die van externe partijen de verstrekte toegangsmiddelen direct worden geblokkeerd bij beëindiging van het dienstverband, het contract of na wijziging van de overeenkomst worden aangepast; • dat calamiteitenplannen worden betrokken in de bewustwordingstrainingen, trainingen en testactiviteiten; • gebruik van de centraal beschikbaar gestelde technische middelen voor fysieke en logische toegang op medewerkers niveau.
	BTMA3	De objectverantwoordelijke/-beheerder/verantwoordelijk management bespreekt en evalueert in de periodieke werkoverleggen de beveiligingsincidenten van de afgelopen periode, hoe op dergelijke incidenten is geacteerd, hoe het beter kan en hoe deze in de toekomst vermeden kunnen worden alsmede de feedback van de bewustwordingsactiviteiten en specifieke trainingen.
	BTMA4	Opdrachtnemer ziet erop toe dat werknemers en ingehuurd personeel zich houden aan de gedragsregels voor beveiliging zoals fysieke en logische toegang en melding van beveiligingsincidenten. Voor zover controle op naleving van gedragsregels mogelijk is, wordt hiervoor een controleprogramma met steeksproefsgewijze controles vastgesteld en uitgevoerd.
	BTMA5	Opdrachtnemer besteedt en bespreekt Cybersecurity in de functioneringsgesprekken met medewerkers en beheerders en maakt hiertoe opleidingsplannen waarbij wordt toegezien op uitvoering.
	BTMA6	Opdrachtnemer dient bij het constateren van onregelmatigheden in de logische toegang tot ICS/SCADA en overige ondersteunende ICT-systemen uit voorzorg in dergelijke situaties het betreffende account en wachtwoord altijd te laten wijzigen.

3.8 Maatregelen gecontroleerd wijzigen

Niveau	Mens	Procedures & Organisatie	Techniek
4	GWM 1	GWPO 1 t/m 9	GWT 1 en 2
3	GWM 1	GWPO 1 t/m 9	GWT 1 en 2
2	GWM 1	GWPO 1 t/m 3, 5, 7 en 9	GWT 1 en 2
1	GWM 1	GWPO 1 t/m 3, 5, 7 en 9	GWT 1 en 2

Mens	GWM1	Voor bewustwording, gedragsregels en training van bedienaars, beheerders en overig ondersteunend personeel zowel van RWS als die van Opdrachtnemer wordt verwezen naar de maatregelenset "bewustwording en training".
Procedures & Organisatie	GWPO1	Opdrachtnemer dient over een geborgde procedure te beschikken voor het (laten) inventariseren en registreren van alle Configuration Items (CI's) met bijbehorende settings/configuraties in een Configuration Management Database (CMDB) die actueel wordt gehouden.
	GWPO2	Opdrachtnemer dient over een geborgde wijzigingsprocedure te beschikken voor het doorvoeren van wijzigingen aan ICS/SCADA en ondersteunende ICT systemen, beveiliging- en netwerkomgeving. Alle wijzigingen worden conform de wijzigingsprocedure geregistreerd.
	GWPO3	Wijzigingen mogen alleen door geautoriseerde beheerders worden aangevraagd en uitgevoerd.
	GWPO4	Voor wijzigingen aan ICS/SCADA en overige ondersteunende ICT-systemen dient altijd een risicoafweging te worden gemaakt. De risicoafweging en de hieruit voortvloeiende maatregelen moeten voordat uitvoering van werkzaamheden plaatsvindt zijn goedgekeurd door de Objectverantwoordelijke/ -beheerder.
	GWPO5	De wijzigingen worden bijgewerkt in de CMDB en jaarlijks worden de settings/configuraties van ICS/SCADA en overige ondersteunende ICT-systemen in de CMDB vergeleken met de daadwerkelijke en de CMDB indien nodig bijgewerkt.
	GWPO6	Wijzigingen in ICS/SCADA en overige ondersteunende ICT-systemen moeten indien mogelijk vooraf aan de implementatie in productie te worden getest om te bewerkstelligen dat er geen nadelige gevolgen zijn voor de functionaliteit of beveiliging van de organisatie. Indien haalbaar moet voor ICS/SCADA en overige ondersteunende ICT-systemen controle worden uitgevoerd voor de authenticiteit/integriteit van de software voorafgaande aan de implementatie op operationele systemen.

