Weerbaarheid verhogen door informatiedeling

- Frans van den Akker
  & Jako Jellema
  ISPT – Grip op drogen
- Floor Terra
  Privacy Company
- Jeroen Poldervaart
  ANDRITZ

Opstap naar **weerbaarheid**
in een digitale **samenleving**

Weerbaarheid verhogen door informatiedeling

uw zaalvoorzitter

Jasper Nagtegaal
Agentschap Telecom

Opstap naar Weerbaarheid

Industry 4.0 Cluster

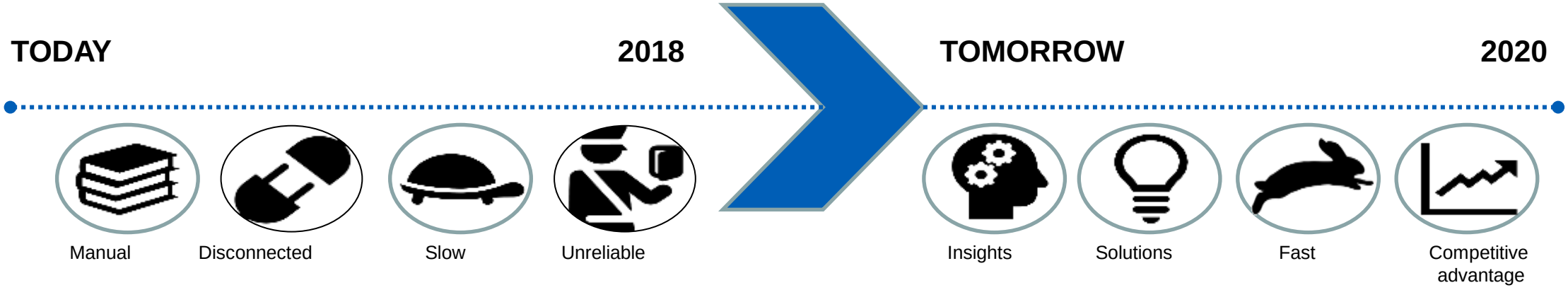

FRAMES
BRONSWERK HEAT TRANSFER BV
evodos DYNAMIC SETTLERS
ISPT
OCI NITROGEN
VanHoutum
VOITH
Eska Graphic Board
Smurfit Kappa
grupo Portucel Soporcel
YARA
Knowledge grows
ROYAL COSUN
parenco
HOLMEN
AkzoNobel
Valmet
DSM BRIGHT SCIENCE. BRIGHTER LIVING.
DOW
CROWN VAN GELDER
evides industriewater
سابك sabic
MM KARTON AG
FrieslandCampina
ebn
HAK
COFELY GDF SUEZ
HEXION
GDF SUEZ
MetsäFibre
UPM
mondi
OMYA
NALCO Champion An Ecolab Company
Corbion purac
stordenso
Buckman
AVEBE
NL Guts

The DIGITAL mission

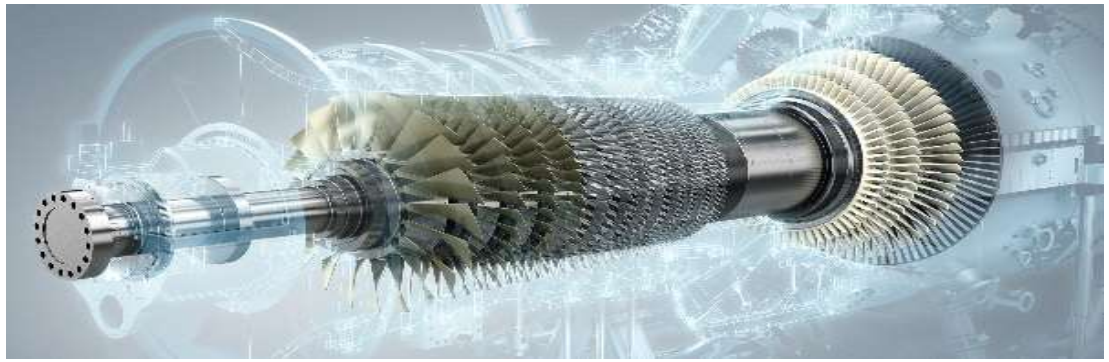
Use digitization to obtain predictive quality, predictive cost, predictive supply and predictive maintenance, and enable information sharing across the supply and value chain and across plants.

Achieve Items Like

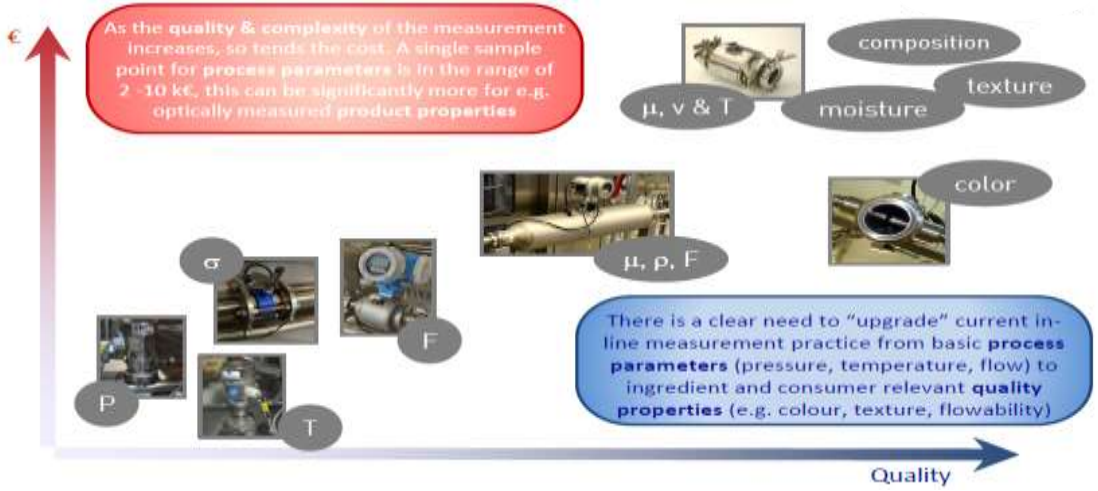
Constant product quality, operator-independency, Reduce Waste, Site invariance, Control waste composition, Continuous vs batch, Measure product characteristics, Energy-Efficiency, Yield, Control product functionality, Measure raw material composition.



