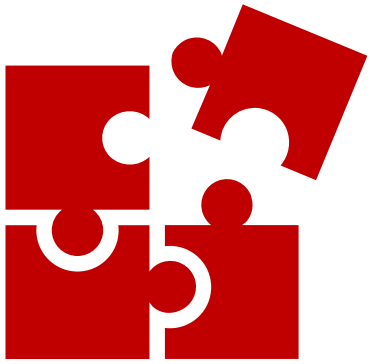
Sist oppdatert 27.09.2023

TTK 2 – Design og analyse for funksjonell sikkerhet 2023

Seminar 4 – 27.09.2023

MARY ANN LUNDTEIGEN

TEKNISK KYBERNETIKK NTNU



4. Cybersikkerhet og sikkerhet

Motivasjon

Sikkerhet handler om å beskytte seg mot risiko for skade på personer, miljø og anlegg. Å ivareta sikkerhet har betydd å dimensjonert systemer for å håndtere **tilfeldige feil** som kan skyldes fysiske svikt, hendelser i omgivelser og menneskelige feilhandlinger.

Cybersikkerhet handler om mulig tap av IKT systemer som et resultat av **villede handlinger** der man i prinsippet kan «designe» hendelser som det ikke er beskyttelse mot.

Sikkerhets-domenet:

Risiko for skade på mennesker, miljø, eiendeler/ infrastruktur

Tilfeldige og utilsiktede hendelser

Identifiserer og implementerer sikkerhetsbarrierer

Security domenet:

Risiko for skade på IKT relaterte systemer og nettverk

Tilsiktede og uautoriserte handlinger

Identifiserer og implementerer cybersikkerhets-barrierer (countermeasures, security level measures)

Litteratur

Pensum:

- Slides
- Den teori fra standarder som må slås opp i/finne tak i for å løse gruppeoppgavene

Nyttig tilleggslitteratur

- Referanser gitt til litteratur i slides
- https://www.exida.com/blog/iec-62443-levels-levels-and-more-levels

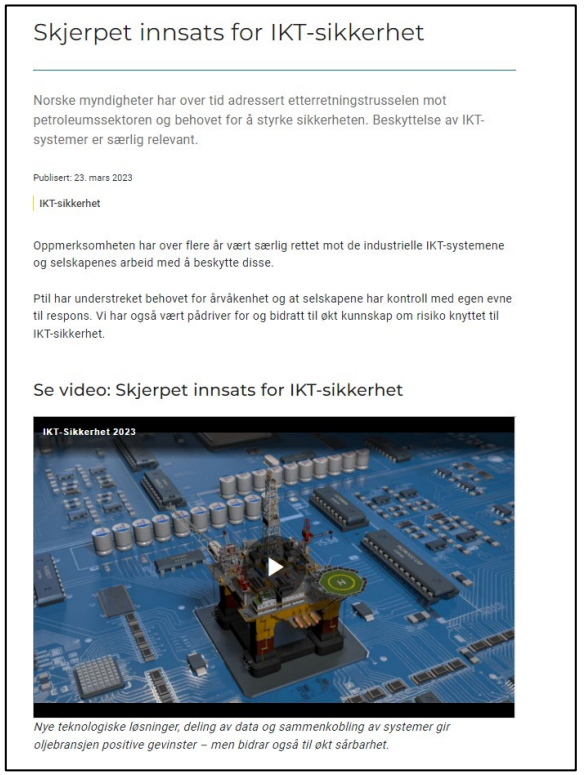
Begrepsavklaringer

Begrepsavklaring

- På norsk mangler vi begrep som skiller **Safety** og **security** slik det gjøres på engelsk
  - Begge engelske begrep oversettes til **sikkerhet** på Norsk – men konteksten og betydningen blir forskjellig

- Derfor har man i flere norske miljøer introdusert følgende **oversettelse** av **security**:
  - **Cybersikkerhet**
  - **IKT sikkerhet**
  - IT sikkerhet
  - …

- Cybersikkerhet/IKT Sikkerhet: Fokus på internetbaserte trusler og påvirkning ovenfor systemer og nettverk. Å oppnå cybersikkerhet er avhengig av både tjenester, systemer, mennesker og infrastrutkru


Skjerpet innsats for IKT-sikkerhet

Norske myndigheter har over tid adressert etterretningstrusselen mot petroleumssektoren og behovet for å styrke sikkerheten. Beskyttelse av IKT-systemer er særlig relevant.

Publisert: 23. mars 2023

IKT-sikkerhet

Oppmerksomheten har over flere år vært særlig rettet mot de industrielle IKT-systemene og selskapenes arbeid med å beskytte disse.

Ptil har understreket behovet for årvåkenhet og at selskapene har kontroll med egen evne til respons. Vi har også vært pådriver for og bidratt til økt kunnskap om risiko knyttet til IKT-sikkerhet.

Se video: Skjerpet innsats for IKT-sikkerhet

Nye teknologiske løsninger, deling av data og sammenkobling av systemer gir oljebransjen positive gevinster – men bidrar også til økt sårbarhet.

https://www.ptil.no/fagstoff/utforsk-fagstoff/fagartikler/2023/styrket-ikt-sikkerhet/


STORE NORSKE LEKSIKON

Søk i Store norske leksikon

cybersikkerhet

Store norske leksikon / Samfunn / Forsvar og sikkerhet / Samfunnssikkerhet og beredskap / Data- og informasjonssikkerhet

Cybersikkerhet er en utvidelse av fagområdet datasikkerhet, som også tar for seg IT-baserte enheter og infrastruktur. Cybersikkerhet fokuserer på internett-relaterte trusler.