	GWPO7	Opdrachtnemer draagt zorg voor en ziet erop toe dat noodwijzigingen die buiten het reguliere wijzigingsproces om zijn aangebrachte als gevolg van incidenten met een bijzonder (urgent) karakter achteraf alsnog de gebruikelijke procedures volgen en de CMDB administratie wordt bijgewerkt.
	GWPO8	Voor elke wijziging is een terugval scenario opgesteld waarin is vastgelegd waaruit de terugval bestaat, onder welke condities tot een terugval wordt overgegaan en wie daartoe kan besluiten. Kort na de implementatie van een wijziging dient een test plaats te vinden om te verifiëren dat de wijziging is gelukt of dat op het terugval scenario moet worden overgegaan.
	GWPO9	Opdrachtnemer ziet erop toe dat naar aanleiding van een wijziging uitgeschakelde beveiligingsmaatregelen weer zijn geactiveerd alvorens de wijziging te sluiten.
Techniek	GWT1	Alle CI's met bijbehorende settings/configuraties en de wijzigingen hierop worden geregistreerd in een CMDB.
	GWT2	Voor zover beschikbaar wordt gebruik gemaakt van testvoorzieningen.

3.9 Maatregelen beheer en onderhoud

Niveau	Mens	Procedures & Organisatie	Techniek
4	BOM 1	BOPO 1 t/m 9	BOT 1 t/m 2
3	BOM 1	BOPO 1 t/m 9	BOT 1 t/m 2
2	BOM 1	BOPO 1 t/m 4, 6 en 9	BOT 1 t/m 2
1	BOM 1	BOPO 1 t/m 4, 6	BOT 1 t/m 2

Mens	BOM1	Voor bewustwording, gedragsregels en training van bedienaars, beheerders en overig ondersteunend personeel zowel van RWS als die van Opdrachtnemer wordt verwezen naar de maatregelenset "bewustwording en training".
Procedures & Organisatie	BOPO1	Opdrachtnemer draagt zorg voor het evalueren van risico's en effectieve werking van de getroffen beheersmaatregelen voor beveiliging in het kader van life-cycle management.
	BOPO2	Opdrachtnemer draagt zorg voor en ziet erop toe dat waar nodig in de beheer en onderhoudscontracten met onderaannemers: • Geheimhouding opgenomen is; • Training- en opleidingsvereisten alsmede overige benodigde certificeringen beschreven zijn; • Welke screening van personeel nodig is (bijv. VOG); • Beschreven is dat de RWS gedragsregels voor beveiliging en communicatie strikt in acht moeten worden genomen; • Een concrete procedure bekend is en is vastgelegd met betrekking tot incidentresponse en voor escalatieprocedures met de leverancier (7*24) • De procedures voor fysieke toegang tot objecten en ruimten en de logische toegang tot systemen vastgelegd zijn; • De registratie en rapportage van beveiligingsincidenten geregeld is; • Beschreven is dat handelingen van medewerkers en systemen gelogd en gemonitord worden; • Beschreven is dat loggegevens van RWS beschermd moeten worden tegen verlies en wijziging en niet voor andere doeleinden gebruikt mogen worden; • De bewaartermijnen van back-ups en logbestanden geregeld is; • De procedures voor aan- en afkoppeling van apparatuur beschreven zijn; • De netwerkaansluitvoorwaarden overeengekomen zijn; • De procedure "Toegang Derden" van de CIV gevolgd moet worden voor de logische toegang tot netwerken en systemen. De tijdelijke toegang tot de systemen ten behoeve van ondersteuning dient geautoriseerd te zijn en handelingen dienen te worden gelogd. • Beschreven is dat onderhoud en wijzigingen op ICS/SCADA systemen alleen uitgevoerd mogen worden vanaf systemen die voorzien zijn van de laatste security update's en patches en actuele viruscontroleprogrammatuur; • Beschreven is dat netwerkkoppelingen op objectnetwerken altijd en strikt via de beveiligde centrale voorzieningen van RWS verlopen;