Smart and in-line Sensors



Siemens' latest gas turbines contain more than 500 sensors, which continuously register pressure conditions, temperatures, component stress, and much more.



ISPT activities

GRIP OP DROGEN:

In line sensors in drying processes paper industry.

PROPOSAL:
Cheap spectroscopic sensors:

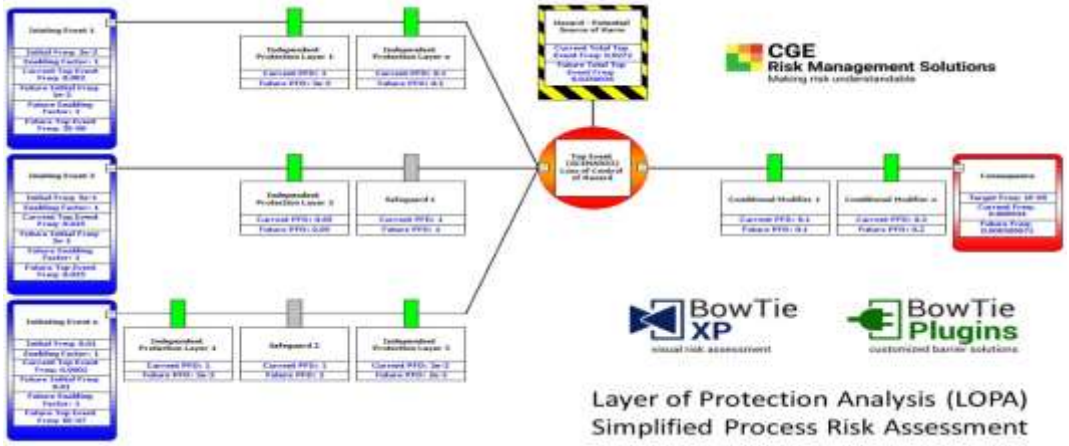
Open innovation collaboration to create cheap in line sensors for spectroscopic measurements (range 400-2500 nm).

Cyber security & Vulnerability

The IT software and hardware for AI/APC/Remote maintenance/ etc. leads to increased vulnerability and the need for:

- **Resilience** of infrastructure and systems

- **Cyber hygiene** and behaviour
- **Security by design**



ISPT activities

Factory

- Ensure continuous production
- Ensure safety for both employees and the environment
- Ensure integrity of systems and ensure that proprietary or sensitive data cannot be accessed.
- Minimize the effects of an incident while quickly restoring operations.

