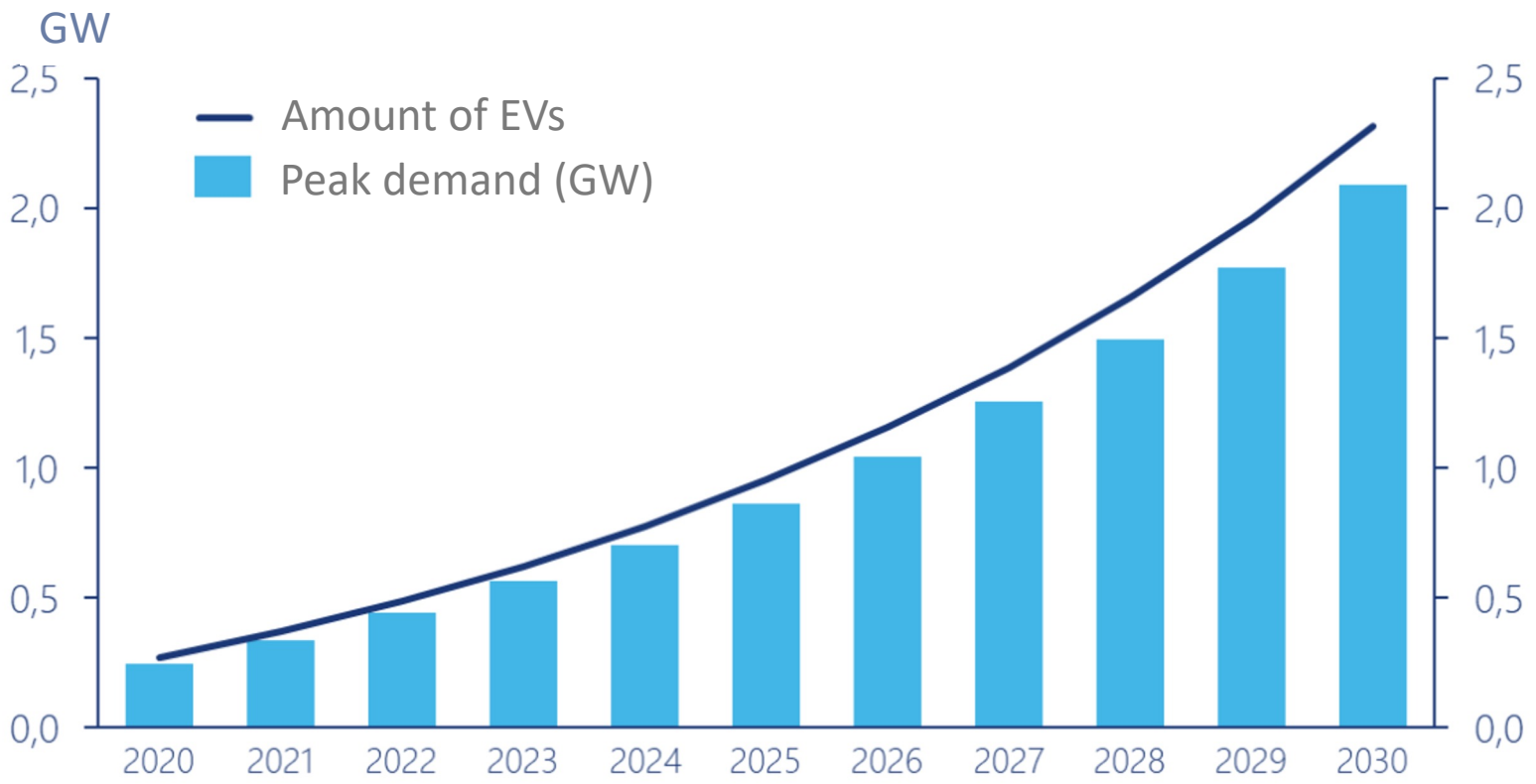
Cyber Security
Energy Management System

Harm van den Brink

Peak demand electric vehicles in NL



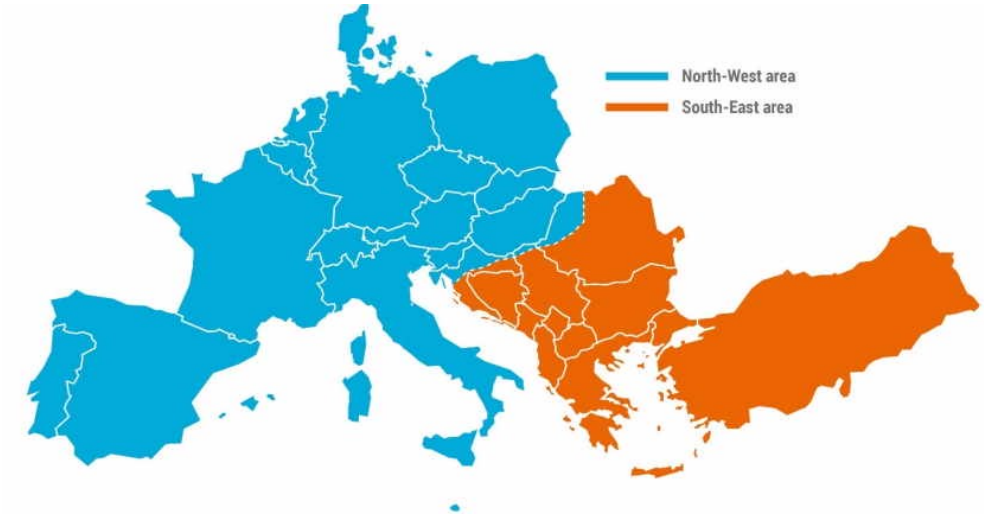
“COMMISSION REGULATION (EU) 2017/1485 establishing a guideline on electricity transmission system operation”

The reserve capacity for FCR (Frequency Containment Reserve) required for the synchronous area shall cover at least the reference incident and, for the CE and Nordic synchronous areas, the results of the probabilistic dimensioning approach for FCR carried out pursuant to point (c);