		• Welke netwerkkoppelingen er toegestaan zijn; • Beschreven is dat logging en monitoring van netwerkverkeer plaatsvindt via de centrale voorzieningen van RWS; • Beschreven is dat wijzigingen conform het wijzigingsproces van RWS uitgevoerd mogen worden; • Beschreven is dat patchen strikt conform de Patchrichtlijnen en doorlooptijden van RWS uitgevoerd moeten worden; • Beschreven is hoe omgegaan moet worden met alarmvoorzieningen van het object en de alarmopvolging; • Beschreven is dat het ongeautoriseerd koppelen van removable media en usb sticks aan het RWS of objectnetwerken strikt verboden is.
	BOPO3	Opdrachtnemer draagt waar nodig zorg voor en ziet erop toe dat in de SLA/DAP afspraken met Opdrachtgever en onderaannemers worden gemaakt over: • De dienstverlening en functionaliteit; • Tijd van openstelling, bereikbaarheid en reactietijd, incident melding en afhandeling; • Wat wordt verstaan onder een storing, beveiligingsincident en zwakke plek; • Het classificeren van incidenten en de geldende maximale oplossingsduur; • Escalatieprocedures (horizontaal en verticaal) bij overschrijding van de overeengekomen normtijden inclusief namen en telefoonnummers. • Het indienen en afhandelen van wijzigingsverzoeken; • Directe melding van beveiligingsincidenten; • Noodprocedures met zowel interne als externe leveranciers voor ICT en ICS/SCADA systemen; • Ondersteuning bij calamiteiten en beschikbaarheid van reserve onderdelen en apparatuur; • De communicatielijnen (wie, wanneer en waarover); • Hoe de fysieke en logische toegang tot systemen en ruimten geregeld is; • De bewaartermijn van back-ups en logbestanden; • Rapportages die verplicht zijn zoals die voor beveiligingsincidenten en welke frequentie daarvoor geldt; • Het signaleren van nieuwe kwetsbaarheden en tijdig uitbrengen van patches door de leverancier; • Het testen van software-updates alvorens deze in productie gaan; • Evaluatie en actualisatie;
	BOPO4	Opdrachtnemer draagt zorg voor de beschikbaarheid en onderhoud van (technische) beheerdocumentatie, gebruikers- en/of installatiehandleidingen voor de ICS/SCADA systemen alsmede procedures voor het opnieuw opstarten en herstellen van het systeem in geval van systeemstoringen.
	BOPO5	Opdrachtnemer draagt zorg voor een geborgde procedure die de personele toegang van al het vast onderhoudspersoneel voorafgaand de uitvoering van werkzaamheden regelt. Hiervoor kan de onderstaande "Good Practice" "**Maatregelen personele toegang**" gebruikt worden.
	BOPO6	Opdrachtnemer houdt toezicht op de operationele uitvoering en naleving van: • de uitvoering van wijzigingen conform de wijzigingen procedure; • de procedure voor fysieke toegang; • de procedure voor logische toegang; • patching, de back-up procedure en bewaartermijnen; • incidentmanagement, log- en incidentrapportages en de analyse

		hiervan.
	BOPO7	Opdrachtnemer draagt zorg voor een geborgde procedure voor incidentrespons en continuïteit van de ICT en ICS/SCADA dienstverlening ingeval van incidenten en calamiteiten. De volgende informatie van ICS/SCADA en overige ondersteunende ICT-systemen dient actueel en beschikbaar te zijn voor herstel na een calamiteit: -type en merk ICS/SCADA middel -Formaat -Locatie -Back-up en licenties -Software en hardware configuratie -Vervangingsinstructie/procedure
	BOPO8	Opdrachtnemer draagt zorg voor en ziet erop toe dat het objectspecifieke continuïteitsplan aanhaakt op het regionale calamiteitenplan van Opdrachtgever en wordt meegenomen in de periodieke oefeningen.
	BOPO9	Opdrachtnemer dient jaarlijks de opzet, bestaan en werking van de getroffen maatregelen te (laten) onderzoeken, evalueren en bij te stellen. De resultaten dienen te worden gerapporteerd aan Opdrachtgever.
Techniek	BOT1	Voor de fysieke toegang (ICT-deel) van bedienaars, beheerders en overig ondersteunend personeel zowel van RWS als die van externe partijen tot objecten en de ruimten hierbinnen wordt gebruikt gemaakt van de PDC producten en diensten van RWS-CIV en RWS-CD.
	BOT2	Voor (remote) logische toegang van bedienaars en beheerders tot het netwerk en ICS/SCADA systemen wordt gebruikt gemaakt van de PDC producten en diensten van RWS-CIV.