- **Booklet on assessment**

To be published in Jan 2019

Thank You

frans.vandenakker@ispt.eu
meine.koeslag@ispt.eu

www.ispt.eu/industrie4-0

ANDRITZ GROEP

OPSTAP NAAR WEERBAARHEID IN EEN DIGITALE SAMENLEVING

UITVAL VAN VERBINDING

22 NOVEMBER 2018

ANDRITZ

ENGINEERED SUCCESS

ANDRITZ GROEP

OPSTAP NAAR WEERBAARHEID IN EEN DIGITALE SAMENLEVING

22 NOVEMBER 2018

ANDRITZ

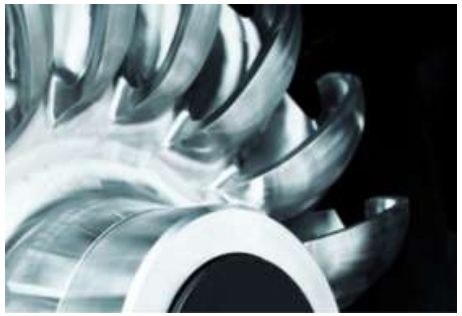
ENGINEERED SUCCESS

INHOUD

ANDRITZ GROEP

ANDRITZ

WATERKRACHT INSTALLATIES



PULP & PAPIER PRODUCTIELIJNEN

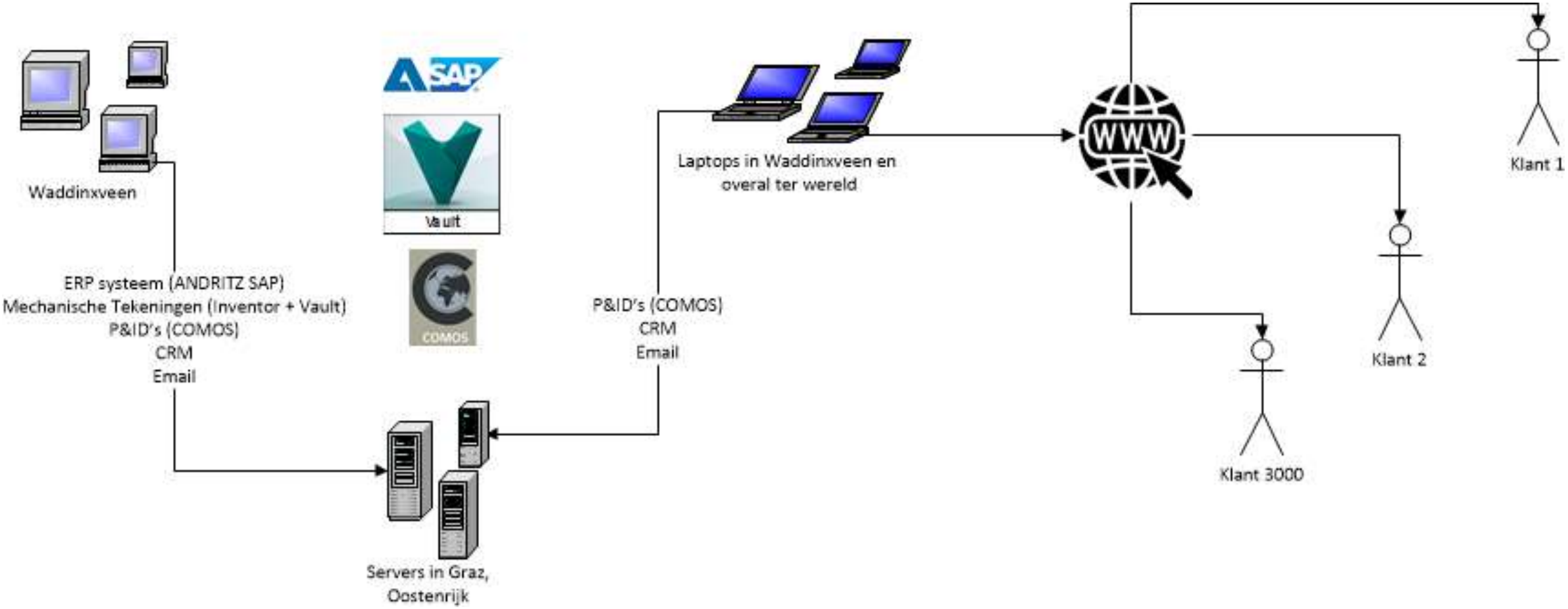
METAALVORMING

SCHEIDINGS-TECHNIEKEN

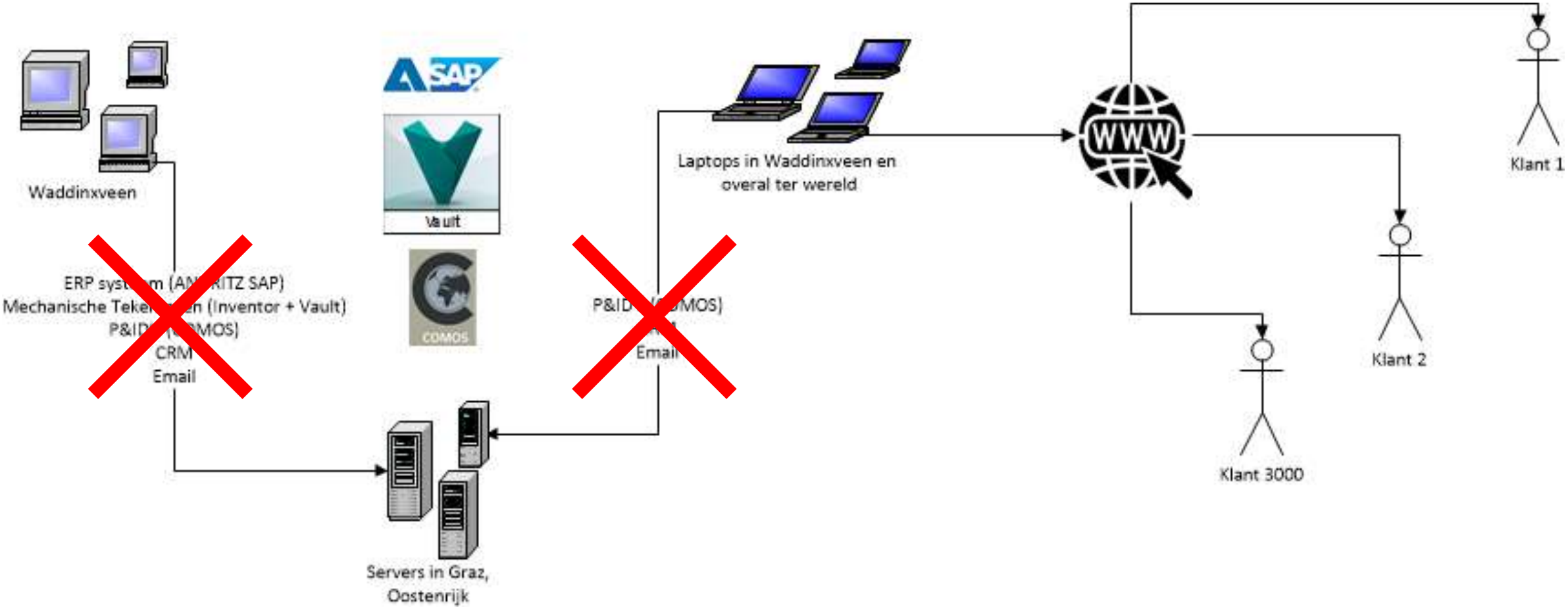
ANDRITZ Gouda:

- Machines en proceslijnen voor m.n. contactdrogen (thermische scheiding)
- Ca. 150 personen in Waddinxveen
- Omzet ca. 48 MEUR (hele groep: 6+ miljard EUR)

