



KIVI Security avond

IT & OT security

De RWS aanpak

Jeroen Gaiser, MSc BSc CISSP
Rijkswaterstaat



@Whoami



LinkedIn
(trust me)

Who am I?

- > IT (side)jobs sinds 1995
- > Begonnen met techniek/(applicatie)beheer, nu focus op beleid/governance
- > Security focus sinds 2010
- > Werkzaam bij RWS sinds 2014
 - Lead Architect Cybersecurity
 - Coordinating advisor Cybersecurity

Wat is een Cyber Physical System?

ook wel: Operational Technology (OT)

"Cyber-Physical Systems (CPS) are integrations of computation and physical processes."

E. A. Lee, "Cyber Physical Systems: Design Challenges," 2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC), vol. 00, no. , pp. 363-369, 2008.
doi:10.1109/ISORC.2008.25

Voor deze presentatie:

Systemen die een digitale actie (Vb. uit software) omzetten in een actie in de fysieke wereld en vice versa.



- > Gemeenschappelijk doel: zorgen voor correcte en betrouwbare werking
- > IT incident: dienst onbereikbaar
- > OT incident: mens/omgeving in gevaar
- > Overzicht belangrijkste verschillen

IT vs OT

	IT	OT/ICS
Performance	Consistent response High throughput of data Delay and jitter are OK	Real-time Response is time-critical Response is deterministic Modest throughput Delay/jitter unacceptable
Availability	Reboot acceptable Small availability issues are OK DoS not critical to business Ops	Always available demand Redundancy is commonplace DoS has significant impact
Security Architecture	Protect IT assets (data in transit/rest) Controls are found everywhere Pentest tools are used	Protect the edge Not many controls at processing level (PLC) Pentesting will break stuff (e.g. portscan)
Users	Everybody	Engineers (user & admin roles)
Risk management	Data CIA Delay of business operations	Human safety first Regulatory compliance, environment impact, equipment damage
Security tooling	LOTS of IT security testing solutions for IT	Tools must be tested before use to ensure no impact on operations/performance
System Operation	Software/systems intended for use with common OS Upgrading/patching is straightforward (and automated)	Different proprietary systems and OS are combined No security capabilities Software changes very complex
Resources	Systems specs can support additional tasks like security controls	Systems designed for (very) specific tasks with no room for additional tasks
Communications	Proprietary and common protocols (slide 17!) Various media used (e.g. serial/Ethernet) Networking requires specific resources and become complex	Standard communication protocols Wired & Wireless Standard networking principles
Change management	Changes are 'going concern' Automation common & increasing	Changes must be thoroughly tested Outages must be planned months beforehand Lack of support on e.g. OS is common
Support	Multiple service providers	Single vendor
Component lifetime	3-5 years	15-20 years
Access to components	Good accessibility	Locations can be isolated and require effort to reach (buoy at sea)



Digitalisering van objecten impoortert IT risico's

- > Digitization of assets has great efficiency & effectivity benefits
- > IT components/libraries find their way into OT
- > Distinction (tech) between IT & OT is fading (a bit)
- > Example: EKANS ransomware



EKANS

"With a limited set of ICS-specific malware in existence, EKANS, though primitive, represents an evolution in adversaries targeting control system environments."

Dragos

> Kills specific ICS processes

- GE's Proficy data historian
- Honeywell's HMIWeb application
- ThingWorx Industrial Connectivity Suite.

> User can access system

- Less disruptive than LockerGoga (Norsk Hydro)
- Focus on enterprise network compromise instead of self-propagation
- Financial incentive or APT? What does the 'less disruptive' approach signify?