Good Practice - Maatregelen personele toegang

De Opdrachtnemer dient te verzorgen dat al het vast onderhoudspersoneel voorafgaand aan zijn/haar operationele inzet en vervolgens steeds binnen een

periode van twee jaar:

- een persoonlijke geheimhoudingsverklaring ondertekent en overhandigt aan de Opdrachtgever;

- zich daarbij legitimeert en een goed gelijkende pasfoto overhandigt aan de Opdrachtgever;

- een Verklaring Omtrent Gedrag (VOG) bezit en een kopie daarvan aan de Opdrachtgever overlegt welke is gerelateerd aan de beoogde Werkzaamheden.

Hangende de aanvraag voor een VOG kan volstaan worden met een eigen verklaring van de betreffende medewerker gedurende een periode van maximaal zes weken

welke niet verlengd kan worden.

De Opdrachtnemer dient er op toe te zien dat al het onderhoudspersoneel dat niet structureel verschijnt:

- Zich legitimeert;

- In specifieke gevallen op eerste verzoek van de Opdrachtgever bereid is een eigen verklaring en een geheimhoudingsovereenkomst te ondertekenen.

De Opdrachtnemer dient al haar medewerkers nadrukkelijk te informeren over het feit dat het doorgeven van informatie over de werking, inrichting, organisatie rondom de objecten in welke vorm dan ook NIET zal geschieden dan na uitdrukkelijke toestemming van de Opdrachtgever.

Iedere geconstateerde afwijking van bovenstaande eisen dient door de Opdrachtnemer te worden behandeld als security incident.

3.10 Maatregelen Back-ups

Niveau	Mens	Procedures & Organisatie	Techniek
4	BUM 1	BUPO 1 t/m 5	BUT 1
3	BUM 1	BUPO 1 t/m 5	BUT 1
2	BUM 1	BUPO 1 t/m 5	BUT 1
1	BUM 1	BUPO 1 t/m 3	BUT 1

Mens	BUM1	Voor bewustwording, gedragsregels en training van bedienaars, beheerders en overig ondersteunend personeel zowel van RWS als die van Opdrachtnemer wordt verwezen naar de maatregelenset "bewustwording en training".
Procedures & Organisatie	BUPO1	Dagelijks dient automatisch een back-up gemaakt te worden van alle in het systeem aanwezige dynamische en configuratiegegevens welke back-up op het systeem zelf of op de hoofdlocatie van het systeem mag worden opgeslagen. De juiste verwerking van de back-up wordt bewaakt op basis van het back-up log. Deze back-ups worden een week bewaard.
	BUPO2	De integriteit en beschikbaarheid van de laatste drie versies van de ICS/SCADA systemen, programmatuur en besturingssystemen dient gewaarborgd te worden door het maken en testen van systeemimages/back-ups, conform een geborgde procedure: • systeemimages/back-ups worden gemaakt na iedere (functionele) systeemwijziging en wanneer wijzigingen uitblijven wordt de systeemimage/back-up van de laatste versie op jaarbasis vernieuwd; • Deze back-ups worden opgeslagen op een locatie die zich op zodanige afstand bevindt dat geen schade aan de back-up kan worden aangericht als een calamiteit zich voordoet op de locatie waar het systeem zich bevind; • Back-ups en de ruimte waarin ze zijn opgeslagen behoren fysiek goed te worden beschermd volgens dezelfde normen die gelden voor de hoofdlocatie en zijn alleen toegankelijk voor bevoegden; • Back-ups worden bewaard tot het moment van uitdienstname van betreffend systeem.
	BUPO3	Er bestaan gedocumenteerde herstelprocedures en volledige en actuele registers van back-up kopieën.
	BUPO4	Herstelprocedures moeten jaarlijks worden gecontroleerd en getest, om te waarborgen dat ze doeltreffend zijn, dat ze werken en dat ze kunnen worden uitgevoerd binnen de daarvoor overeengekomen tijd. Jaarlijks wordt een recovery test gedaan om te zien of de media nog leesbaar is. Herstelprocedures zijn onderdeel van de disaster recovery planning.
	BUPO5	Door Opdrachtnemer worden maandelijks de gemelde incidenten en storingsmeldingen inzake back-up geëvalueerd en waar nodig

		maatregelen getroffen.
Techniek	BUT1	Benodigde voorzieningen voor het back-up en restoreproces worden in overleg met de Opdrachtgever ingevuld.