ANDRITZ NETWERK



ALS DE VERBINDING WEG VALT – INTERN



ALS DE VERBINDING WEG VALT – INTERN

Sales

Process Engineering

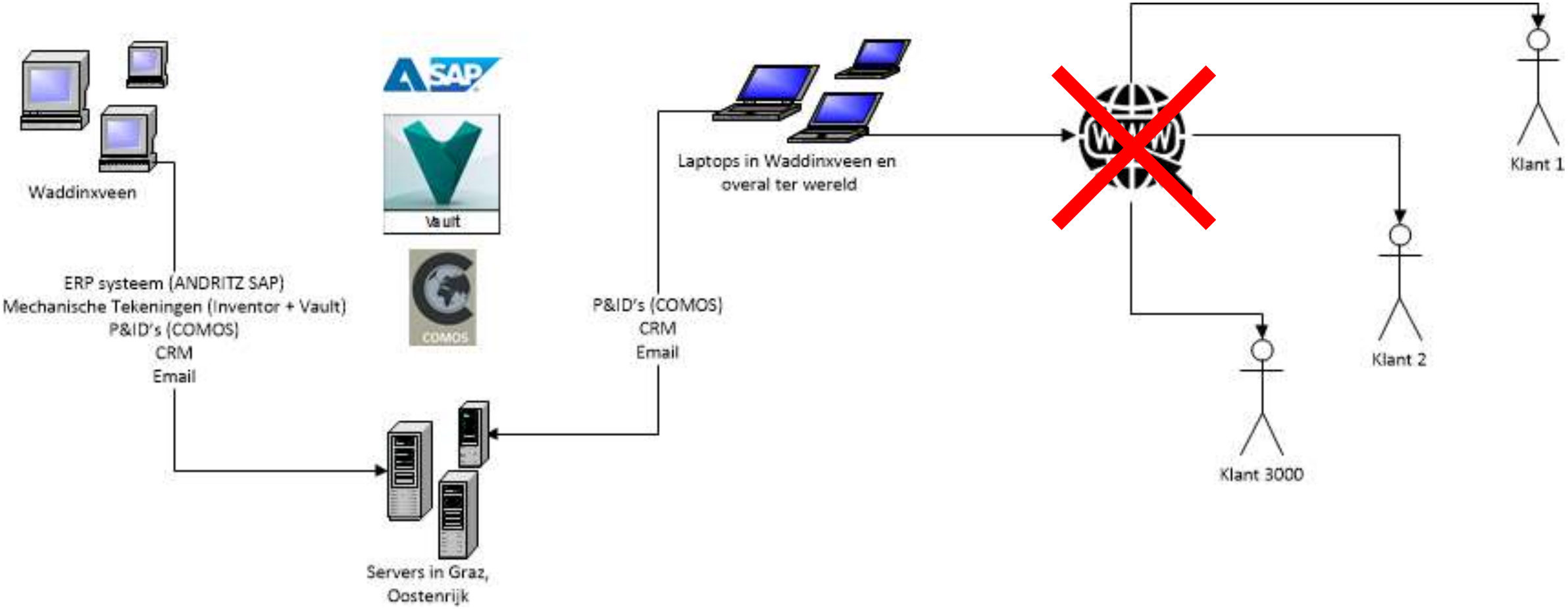
(Mechanical) Engineering

Supply Chain

Finance

… eigenlijk iedereen

ALS DE VERBINDING WEG VALT – MET DE KLANT



ALS DE VERBINDING WEG VALT – MET DE KLANT

Gebruik klantverbinding nu:

- Trouble shooting
- Data collectie
- Niet altijd actief

Probleem aan klantzijde mogelijk groter i.v.m. (voedsel) veiligheid

LEGAL DISCLAIMER

© ANDRITZ AG 2018

This presentation contains valuable, proprietary property belonging to ANDRITZ AG or its affiliates (“the ANDRITZ GROUP”), and no licenses or other intellectual property rights are granted herein, nor shall the contents of this presentation form part of any sales contracts which may be concluded between the ANDRITZ GROUP companies and purchasers of any equipment and/or systems referenced herein. Please be aware that the ANDRITZ GROUP actively and aggressively enforces its intellectual property rights to the fullest extent of applicable law. Any information contained herein (other than publically available information) shall not be disclosed or reproduced, in whole or in part, electronically or in hard copy, to third parties. No information contained herein shall be used in any way either commercially or for any purpose other than internal viewing, reading, or evaluation of its contents by recipient and the ANDRITZ GROUP disclaims all liability arising from recipient’s use or reliance upon such information. Title in and to all intellectual property rights embodied in this presentation, and all information contained therein, is and shall remain with the ANDRITZ GROUP. None of the information contained herein shall be construed as legal, tax, or investment advice, and private counsel, accountants, or other professional advisers should be consulted and relied upon for any such advice.

All copyrightable text and graphics, the selection, arrangement, and presentation of all materials, and the overall design of this presentation are © ANDRITZ GROUP 2018. All rights reserved. No part of this information or materials may be reproduced, retransmitted, displayed, distributed, or modified without the prior written approval of Owner. All trademarks and other names, logos, and icons identifying Owner’s goods and services are proprietary marks belonging to the ANDRITZ GROUP. If recipient is in doubt whether permission is needed for any type of use of the contents of this presentation, please contact the ANDRITZ GROUP at welcome@andritz.com.

PRIVACY COMPANY

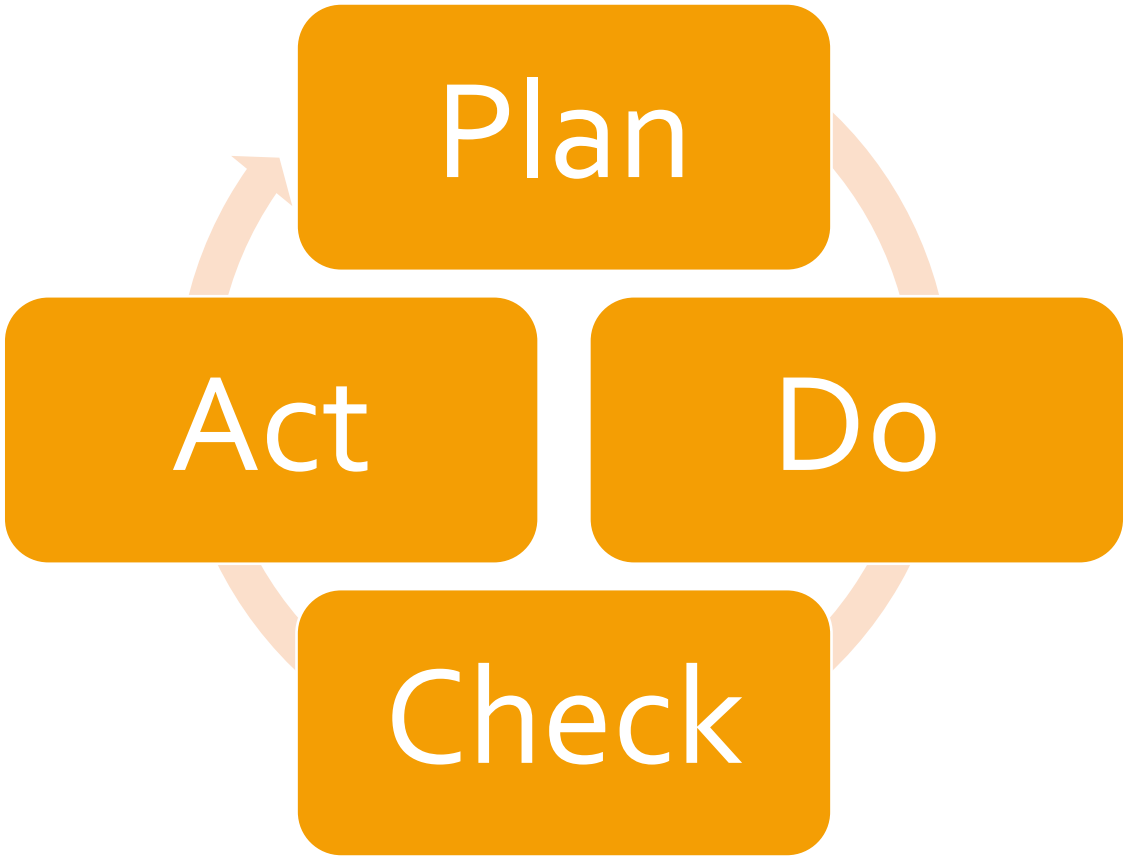
Symposium ’Opstap naar weerbaarheid in een digitale samenleving’

22 November 2018

Weerbaarheid door openheid

PRIVACY COMPANY

Doel: Verbetercyclus inkorten



Hyperconnectiviteit

- Beveiligingsincident bij baby-dump.nl
  - Misbruikt voor misinformatie over KPN
  - KPN haalt uit voorzorg dienstverlening offline
- Diginotar wordt gehackt
  - Toegang wordt misbruikt om communicatie in Iran af te luisteren
  - Als Diginotar onmiddellijk uitgezet word verstoord dit o.a. dienstverlening die afhankelijk is van PKIO certificaten.
  - Hoe langer Diginotar blijft functioneren, hoe hoger het risico voor dissidenten waarvan communicatie afgeluisterd kan worden.