_ctypes_test.pydHHzWX	1/10/2020 12:48 PM	PVDHHzWX File	17 KB
_elementtree.pydalrZN	1/10/2020 12:48 PM	PYDAIRZN File	178 KB
_hashlib.pydXyprM	1/10/2020 12:48 PM	PYDXYPRM File	1,448 KB
_msi.pydZVneo	1/10/2020 12:48 PM	PVDZVNEO File	24 KB
_multiprocessing.pydveQfR	1/10/2020 12:48 PM	PYDVEQFR File	35 KB
_socket.pyddTryq	1/10/2020 12:48 PM	PYDDTRYQ File	50 KB
_sqlite3.pydnoilP	1/10/2020 12:48 PM	PVDNOILP File	63 KB
_ssl.pydpHqpx	1/10/2020 12:48 PM	PYDPHQPX File	2,052 KB
_testcapi.pydkGkY	1/10/2020 12:48 PM	PYDKGKY File	51 KB
_tkinter.pydQVLki	1/10/2020 12:48 PM	PVDQLKI File	51 KB
bz2.pydxbUM	1/10/2020 12:48 PM	PVDNxBUM File	91 KB
py.icoZLDOH	1/10/2020 12:48 PM	ICOZLDOH File	20 KB
py.icoMCoBU	1/10/2020 12:48 PM	ICOMCOBU File	20 KB
pyexpat.pydJSyqK	1/10/2020 12:48 PM	PYDJSYQK File	176 KB
select.pydOmPxn	1/10/2020 12:48 PM	PYDOMPXN File	12 KB
sqlite3.dllDZBgd	1/10/2020 12:48 PM	DLLDZBGD File	768 KB
tk85.dllwMxxt	1/10/2020 12:48 PM	DLLWMXXT File	1,178 KB
tcpip85.dllysoHQ	1/10/2020 12:48 PM	DLLYSOHQ File	10 KB
tk85.dllVRcev	1/10/2020 12:48 PM	DLLVRCEV File	1,732 KB



Cyberaanvallen op vitale infrastructuur



MUST READ

No rei

The show By



WaterNews Podcast Features Zeropolis HotS

WaterNews

Water Sector Prepares For Cyber

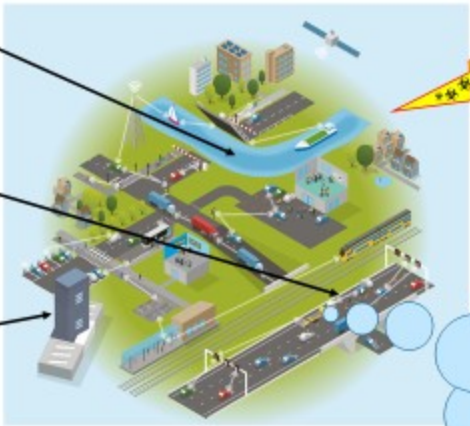
June 9, 2016 / in Infrastructure, United States, Water Management, Water

Security threats evolve as water systems connect to the internet



Our Challenge

- OT**
 - Bridge controls
 - Traffic management signals
 - Storm Surge Barrier controls
- IoT**
 - Water level sensors
 - Bridge alignment sensor
 - Drone inspections
- IT**
 - Laptops/desktops
 - Datacenter
 - Devices
 - Network



Cyber Security Assessment Netherlands



Context:

- Complex supply chain
- Safety vs security language
- Awareness
- Riskmanagement

REPORT SEEN AS 'GENTLE REMINDER'

Cyberattack on Israel's water supply could have hundreds – report

April hack aimed to raise chlorine to dangerous levels, says attack began tit-for-tat on civilian targets