(b) the size of the reference incident shall be determined in accordance with the following conditions:

(i) for the CE (Continental Europe) synchronous area, the reference incident shall be **3 000 MW in positive direction and 3 000 MW in negative direction**;

Netsplit 8th of January 2021



On 8 January 2021 at 14:05 CET

Tripping of a 400 kV busbar coupler in the substation Ernestinovo (Croatia) by overcurrent protection

Cascading effect: lead to the shifting of electric power flows to neighbouring lines which were subsequently overloaded

https://gridradar.net/en/blog/post/underfrequency_january_2021


Strom-
tankstelle
Ladeplatz

Analysis and advice

The scenarios studied are real and in the future will pose a real risk to the mobility of the Netherlands, the national charging infrastructure and the stability of the electrical grid. An estimate of the potential negative economic impact of such an incident could be as much as approximately 4 billion euros per day for the Netherlands. The social impact of a power failure depends largely on its duration. The social costs associated with power failures range from loss of leisure time to mobility, business activity and even life.

REPORT

Impact of cyber-security risks on the Dutch national charge point infrastructure

National charging infrastructure

Risks within EMS

- Hack
- Human error
- Algorithm (flash crash)
- Normal behavior

A Hack

- Large scale hack could lead to grid instability
- Consumers could face issues like no climate control, no heating/cooling or charging
- Financial losses to company selling EMS solutions, especially when business cases are stacked (Day ahead prices, FCR, aFRR, …)

Cyber Security best practices

Secure development lifecycle

Implement a secure software development lifecycle (SDLC) that incorporates security requirements, threat modeling, and regular security testing at all stages. Train developers in secure coding practices and increase awareness of common vulnerabilities and attack vectors.

Cyber Security best practices

Cyber security by design

Integrate security and privacy features from the *initial design stage*, such as robust encryption for data storage and transmission, secure authentication mechanisms, and privacy-preserving data collection methods. Configure the appliance *securely by default* and avoid relying on users to make security-critical decisions.

Cyber Security best practices

Vulnerability and patch management

Establish a clear process for releasing *firmware updates* and *security patches* to address any discovered vulnerabilities. Make it easy for users to update their appliances by enabling automatic updates or providing clear instructions for manual updates.

Cyber Security best practices

Cyber security by default

Ensure that the *default settings* of the home appliance prioritize security, with strong, unique default passwords and minimal open ports. Disable any unnecessary features that may pose security risks, allowing users to enable them only if required.

Cyber Security best practices

Pentesting, audits and certification

Regularly engage independent third-party security experts to *audit* the security of your home appliances, providing an external perspective on potential vulnerabilities and areas for improvement. Obtain relevant *security certifications* to demonstrate adherence to industry standards and best practices.

Legislation and regulation

Radio Equipement Directive 3.3 (RED 3.3)

Network and Information Security 2 (NIS2)

Network Code on Cyber Security

Technolution

Hoe bepaal je welke maatregelen je moet nemen

Expertsessie EMS workshop:
Cybersecurity voor een betrouwbaar en functionerend EMS

Redefining solutions

Handreiking Cyber security voor smart energy

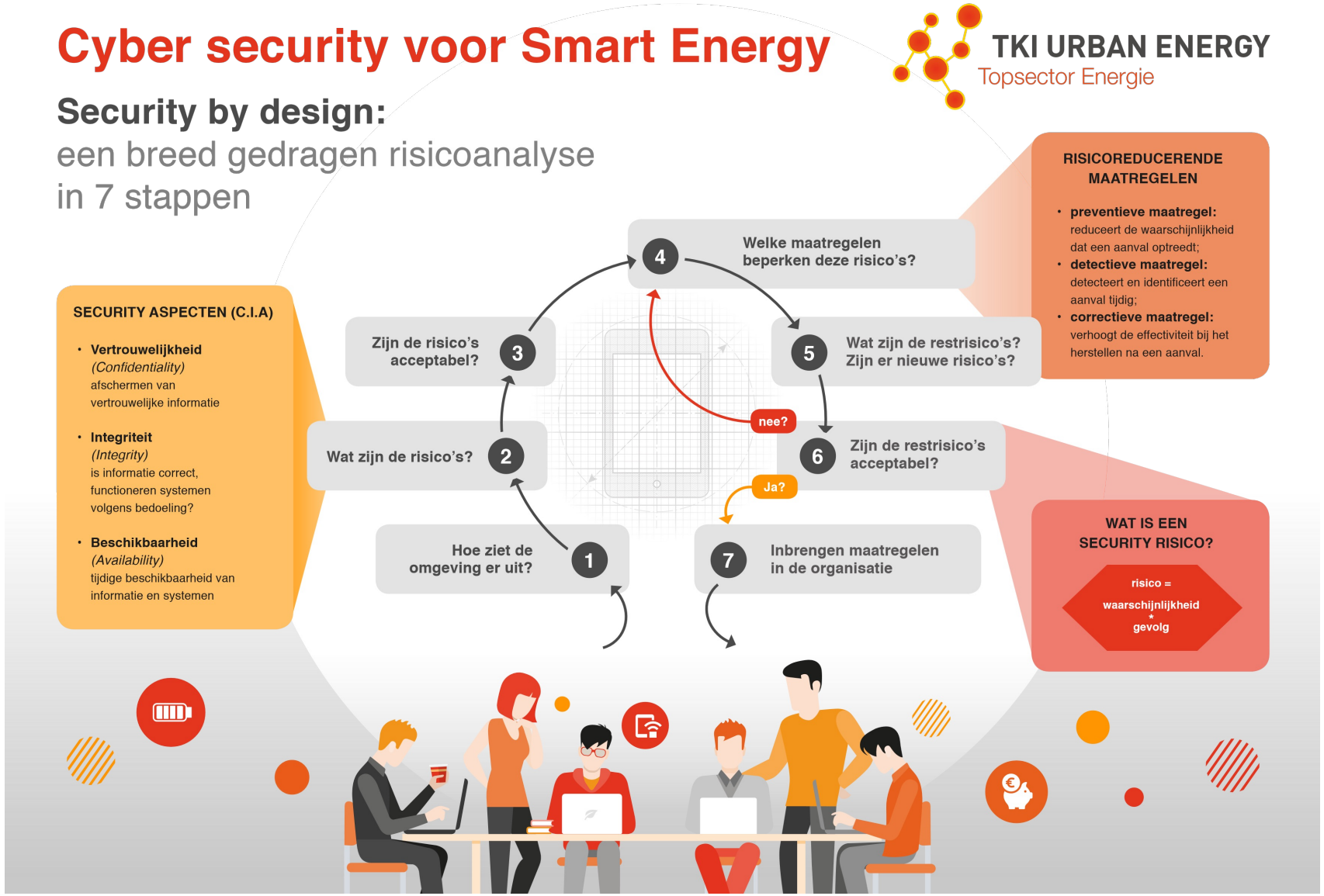
https://www.topsectorenergie.nl/cyber-security-voor-smart-energy