Bijlage A: Wachtwoord Richtlijn

Er is een wachtwoordbeleid geïmplementeerd voor de ICS/SCADA systemen die het achterhalen van wachtwoorden economisch onrendabel en praktisch onhaalbaar maakt. Eindgebruikers en beheerders leven dit wachtwoordbeleid na. De "factsheet wachtwoorden" maakt integraal onderdeel uit van de Wachtwoord Richtlijn.

De eisen aan een wachtwoord zijn als volgt:

- Lengte: wachtwoorden bestaan minimaal uit 8 karakters voor gebruikers en minimaal 15 karakters voor beheerders;
- Sterkte: wachtwoorden moeten minimaal bestaan uit een combinatie van cijfers, hoofd- en kleine letters en leestekens;
- Hergebruik van hetzelfde wachtwoord op vervangingsmomenten is niet toegestaan;
- De standaard/default account en wachtwoord wordt uitgeschakeld of na eerste gebruik tijdens installatie gewijzigd;
- Na de initiële installatie van een IA- of ICT-component mag er geen default account/wachtwoordcombinaties meer aanwezig zijn in de component.

Voor de hieronder genoemde accounttypen dient de standaard fabrieksaccount met bijbehorend wachtwoord altijd gewijzigd te worden door een persoonlijk account en wachtwoord. Tevens dient voor de onderkende accounttypen de aangegeven duur voor wachtwoordvervanging alsmede de wachtwoordlengte aangehouden te worden. Bij (legacy) systemen en procestoepassingen waar dit niet mogelijk is, moet een risico-inschatting worden gemaakt en compenserende maatregelen worden getroffen. De afwijkingen worden gedocumenteerd.

De voorschriften rondom accounts en wachtwoorden voor kantoorautomatiseringstoepassingen zijn ter verkrijgen bij de afdeling IV - Security Center van RWS-CIV.

Onderkend worden de volgende typen accounts voor ICS/SCADA met bijbehorende eisen:

Standaardaccount fabrikant: Standaard accounts en -wachtwoorden die toegepast worden in ICT-producten van fabrikanten worden gewijzigd.

Alle accounts dienen in een onderstaande **account-type** te worden ingedeeld en te voldoen aan de eisen die aan het betreffende type account gesteld worden:

SCADA-Operatoraccount
Een persoonlijk account dat wordt gebruikt voor de bediening van SCADA systemen
Soort: persoonsgebonden (terug te herleiden naar een individu)
Wachtwoord vervanging: 90 dagen
Wachtwoordlengte: min. 15 karakters

SCADA-applicatiebeheeraccount
Een persoonlijk account dat wordt gebruikt om de applicatie op het SCADA systemen te beheren
Soort: persoonsgebonden (terug te herleiden naar een individu)
Wachtwoord vervanging: 30 dagen
Wachtwoordlengte: min. 15 karakters

SCADA-Systeemaccount (service/applicatie account)
Een account dat ervoor zorg draagt dat een applicatie zonder menselijke interventie applicatieopdrachten kan uitvoeren onder speciale rechten.
Soort: service
Wachtwoord vervanging: 365 dagen
Wachtwoordlengte: min. 15 karakters

SCADA-Administratoraccount
Een persoonlijk account dat op de systemen volledig beheer heeft d.m.v. administrator rechten.
Soort: persoonsgebonden (terug te herleiden naar een individu)
Wachtwoord vervanging: 30 dagen
Wachtwoordlengte: min. 15 karakters

Kantoorautomatiseringsaccount (KA-account)
Het persoonlijke gebruikers account waarmee men kan werken op de Rijkswaterstaat Kantoorautomatiseringsomgeving.
Soort: persoonsgebonden (terug te herleiden naar een individu)
Wachtwoord vervanging: 90 dagen
Wachtwoordlengte: min. 8 karakters

Bijlage B: Factsheet Wachtwoorden

Factsheet wachtwoorden voor gebruikers van IA systemen

Aanleiding

Steeds meer Industriële Automatiseringssystemen worden aan andere computersystemen of netwerken gekoppeld. Daarmee neemt de kans toe dat deze systemen vanaf een andere computer of netwerk worden gehackt, met mogelijk verstrekkende gevolgen.