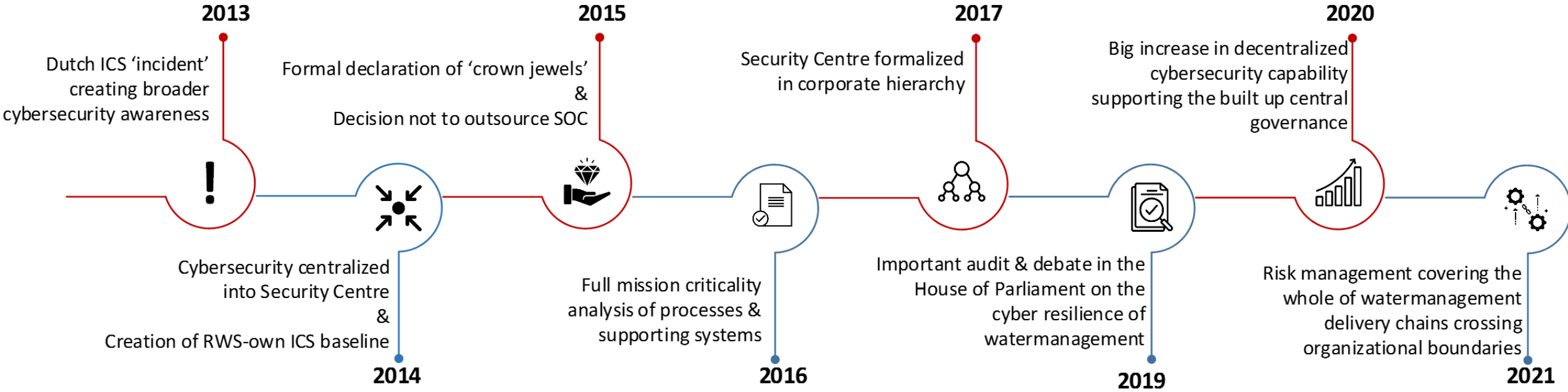
group known as the banoffee team – widely reported to have links to Russian intelligence service – began emulating BlackEnergy (BE2) to conduct espionage against industrial control system networks. The malware is highly modular, meaning it consists of many different components which serve different functions and not all functionality is delivered to all victims.

Most recently, BlackEnergy3 (BE3) was involved in the 2015 cyberattacks in Ukraine that resulted in power outages. Although BE3 did not have a direct role in cutting off the power, it was used in the lead-up to the attack to collect information about the ICS environment and was likely used to compromise user credentials of network operators. Unlike previous incidents involving variants of BlackEnergy, BE3 was delivered to the Ukrainian energy companies via spear-phishing emails and weaponized Microsoft Word documents.

Prior to the involvement of BE3 in the attacks in Ukraine, BE2 made the news in 2014 when it was found to have infected numerous critical infrastructure sites in the United States. Unlike BE3, BE2 gained access to networks by exploiting vulnerabilities in internet-connected ICS devices, specifically Human Machine Interface (HMI) products from various vendors, including GE Cimplicity, Advantech/Broadwin WebAccess, and Siemens SIMATIC WinCC. Compromising internet-connected HMI devices provided the malicious actors with a foothold on the network that allowed them to maintain command and control, and collect information on the ICS environment and its processes. According to numerous media and government reports, BE2 infections in the United States began as early as 2011 and affected the water, energy, rail, estate, and telecommunications sectors. However, to date, there are no public reports of BE2 or BE3 damaging, modifying, or otherwise disrupting victimized ICS networks in the United States.

Indicators of Compromise (IOCs)