Never waste a good crisis

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

- Een crisis kan leerzaam zijn
  - Praktijkervaring is veel waard
  - Onderzoek de oorzaak
  - Voorkom herhaling door kennisdeling
- Dezelfde lessen zonder echte crisis
  - Crisisoefening
  - ChaosMonkey (Netflix)
  - Responsible disclosure of Coordinated Vulnerability Disclosure

Coordinated Vulnerability Disclosure: de Leidraad

Coordinated Vulnerability Disclosure

Website	privacycompany.eu
Email	floor.terra@privacycompany.eu
Phone	+ 31 (6) 152 48 422

Delen – TLP:White

ir. jako jellema (Agentschap Telecom & Grip op drogen)

ABCDtje [notitie]

Doel presentatie: Aanvulling op Jeroen & Floor – Hoe willen wij incidenten delen?

Conclusie:

- TLP is nuttig. Verschillende benaderingen zijn mogelijk.
- Delen van incidenten gebeurt al. ‘Hoe willen wij het in 2019 in de industrie doen?’

Betoog:

- Nog even de CIAtriad (o.a. omdat FT komt uit de C wereld)
- TLP helpt om bewust te zijn over wat voor info je deelt en met wie
- Bestaande modellen (o.a. bij ‘mailicious intent’), voorbeelden:
  - ISAC
    - Energie
    - Financieel
  - Open database
    - (door bedrijf?)
    - Open database door overheid (Agentschap T)
- **Aandacht trekker:** TLP wit, start, einde en tussendoor. Maar tuurlijk is amber ook nuttig.

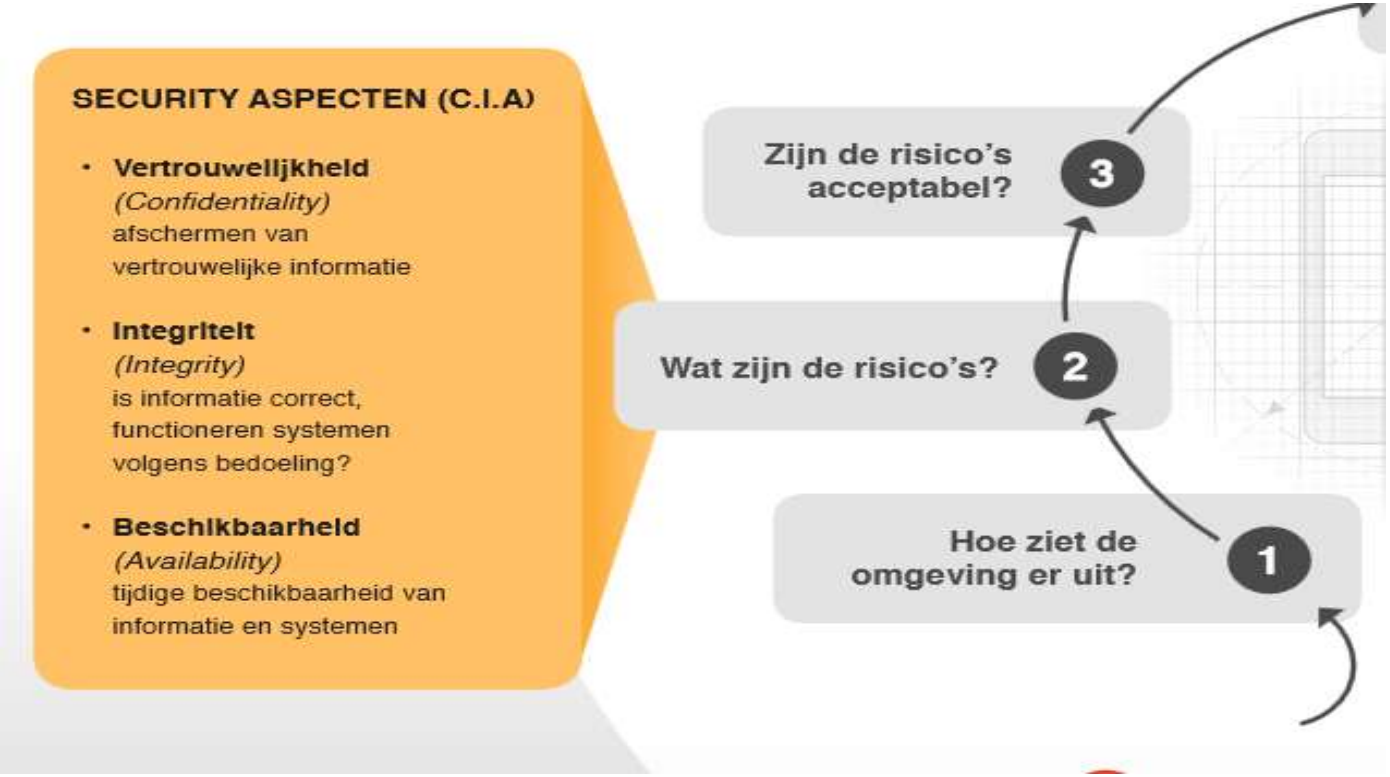
C.I.A. triad:

Confidentiality

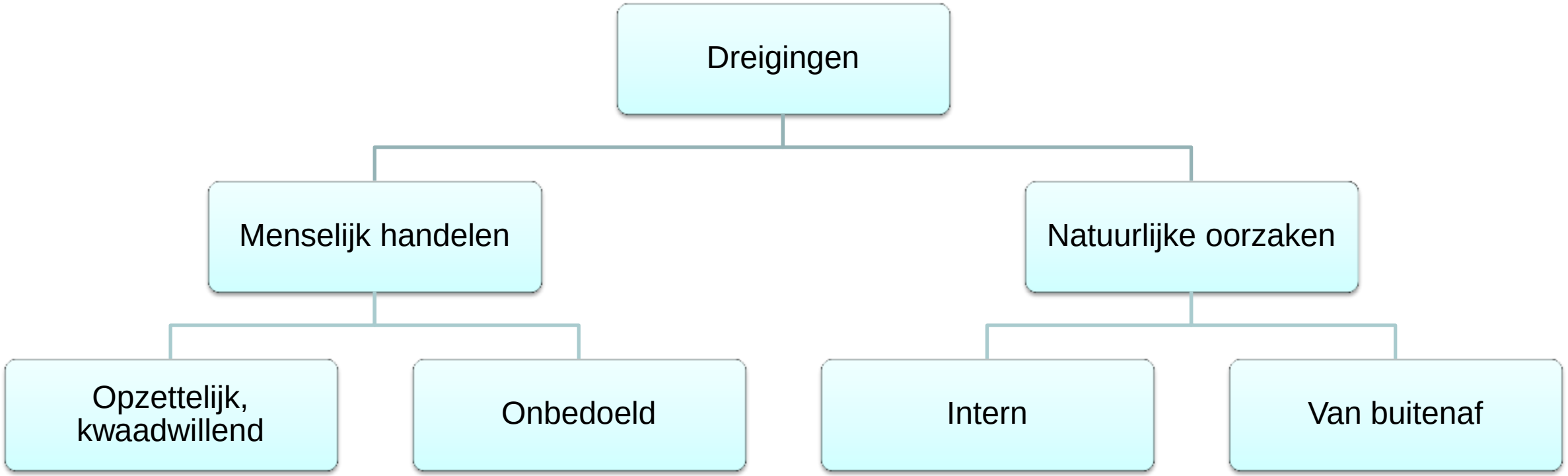
Integrity

& Availability

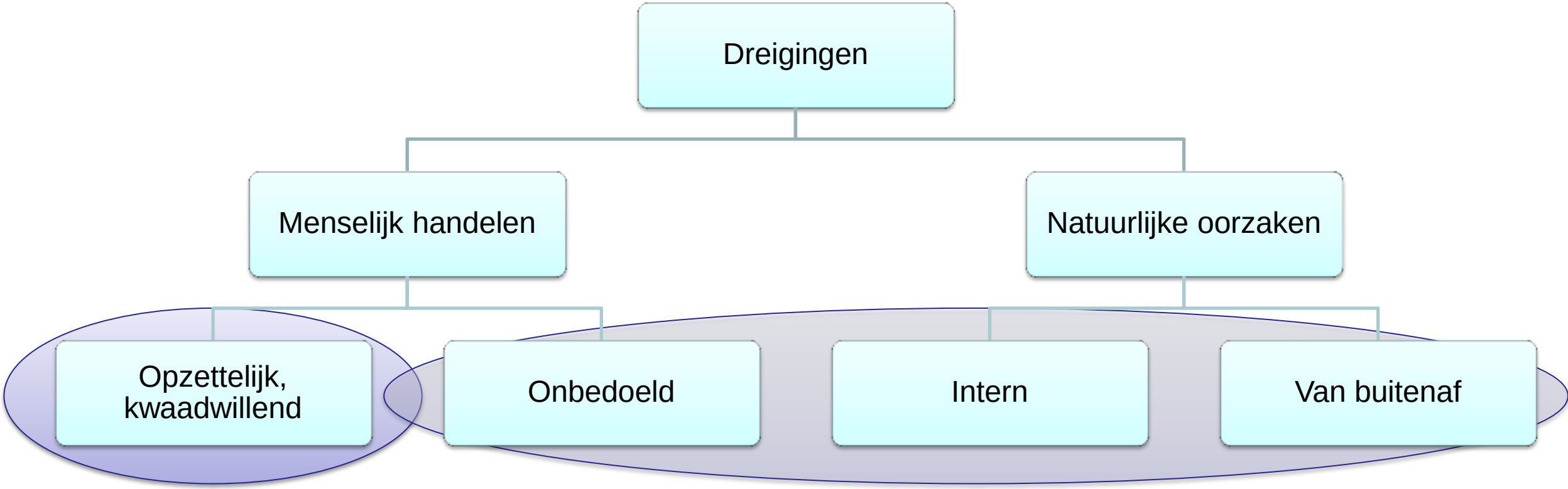
C. I. A! [notitie]
zie handreiking van de TKI over CyberSecurity



Telekwetsbaarheid en cyberveiligheid



Telekwetsbaarheid en cyberveiligheid



Informatiebeveiliging, systeembeveiliging.

Beschikbaarheid, continuïteit.

4

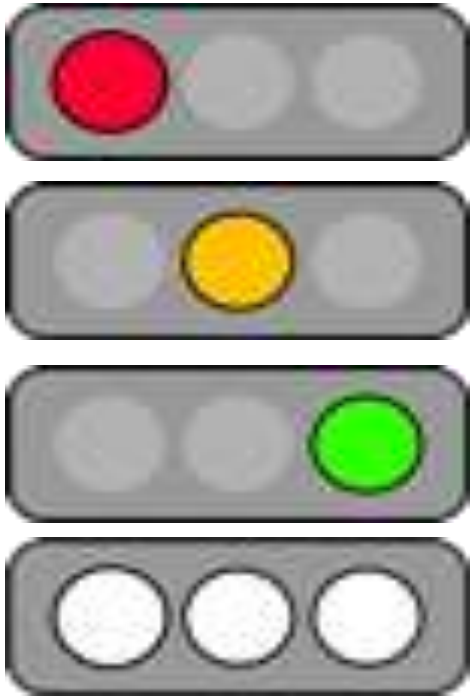
Mitigation

Enexis & SCADA [notitie] BRON:

Duinmaijer, David. “Slecht mobiel bereik in het buitengebied hoort erbij, ook voor monteurs van Enexis.” Energeia (Financieel Dagblad), October 31, 2018. https://energeia.nl/energeia-artikel/40073304/slecht-mobiel-bereik-in-het-buitengebied-hoort-erbij-ook-voor-monteurs-van-enexis.