Bepalen van securitymaatregelen

- Risico’s, maatregelen, restrisico’s
- Vastlegging
- Regelmatige controle

- Wat is een risico eigenlijk?

Stappenplan risicoanalyse



identiality)
rmen van
uwelijke informatie

riteit
rity)
rmatie correct,
neren systemen
s bedoeling?

hikbaarheid
ability)
beschikbaarheid van
atie en systemen

acceptabel? 3

Zij

nee?

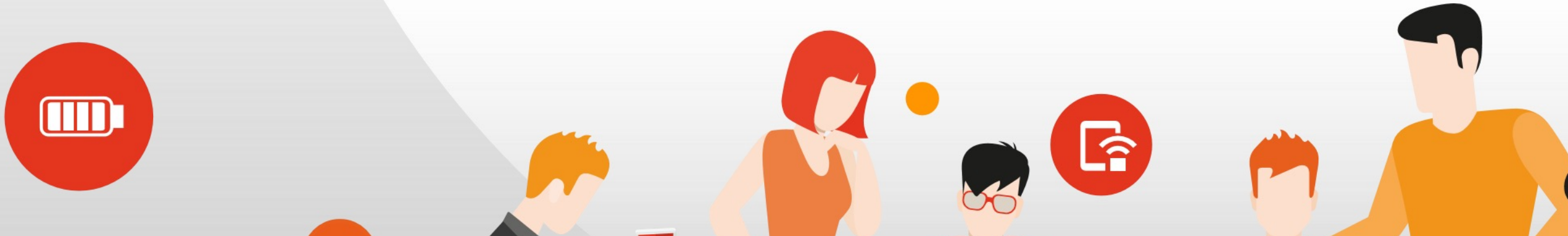
Wat zijn de risico's? 2

6 Zi ac

Ja?

Hoe ziet de omgeving er uit? 1

7 Inbrengen m in de organis

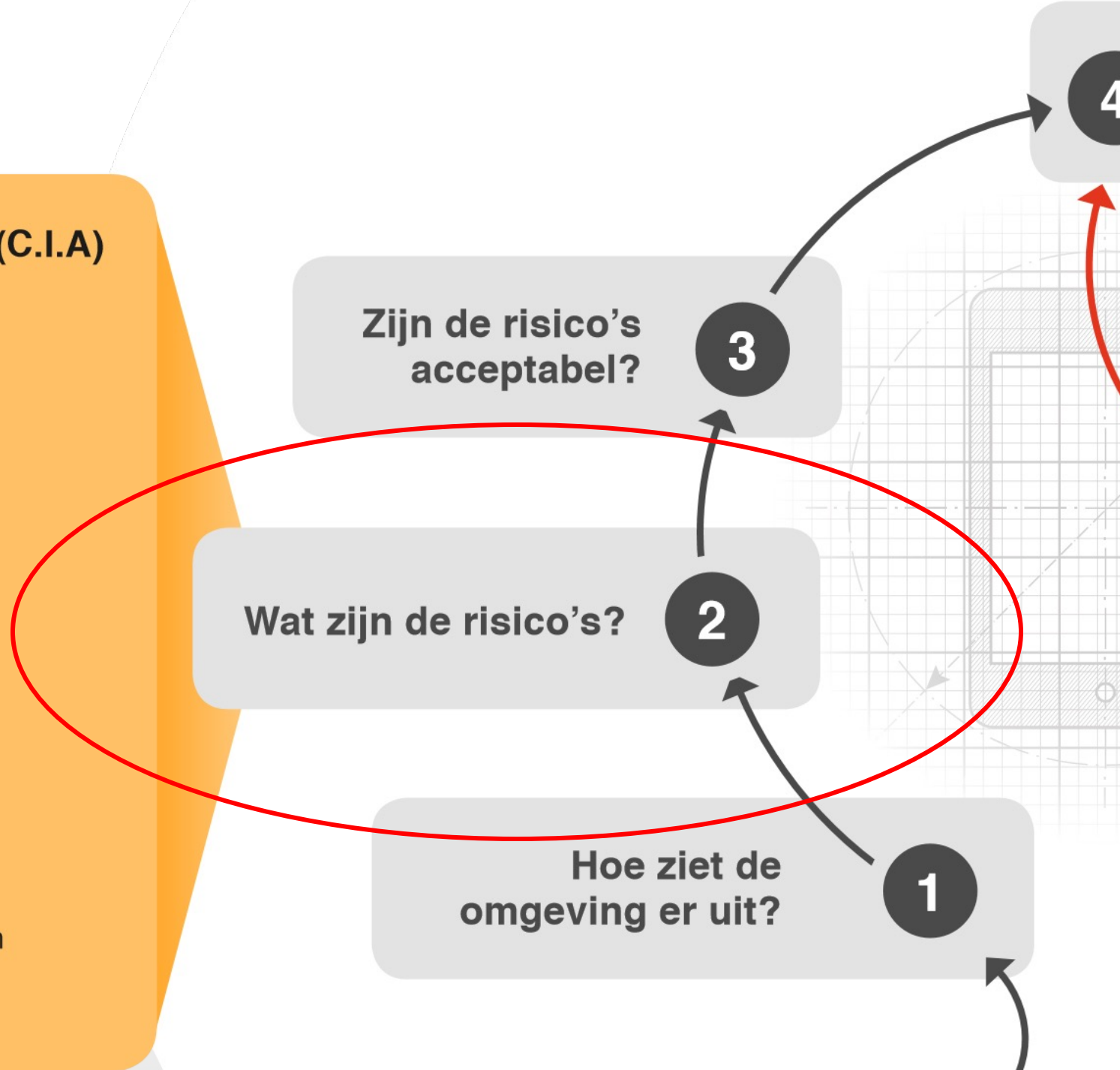


SECURITY ASPECTEN (C.I.A)