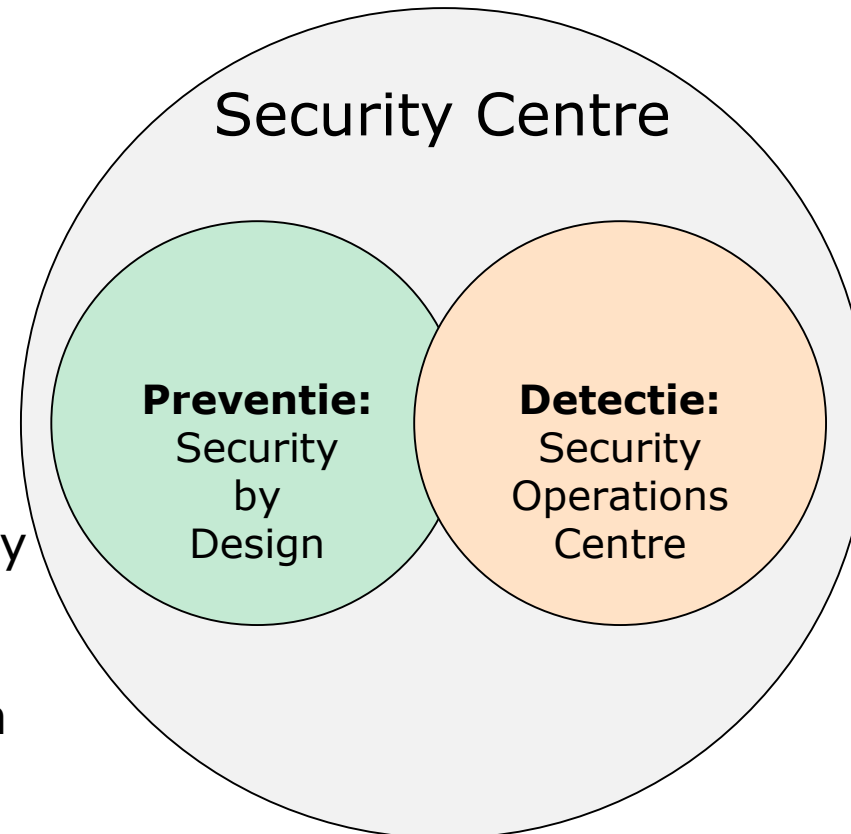
De RWS aanpak

- > IT en OT holistisch aanpakken en niet in silo's
- > Multi disciplinair security team
- > Cybersecurity inbedden in bestaande voortbrengingsprocessen
- > Samenwerking tussen security experts en engineers is essentieel!
- > Governance cybersecurity omvat alle digitale risico's



Organisatie: Preventie & detectie

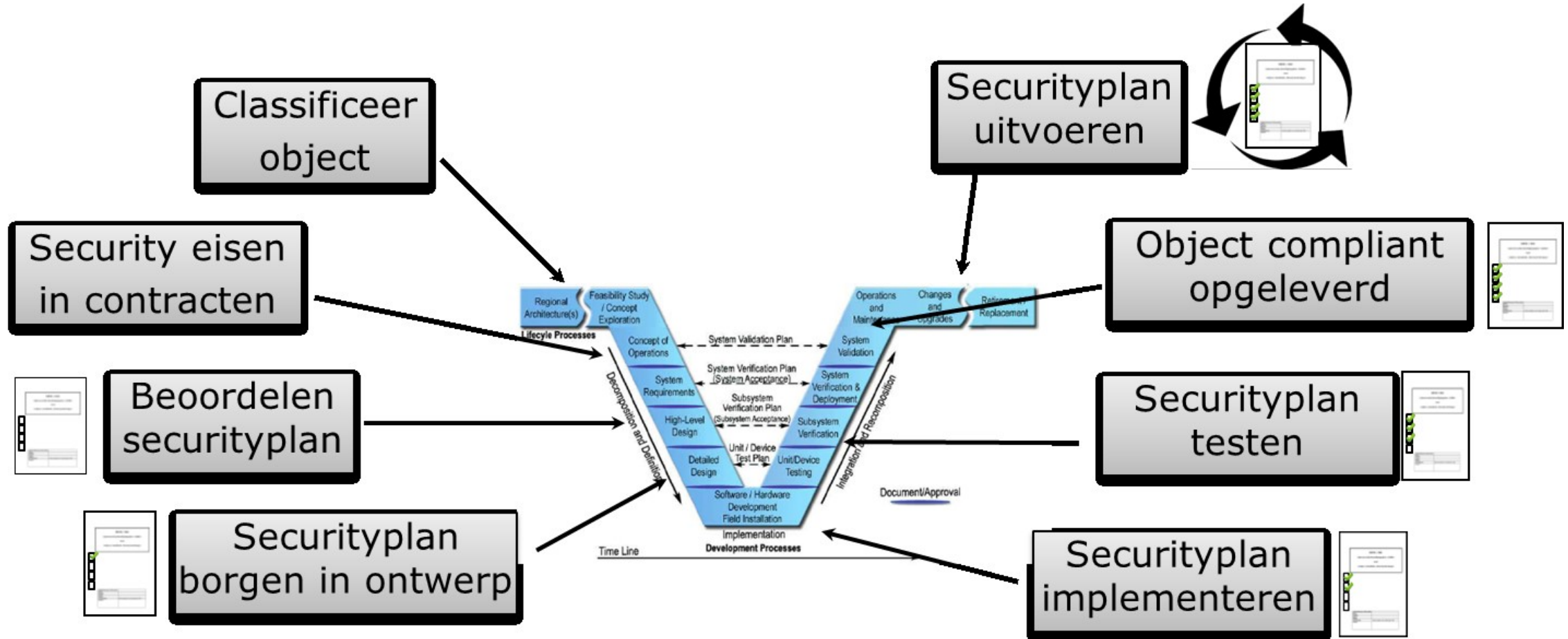
- Zo vroeg mogelijk in een bouwtraject security eisen meegeven
- Zowel bij IT als Industriële Automatisering (objecten)
- Voor IT: BIO
- Voor IA: CSIR (Cybersecurity Implementatie Richtlijn Objecten)
- Advies bij ontwerp, bouw en beheer