Foto: Bedrijfsvoeringscentrum Weert, Enexis

TLP



TLP [notitie]

BRON: plaatjes
https://www.us-cert.gov/tlp

BRON:

Factsheet van Nationaal Cyber Security Centre (NCSC) met toelichting op het TLP
https://www.ncsc.nl/actueel/factsheets/factsheet-indicators-of-compromise.html

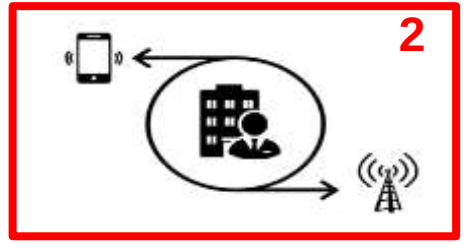
Overig bronnen:

https://www.first.org/tlp/

https://en.wikipedia.org/wiki/Traffic_Light_Protocol

TLP-categorieën

TLP-RED	"For your eyes only". Alleen door u te gebruiken en niet voor verspreiding naar andere personen, zelfs niet binnen uw organisatie.
TLP-AMBER	Te gebruiken en te delen met collega's binnen uw organisatie op basis van need-to-know en met klanten die deze informatie moeten krijgen zodat zij zichzelf kunnen beschermen of verdere schade hiermee kunnen voorkomen.[4]
TLP-GREEN	Niet al te gevoelige informatie die u mag verspreiden naar al uw contacten zolang u het niet publiceert op een openbare plek zoals een blog of website.
TLP-WHITE	Openbare informatie die vrij verspreid mag worden, rekening houdend met het auteursrecht.



Dependencies

Chemie Park Delfzijl

[notitie] Project CPD

“Onlangs werd op Chemie Park Delfzijl (CPD) een nieuwe kazerne voor de bedrijfsbrandweer in gebruik genomen. Ook zijn er plannen voor de verhuizing van de centrale meldpost en de beveiligers naar de nieuwe kazerne. Een goed moment om te na te gaan wat de gevolgen voor de communicatie zijn bij een calamiteit. Agentschap Telecom deed samen met het CPD onderzoek naar de risico’s en vandaag ontving Hilda Godlieb, Manager Shared Service Centre, uit handen van Jako Jellema van Agentschap Telecom het eindrapport. Hilda: ‘Door het onderzoek weten we welke telecomdiensten we gebruiken bij calamiteiten en hoe solide ze zijn. Maar we hebben ook beter zicht op de zwakke schakels en kunnen bewustere keuzes maken.’ Het CPD gaat nu met de aanbevelingen aan de slag. In september komen beide partijen weer bij elkaar om de stand van zaken te bespreken.”

https://www.linkedin.com/showcase/telekwetsbaarheid/

Leren van incidenten – 4 modellen:

- Information Sharing & Analysis Centre
  - FSISAC – Financial & international
  - ISAC – energy (The Netherlands)

- Database
  - Online – (International)
  - Overheid – (The Netherlands)

Information Sharing and Analysis Center

ISPT

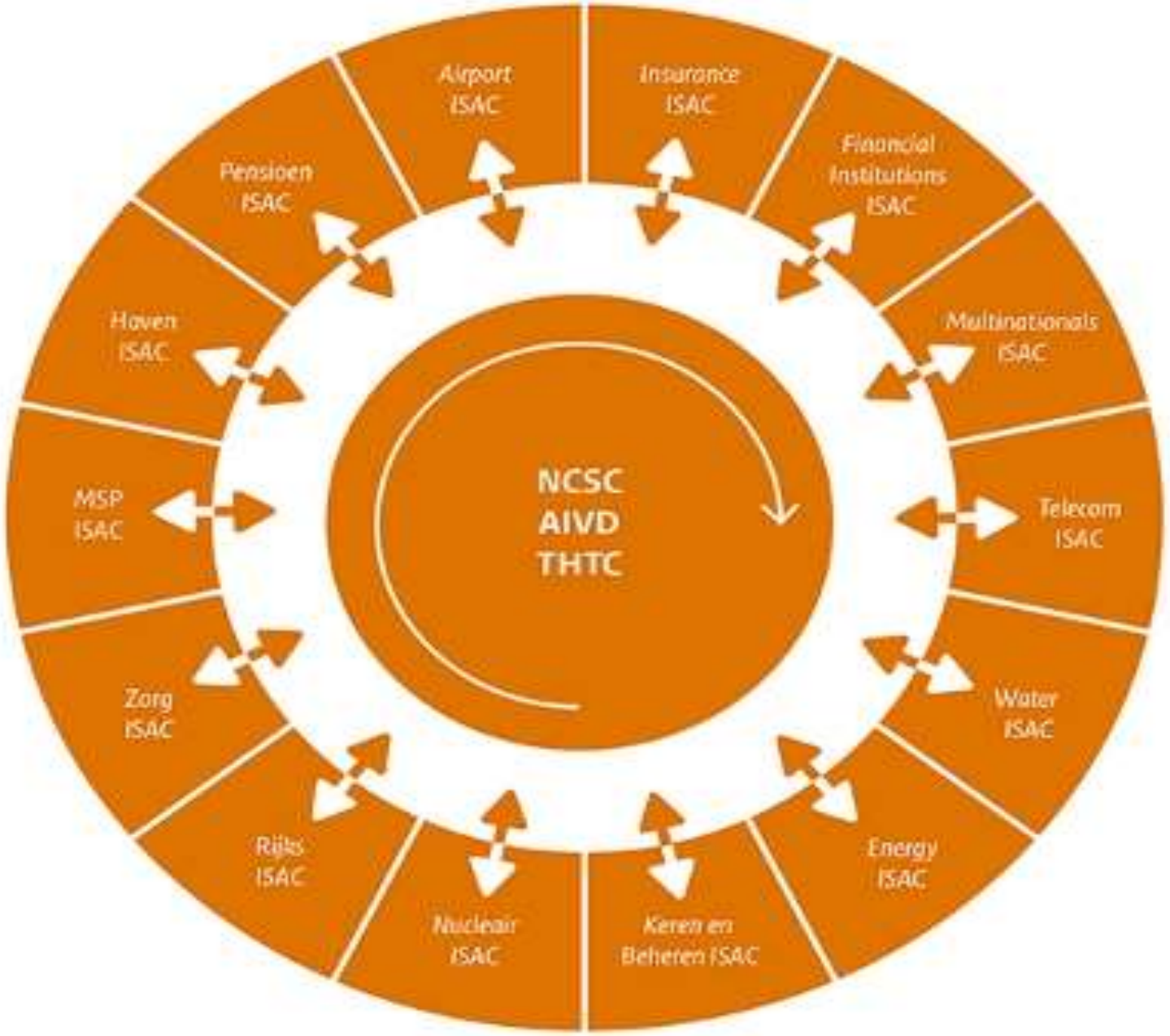
FSIAC [notitie]

https://www.fsisac.com/

“Financial Services Information Sharing and Analysis Center”

The only industry forum for collaboration on critical security threats facing the global financial services sector.