- **Vertrouwelijkheid**
  (Confidentiality)
  afschermen van
  vertrouwelijke informatie

- **Integriteit**
  (Integrity)
  is informatie correct,
  functioneren systemen
  volgens bedoeling?

- **Beschikbaarheid**
  (Availability)
  tijdige beschikbaarheid van
  informatie en systemen



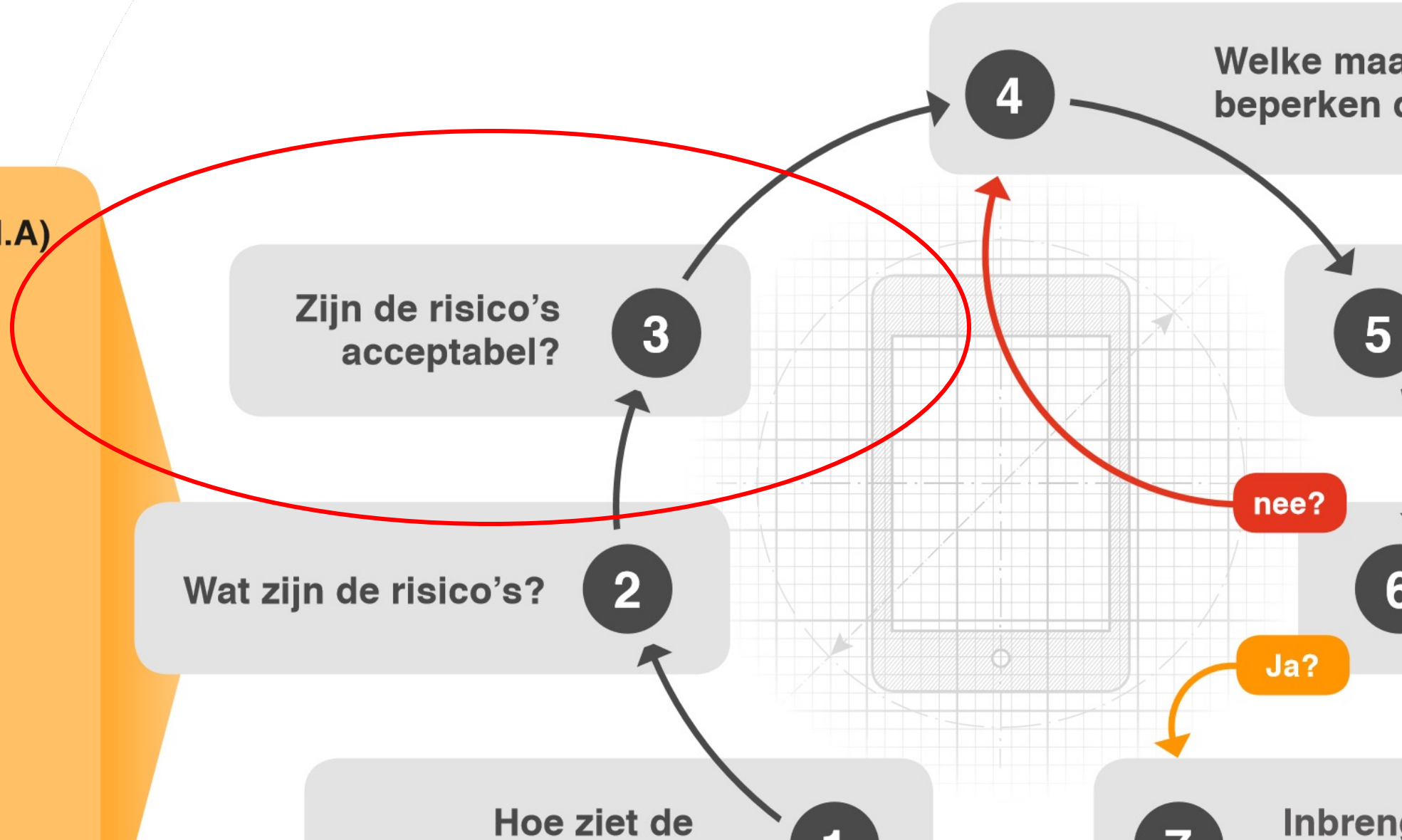
en breed gedragen risicoanalyse
7 stappen

ECURITY ASPECTEN (C.I.A)

Vertrouwelijkheid
(Confidentiality)
afschermen van
vertrouwelijke informatie

Integriteit
(Integrity)
is informatie correct,
functioneren systemen
volgens bedoeling?

Beschikbaarheid



Smart Energy

TKI URBAN ENERGY
Topsector Energie

yse

4 Welke maatregelen beperken deze risico's?

5 Wat zijn de restrisico's? Zijn er nieuwe risico's?

nee?

6 Zijn de restrisico's

RISICOREDUCERENDE MAATREGELEN

- **preventieve maatregel:** reduceert de waarschijnlijkheid dat een aanval optreedt;
- **detectieve maatregel:** detecteert en identificeert een aanval tijdig;
- **correctieve maatregel:** verhoogt de effectiviteit bij het herstellen na een aanval.

yse

4 Welke maatregelen beperken deze risico's?

5 Wat zijn de restrisico's? Zijn er nieuwe risico's?

nee?

6 Zijn de restrisico's acceptabel?

Ja?