- Monitoring van IT en OT infrastructuur oa de RWS netwerken
- Monitoring van objecten is aparte uitdaging
- Analyseren ca 34,5 miljard (!) events per week
- Threat intelligence
- Forensics
- Pentesting
- Expert bij een incident of CERT

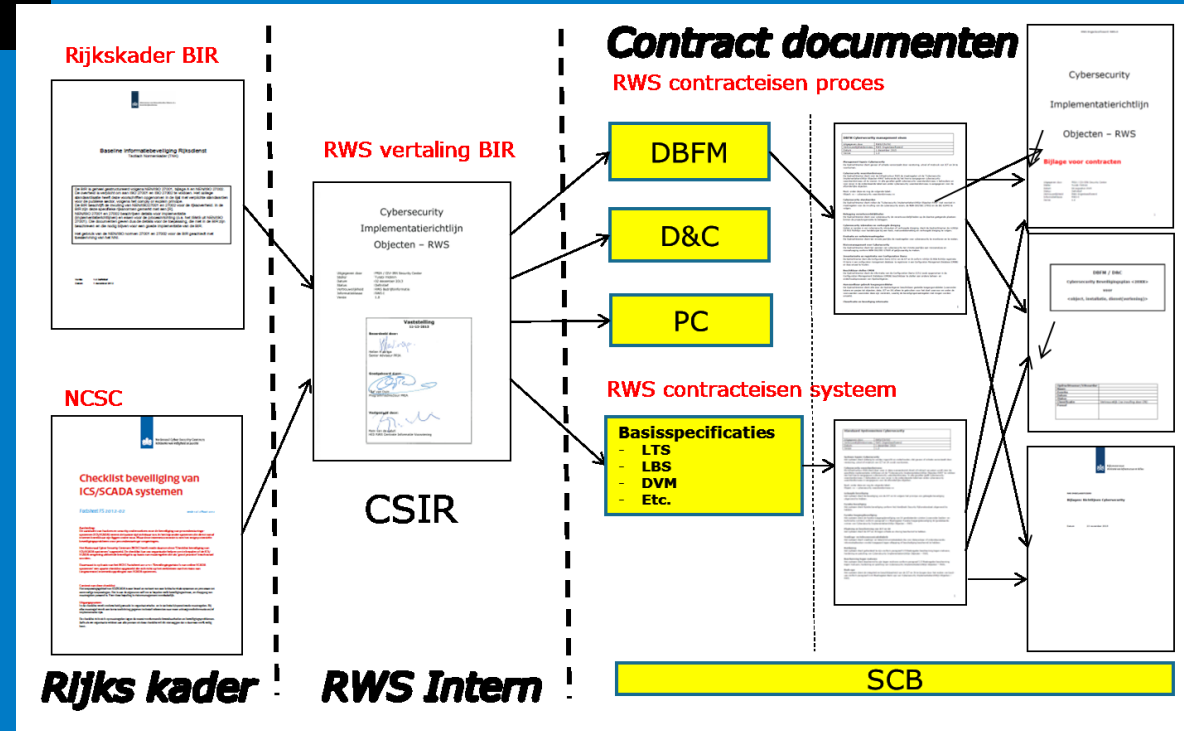


Security in OT lifecycle





CSIR: Cybersecurity Implementatierichtlijn Objecten RWS



BOX	Weerstands niveau
A	4
B	3
C	2
D	1
E	





Vragen?