Door het handhaven van fabriekswachtwoorden of eenvoudig te kraken wachtwoorden op IA systemen kunnen kunstwerken en verkeerssystemen relatief eenvoudig worden overgenomen door hackers, als ze via internet of fysiek toegang kunnen krijgen tot de IA systemen.

Toepassing factsheet

In deze factsheet zijn de richtlijnen opgenomen, die binnen Rijkswaterstaat gelden voor het gebruik en wijzigen van sterke wachtwoorden in IA systemen. Ook zijn richtlijnen opgenomen hoe de wachtwoorden moeten worden beschermd.

De richtlijnen zijn niet altijd implementeerbaar in bestaande IA systemen. Als dit het geval is moet een risicoanalyse worden gemaakt door de systeemeigenaar en moeten aanvullende maatregelen worden getroffen om risico's tot een aanvaardbaar niveau terug te brengen. Bijlage 1 geeft door middel van een risico reductie overzicht aan met welke risico's rekening is gehouden in de richtlijn en welke maatregelen daartegen moeten worden getroffen.

Checklist eigenschappen sterke wachtwoorden

1. een wachtwoord moet uit minimaal 15 karakters bestaan
2. een wachtwoord moet minimaal drie van de volgende 5 soorten karakters bevatten:
    a. gewone letters
    b. hoofdletters
    c. getallen
    d. punctuatie (bijvoorbeeld: ";'?,!)
    e. speciale karakters (bijvoorbeeld: @#$%^&*<>~+=)
3. het default account en wachtwoord van de applicatie mogen niet worden gehandhaafd en moeten beiden bij ingebruikname van de applicatie direct worden gewijzigd en verwijderd.

Zwakke wachtwoorden hebben de volgende eigenschappen:

- het wachtwoord bevat minder dan 15 karakters (en kan door een hacker binnen enkele uren worden gekraakt door willekeurige karakters uit te proberen)
- het wachtwoord is terug te vinden in een woordenboek (en kan door een hacker makkelijk worden geraden met behulp van een woordenboekaanval)
- het wachtwoord is voor de gebruiker makkelijk te bedenken (en voor de hacker dus makkelijk te raden):
    a. namen van familieleden, huisdieren, vrienden, collega's, stripfiguren, etc.
    b. computer namen en -termen, commando's, naam van de software of hardware, naam van het bedrijf dat het heeft geleverd
    c. woorden als "Rijkswaterstaat"; Amaliasluis, Rotterdam, etc.
    d. geboortedata en andere persoonlijke informatie als adres en telefoonnummers
    e. één van de voorafgaande woorden, gevolgd door een getal (bijvoorbeeld: geheim01, welkom123, GuustFlater13, etc.)
- het default account/wachtwoord is nog steeds in gebruik (en de hacker kent die ook of kan het eenvoudig opzoeken op internet of in de handleiding)

Tips voor het maken en onthouden van sterke wachtwoorden

- maak een wachtwoord dat is gebaseerd op een songtekst of een rijmpje. Zet de eerste letters van ieder woord achterelkaar, en probeer letters door cijfers te vervangen (Bijvoorbeeld: Het rijmpje "Als het regent in mei is april voorbij en leggen alle vogels een ei" wordt "Ahri5i4velavee", waarbij de maanden zijn vervangen door cijfers)
- maak een zin (passphrase) in plaats van een wachtwoord (password). Typ de woorden van een makkelijke zin achterelkaar en vervang woorden of letters door hoofdletters, getallen of lettertekens (Bijvoorbeeld: 03KleineKleutertjesdiezatenopeen###).