Inbrengen maatregelen

RISICOREDUCERENDE MAATREGELEN

- **preventieve maatregel:** reduceert de waarschijnlijkheid dat een aanval optreedt;
- **detectieve maatregel:** detecteert en identificeert een aanval tijdig;
- **correctieve maatregel:** verhoogt de effectiviteit bij het herstellen na een aanval.

WAT IS EEN SECURITY RISICO?


4
Welke maatregelen beperken deze risico's?
5
Wat zijn de restrisico's? Zijn er nieuwe risico's?
nee?
6
Zijn de restrisico's acceptabel?
Ja?
1
7
Inbrengen maatregelen in de organisatie
dat een aanval optreedt;
• detectieve maatregel: detecteert en identificeert een aanval tijdig;
• correctieve maatregel: verhoogt de effectiviteit bij het herstellen na een aanval.
WAT IS EEN SECURITY RISICO?
risico = waarschijnlijkheid * gevolg

Zijn er nieuwe risico's?

nee?

6 Zijn de restrisico's acceptabel?

Ja?

7 Inbrengen maatregelen in de organisatie

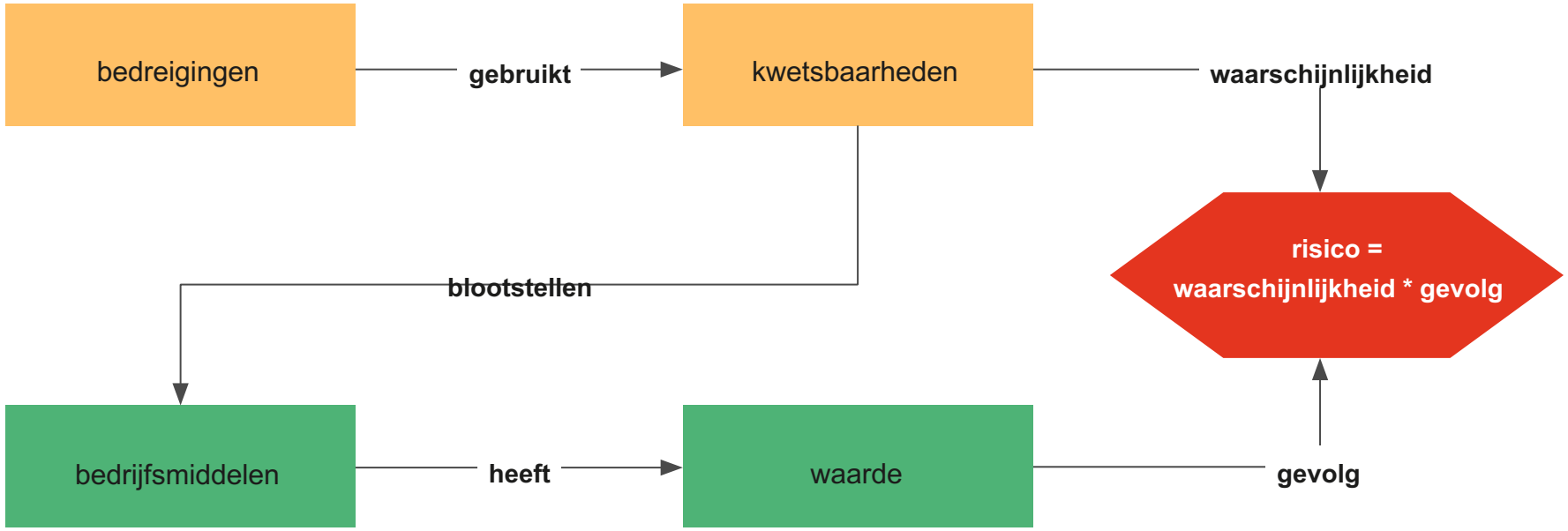
1 oe ziet de ng er uit?

2 ?

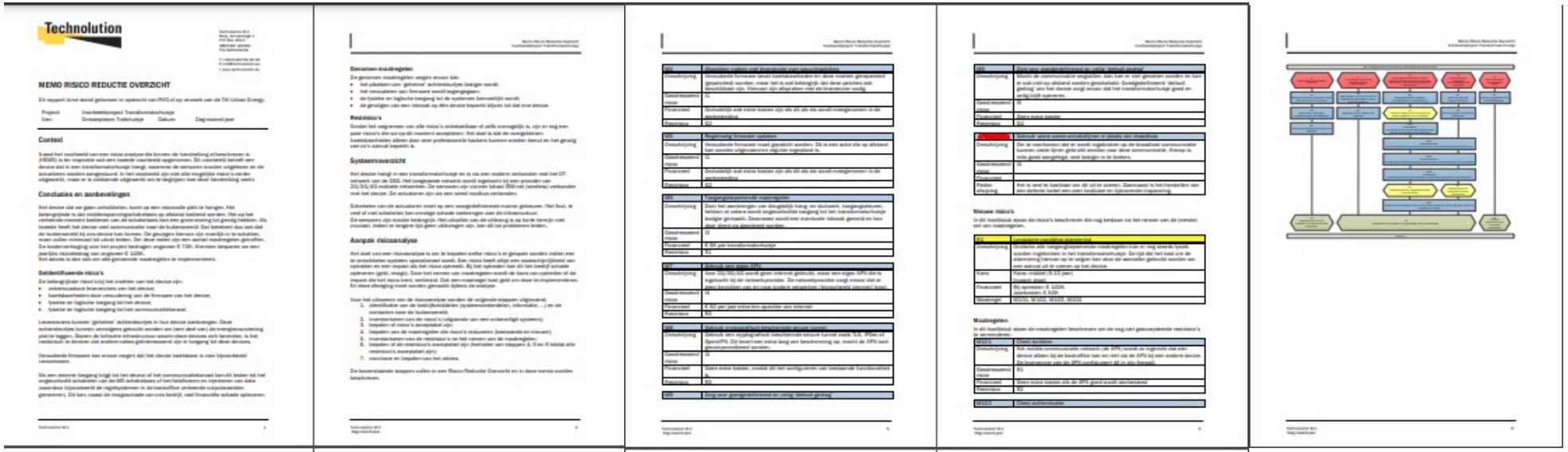
WAT IS EEN SECURITY RISICO

risico = waarschijnlijkheid * gevolg

Cybersecurity risico’s



Voorbeeld



Voorbeeld

Maatregelen

In dit hoofdstuk staan de maatregelen beschreven die genomen worden naar aanleiding van de (initiële) set van risico's.