When attacks occur, early warning and expert advice can mean the difference between business continuity and widespread business catastrophe. Members of the Financial Services Information Sharing and Analysis Center (FS-ISAC) worldwide receive timely notification and authoritative information specifically designed to help protect critical systems and assets from cyber and physical security threats.


Airport ISAC
Insurance ISAC
Financial Institutions ISAC
Multinationals ISAC
Telecom ISAC
Water ISAC
Energy ISAC
Keren en Beheren ISAC
Nuclear ISAC
Rijks ISAC
Zorg ISAC
MSP ISAC
Haven ISAC
Pensioen ISAC
NCSC
AIVD
THTC

ISAC – energy [notitie]

https://www.ncsc.nl/samenwerking/_samenwerken/sectorale-samenwerking-isac.html

Wat is een ISAC?

Een ISAC is een frequent overleg over cybersecurity: een middel om een vertrouwde omgeving te creëren waarbinnen organisaties uit dezelfde sector gevoelige en vertrouwelijke informatie over incidenten, dreigingen, kwetsbaarheden, maatregelen en leerpunten delen. Deze uitwisseling van kennis, informatie en expertise maakt het een uitstekend middel om de digitale weerbaarheid van uw organisatie en sector te vergroten. Een ISAC biedt u ook een netwerk aan specialisten binnen uw sector die u in het geval van een bedrijfsoverstijgend ICT-incident makkelijk weet te vinden.

‘Telekwetsbaarheid aanpak’ [notitie]

Incidentenmonitoring

Stap 1

Inspanning:	snel & goedkoop	| – – – – x |	langdurig of duur
Complexiteit:	eenvoudig	| – – x – – |	ingewikkeld

Wat is het? Over langere periode bijhouden van incidenten in de organisatie en de branche.

Wat levert het op? Inzicht in risico’s die daadwerkelijk voorgekomen zijn, en de gevolgen die dat heeft gehad. Voorbeelden om anderen bewust te maken dat incidenten niet denkbeeldig zijn.

Wanneer gebruiken? Wanneer er behoefte is om te leren van verstoringen en fouten, en de wens om voortdurend te verbeteren.

Hoe gaat het in zijn werk? Incidenten met telecomuitval worden gesignaleerd, via social media, traditionele media, ‘wandelganggesprekken’ of spontane tips vanuit het netwerk.

Wie heb ik nodig? Meerdere mensen die incidentmeldingen opmerken en aangeven. Iemand met ruime ervaring met telecom of ICT om de incidenten te classificeren en in te voeren.

Wat heb ik nodig? Abonnementen op (social) media-monitoringdiensten.

Nadelen: Erg afhankelijk van het detailniveau van gemelde incidenten. Vergt aandacht over een langere periode (een jaar of langer).

Meer informatie:

Never waste a good crisis [notitie]
vb: www.inspectie-jenv.nl/Publicaties/rapporten/2012/07/16/storing-telecommunicatienetwerk-waalhaven-rotterdam

Never waste a good crisis' of 'Een ramp op zijn tijd, is goed voor beleid.' Organisaties leren van fouten. Mogelijk is dit op het vlak van telekwetsbaarheid ook de meest effectieve manier om aan te zetten tot actie. Hoe dichter bij de persoonlijke ervaring hoe makkelijker het is om een leermoment te vinden. De beste voorbeelden verzinnen mensen zelf of kennen ze al als het besproken wordt. Idealiter wordt de monitoring binnen de sector gedaan met sectorale expertise en duiding.

Theoretisch zou ook gebruik kunnen worden gemaakt van fictieve verhalen. Realistisch en aannemelijk. Maar de meeste kracht zit in 'gebaseerd op feiten' - waargebeurd.

Het programma telekwetsbaarheid kijkt wekelijks naar incidenten met telecom uitval. Daarbij wordt gebruik gemaakt van de LexisNexis database van regio- en dagbladen en Coosto analyses van social media. In de wandelgangen worden ook incidenten verzameld.

Soms wordt een incident uitgewerkt tot een casus die gebruikt wordt in voorlichting. Een voorbeeld van een uitgebreide uitwerking van een incident:

RISI Online Incident Database

Event Year:	2014	**Reliability:**	Confirmed
Country:	Germany		
Industry Type:	Metals		
Description:	Multiple attackers used an advanced social engineering attack to gain access to the company network and then worked their way onto the control system network. This resulted in an incident where a furnace could not be shut down in the regular way and the furnace was in an undefined condition which resulted in massive damage to the whole system."		
Impact:	A furnace could not be shut down in the regular way and the furnace was in an undefined condition which resulted in massive damage to the whole system."		

[notitie] RISI - risidata.com – NB: NOT UPDATED!!!
Repository of Industrial Security Incidents (RISI)

Last Updated: Wed, January 28, 2015

Updates to this database are currently on hold. We hope to proceed with updating it soon. Thank you for your patience.

Title	Year	Industry Type	Country	Brief
Page 1 of 9 pages **1** 2 3 > Last ›				
Process Control Network Infected with a Virus	2012	Petroleum		
Gas Company Virus Infection	2012	Petroleum		
Steel plant infected with Conficker	2011	Metals		
Computer Glitch Causes Airplane Plunge	2008	Transportation	Australia	
Computer glitch blamed for train signalling failure	2011	Transportation	Australia	

Leren van incidenten

- FSISAC
- ISAC – energy

- Database
  - Overheid
  - Online

...en in 2019?

Delen – TLP:White

jako.jellema@agentschaptelecom.nl
linkedin.com/in/jakojellema/
twitter.com/jakojellema
+31(0)6 161 33 471

Weerbaarheid verhogen door informatiedeling

- Frans van den Akker
  & Jako Jellema
  ISPT – Grip op drogen
- Floor Terra
  Privacy Company
- Jeroen Poldervaart
  ANDRITZ