Checklist wachtwoordbescherming

1. Gebruik voor je bedrijfs-account niet hetzelfde wachtwoord als voor je privéaccounts (bijvoorbeeld: persoonlijke gmail, facebook, ANWB site, bol.com, etc.).
2. Gebruik binnen het bedrijf niet overal hetzelfde wachtwoord. Gebruik een verschillend wachtwoord voor je gewone desktopomgeving, je bedienplek of je yammer account.
3. Deel je wachtwoord met niemand, tenzij dit is vereist volgens de procedures.
4. Wachtwoorden mogen nooit worden opgeschreven of digitaal worden opgeslagen zonder te zijn vercijferd.
5. Schrijf nooit een wachtwoord in e-mail, chat of ander communicatiemiddel.
6. Praat niet over je wachtwoord, geef geen hints over je wachtwoord aan anderen.

Slechte opslag van wachtwoorden voldoet aan de volgende eigenschappen:

- Het wachtwoord is opgeschreven en ligt binnen handbereik (en de hacker die fysiek binnendringt, kan het wachtwoord ook gemakkelijk vinden).
- Het wachtwoord van 15 karakters is opgeslagen in een applicatie dat is beveiligd met 8 karakters (en daarmee is de wachtwoordlengte gereduceerd tot 8 karakters, want nu hoeft de hacker alleen nog een wachtwoord van 8 karakters te kraken om bij het wachtwoord van 15 karakters te komen).
- Het wachtwoord is opgeslagen in een document op een gezamenlijke schijf of op sharepoint (en de hacker kan het op afstand of ter plaatse ook vinden. Op afstand heeft hij alle tijd om rustig op zoek te gaan).

Tips voor het opslaan van wachtwoorden

- Als het niet anders kan en wachtwoorden moeten toch worden opgeslagen (bijvoorbeeld, omdat dat volgens een veiligheidsprocedure moet), sla een wachtwoord dan op in een fysieke kluis of een speciaal daarvoor ontwikkelde beveiligde applicatie.
- Als een wachtwoord in een kluis wordt opgeslagen, zorg er dan voor dat de sleutel niet eenvoudig te vinden is of dat de kluis op een andere locatie staat.
- Als een wachtwoord in een beveiligde applicatie wordt opgeslagen, dan is er vaak weer een wachtwoord nodig om die applicatie te openen. Daarvoor geldt wederom de wachtwoordrichtlijn.

Checklist wachtwoordwijziging

1. Wachtwoorden moeten regelmatig worden gewijzigd, met een frequentie die is voorgeschreven in de wachtwoordrichtlijn (in de bijlage staat de wachtwoordrichtijn van mei 2013. Op intranet is steeds de meest recente richtlijn te vinden).

Tips voor het wijzigen van wachtwoorden

- Als het afdwingen van wijzigen van wachtwoorden niet automatisch wordt afgedwongen, zorg dan dat het procedureel wordt afgedwongen. Dit kan simpelweg door zelf (bijvoorbeeld op de eerste maandag van de maand) het wachtwoord te wijzigen.

Checklist locken bedien- of beheerstation

1. Als bedienaars of beheerders een bedien- of beheerruimte langere tijd geheel verlaten, dienen zij het bedien- of beheerstation af te sluiten.
2. Als bedienaars of beheerders een bedien- of beheerruimte korte tijd geheel verlaten, dienen zijn het bedien- of beheerstation te locken.

Tips voor het locken van bedien- of beheerstation

- Het is niet nodig om terminals af te sluiten waarop alleen informatie te zien is als camerabeelden of radarbeelden. Het gaat er om dat een onbevoegde geen toegang heeft tot bediening- en beheeromgevingen.
- In sommige situaties mogen of kunnen bedienstations niet worden afgesloten, omdat daardoor juist onacceptabele risico's worden geïntroduceerd. In overleg met de beheerder moet dan worden afgesproken en vastgelegd op welke wijze wordt voorkomen dat onbevoegden toegang krijgen tot de bedien- of beheerruimte als die korte of lange tijd geheel wordt verlaten.

Bijlage 1 Gebruikersmaatregelen

Risicoreductieoverzicht logische toegang IA bediening en beheer vanuit gebruikersperspectief