M1	Maak gebruik van open standaarden
Omschrijving	Door gebruik te maken van open standaarden creëer je keuzevrijheid van leverancier/producent van de apparatuur die ingekocht wordt. Deze vrijheid is nodig als apparatuur, waarvan achteraf is aangetoond dat deze 'geheime' achterdeurtjes bevat, uit te kunnen faseren.
Geadresseerd risico	I1
Financieel	Verwachting is dat dit geen extra kosten met zich meebrengt.
Restrisico	G1

Risico's

In dit hoofdstuk staan de initiële risico's van het systeem beschreven zonder dat er al tegenmaatregelen zijn genomen.

I1	Apparatuur van onbetrouwbare leveranciers
Omschrijving	De apparatuur die wordt gekocht, wordt vaak ontworpen en/of geproduceerd in landen die zich ook bezighouden met cyberaanvallen op kritische infrastructuur van Nederland. Het kan dan zijn dat in de apparatuur functionaliteit zit om deze landen toegang te laten krijgen tot het systeem en daarmee de energievoorziening kunnen beïnvloeden.
Kans	Kans: relatief klein, eens in de 10 à 20 jaar Impact: kan groot worden doordat energielevering stil kan komen te liggen
Financieel	Bij optreden kunnen de kosten tot € 1M oplopen. Jaarbedrag van dit risico is dan: € 75K
Maatregel	M1, M2, M3

Nieuwe risico's

In dit hoofdstuk staan de risico's beschreven die nog bestaan na het nemen van de (eerste) set van maatregelen.

R1	Langzame opvolging alarmering
Omschrijving	Ondanks alle toegangbeperkende maatregelen kan er nog steeds fysiek worden ingebroken in het transformatorhuisje. De tijd die het kost om de alarmering hiervan op te volgen kan door de aanvaller gebruikt worden om een aanval uit te voeren op het device.
Kans	Kans: middel (5-10 jaar) Impact: groot
Financieel	Bij optreden: € 100K Jaarkosten: € 50K
Maatregel	M101, M102, M103, M104

Maatregelen

In dit hoofdstuk staan de maatregelen beschreven om de nog niet geaccepteerde restrisico's te verminderen.

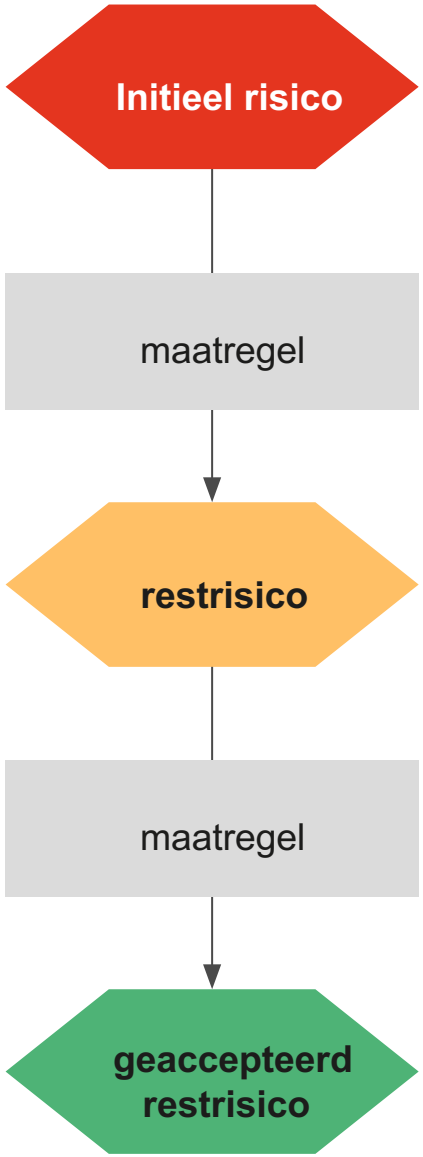
M101	Client isolation
Omschrijving	Het mobile communicatie netwerk (de APN) wordt zo ingericht dat een device alleen bij de backoffice kan en niet via de APN bij een andere device. De leverancier van de APN configureert dit in zijn firewall.
Geadresseerd risico	R1
Financieel	Geen extra kosten als de APN goed wordt aanbesteed
Restrisico	R2

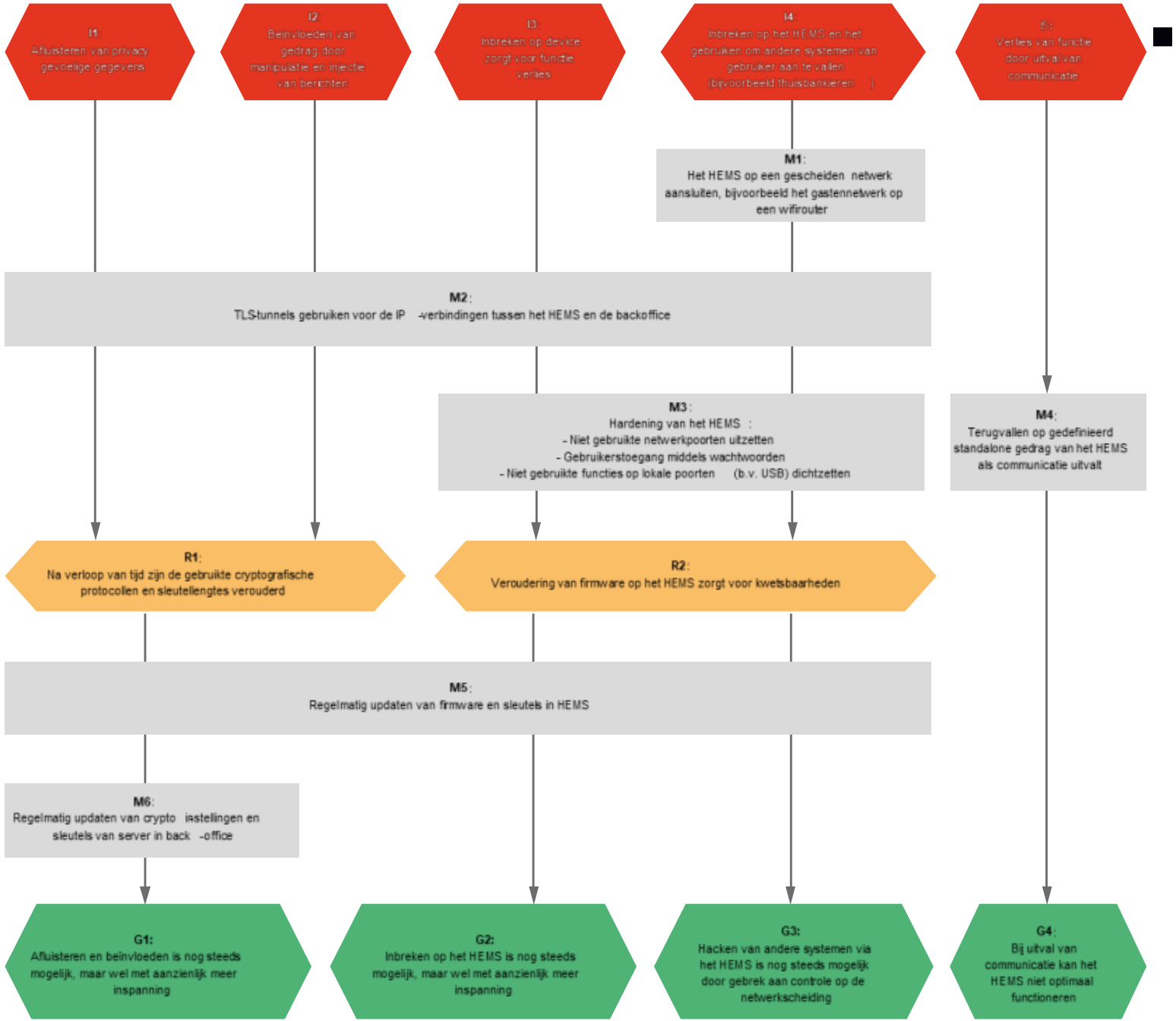
Restrisico's

In dit hoofdstuk staan de uiteindelijk geaccepteerde risico's beschreven.

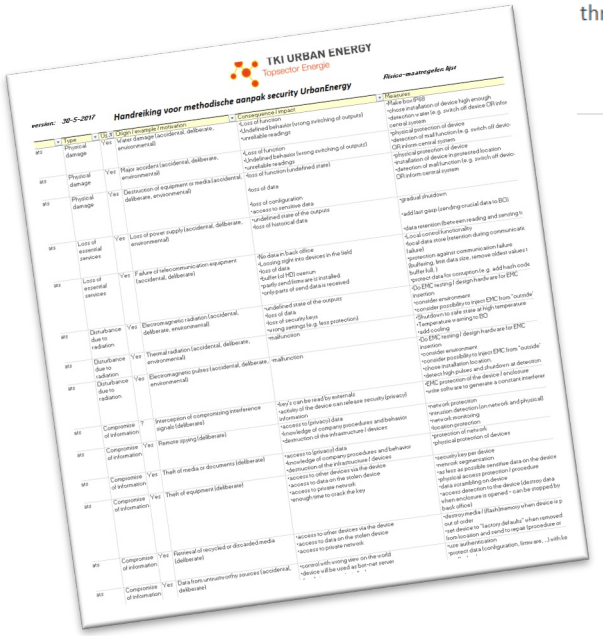
G1	Mogelijkheid dat er nog een 'achterdeur' in zit, maar dit is minder waarschijnlijk.
Omschrijving	Ondanks dat er van alles is geaudit en getest, kan er nog wel een 'achterdeur' in de code zitten. Door gebruik van open standaarden kan een alternatief worden gevonden.
Kans	Klein
Financieel	-

Voorbeeld


Initieel risico
maatregel
restrisico
maatregel
geaccepteerd restrisico


I1:
Afluisteren van privacy gevoelige gegevens
I2
Beïnvloeden van gedrag door manipulatie en injectie van berichten
I3:
Inbreken op device zorgt voor functie verlies
I4:
Inbreken op het HEMS en het gebruiken om andere systemen van gebruiker aan te vallen (bijvoorbeeld thuisbankieren)
I5:
Verlies van functie door uitval van communicatie
M1:
Het HEMS op een gescheiden netwerk aansluiten, bijvoorbeeld het gastennetwerk op een wifirouter
M2:
TLS-tunnels gebruiken voor de IP -verbindingen tussen het HEMS en de backoffice
M3:
Hardening van het HEMS :
- Niet gebruikte netwerkpoorten uitzetten
- Gebruikerstoegang middels wachtwoorden
- Niet gebruikte functies op lokale poorten (b.v. USB) dichtzetten
M4:
Terugvallen op gedefinieerd standalone gedrag van het HEMS als communicatie uitvalt
R1:
Na verloop van tijd zijn de gebruikte cryptografische protocollen en sleutellengtes verouderd
R2:
Veroudering van firmware op het HEMS zorgt voor kwetsbaarheden
M5:
Regelmatig updaten van firmware en sleutels in HEMS
M6:
Regelmatig updaten van crypto instellingen en sleutels van server in back -office
G1:
Afluisteren en beïnvloeden is nog steeds mogelijk, maar wel met aanzienlijk meer inspanning
G2:
Inbreken op het HEMS is nog steeds mogelijk, maar wel met aanzienlijk meer inspanning
G3:
Hacken van andere systemen via het HEMS is nog steeds mogelijk door gebrek aan controle op de netwerkscheiding
G4:
Bij uitval van communicatie kan het HEMS niet optimaal functioneren

Hulpmiddelen


TKI URBAN ENERGY
topsector Energie
Handreiking voor methodische aanpak security UrbanEnergy
Risico-maatregelen lijst

	Type	Use	Origin / example / motivation	Consequence / impact	Measures
threats	Physical damage	Yes	Water damage (accidental, deliberate, environmental)	•Loss of function •Undefined behavior (wrong switching of outputs) •unreliable readings	•Make box IP68 •chose installation of device high enough •detection water (e.g. switch off device OR inform central system

	Type	Use	Origin / example / motivation	Consequence / impact	Measures
threats	Loss of essential services	Yes	Failure of telecommunication equipment (accidental, deliberate)	•No data in back office •Loosing sight into devices in the field •loss of data •buffer (of HD) overrun •partly send firmware is installed. •only parts of send data is received	•Local control functionality •local data store (retention during communication failure) •protection against communication failure (buffering, limit data size, remove oldest values to buffer full,) •protect data for corruption (e.g. add hash code)

	Type	Use	Origin / example / motivation	Consequence / impact	Measures
threats	Compromise of information	Yes	Theft of equipment (deliberate)	•access to other devices via the device •access to data on the stolen device •access to private network •enough time to crack the key	•security key per device •network segmentation •as less as possible sensitive data on the device •physical access protection / procedure •data scrambling on device •access detection to the device (destroy data when enclosure is opened - can be stopped by the back office)

	Type	Use	Origin / example / motivation	Consequence / impact	Measures
vulnerabilities	Hardware	Yes	Lack of efficient configuration change control	•not known what the used configuration •unexpected behavior •wrong access / certificates used	•add configuration control •make it possible to (remote) read the configuration items

	Type	Use	Origin / example / motivation	Consequence / impact	Measures
vulnerabilities	Personnel	Yes	Lack of security awareness	•Error in use	•organize meetings to increase security awareness •make security a topic of all (not only the security officer) •keep on learning on security

Cyber security moet “fit for purpose” zijn:

voldoende maatregelen om veilig te zijn, voldoende openheid om betaalbaar / bruikbaar te blijven

Redefining
solutions

Vragen?

Redefining
solutions

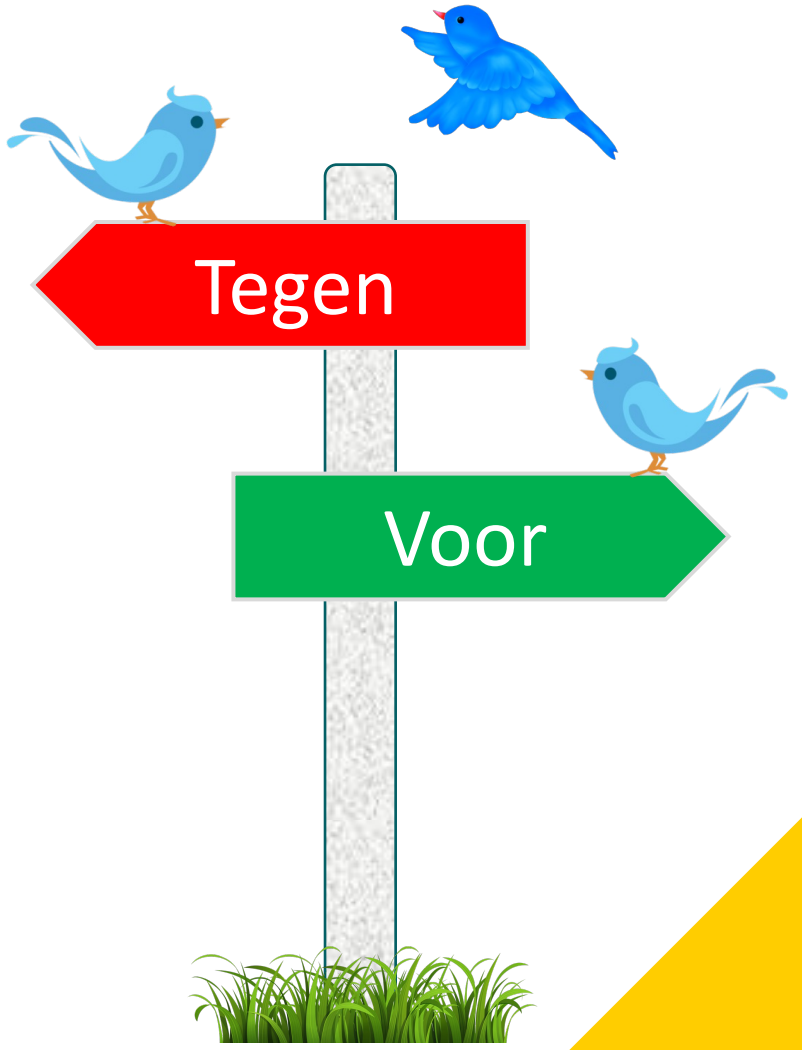
Vraag aan jullie:

Wat zijn jullie grootste uitdagingen bij Cyber security?

Redefining
solutions

Lagerhuis

Nu zelf aan de slag met stellingen



Redefining
solutions

Stelling: Cybersecurity by design

Het later toevoegen van cybersecurity maatregelen kan helemaal niet. Het kan alleen goed gebeuren als je cyber security in het eisenpakket en in je ontwerp al meeneemt.

Stelling: Businesswise

Je kan geen system maken wat “cyber secure” is zonder het mee laten werken van de rest van je organisatie / het MT

Stelling: Techniek

Wat je ook doet, je systeem is nooit veilig genoeg. Er zijn altijd risico’s die je gewoon moet accepteren.

Stelling: Verzekeringen

Als jou systemen niet goed cyber secure zijn, kan jij jezelf niet verzekeren.

Stelling: Businesswise

Bewustwording van wat cybersecurity is binnen jou organisatie is eigenlijk belangrijker dan je IT/OT systemen helemaal secure maken.

Stelling: Businesswise

Als ik gehackt wordt is dat mijn probleem. De andere hebben daar geen last van.