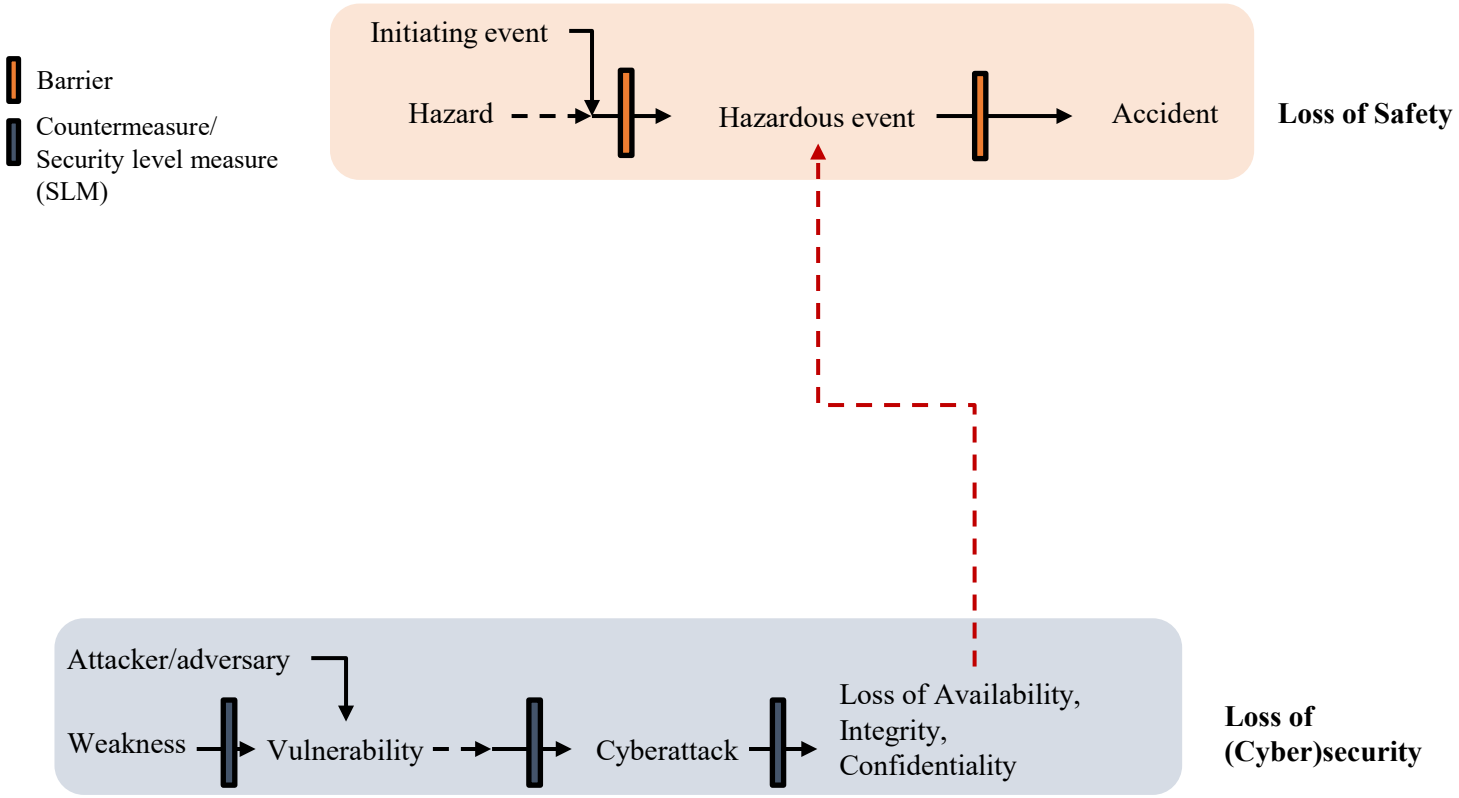
SKREVET AV FØRSTELEKTOR Tom Heine Nätt HØGSKOLEN I ØSTFOLD

OGSÅ KJENT SOM engelsk *cyber security*

Cybersikkerhet er ikke direkte knyttet til informasjonen som oppbevares, men til tjenestene, systemene, menneskene og infrastrukturen rundt. Ved å sikre disse vil imidlertid også informasjonen indirekte sikres. Cybersikkerhet omhandler aktive handlinger gjort av en trusselaktør, ikke uhell og feil som oppstår.

https://snl.no/cybersikkerhet

Mulige sammenhenger mellom sikkerhet og cybersikkerhet



Safety: Freedom from unacceptable risk

Cybersecurity: Actions required to preclude unauthorized use of, denial of service to, modifications to, disclosure of, loss of revenue of, or destruction of critical systems or information assets”

Eksempel på sammenheng sikkerhet og cybersikkerhet

Eksempel: BP texas city raffineriulykken

Operasjonelle feilhandlinger og sensorfeil…

…førte til lekkasje av brennbar væske ut gjennom fakkeltårnet, noe som førteantennelse og brann med 15 mennesker drept og 150 skadet

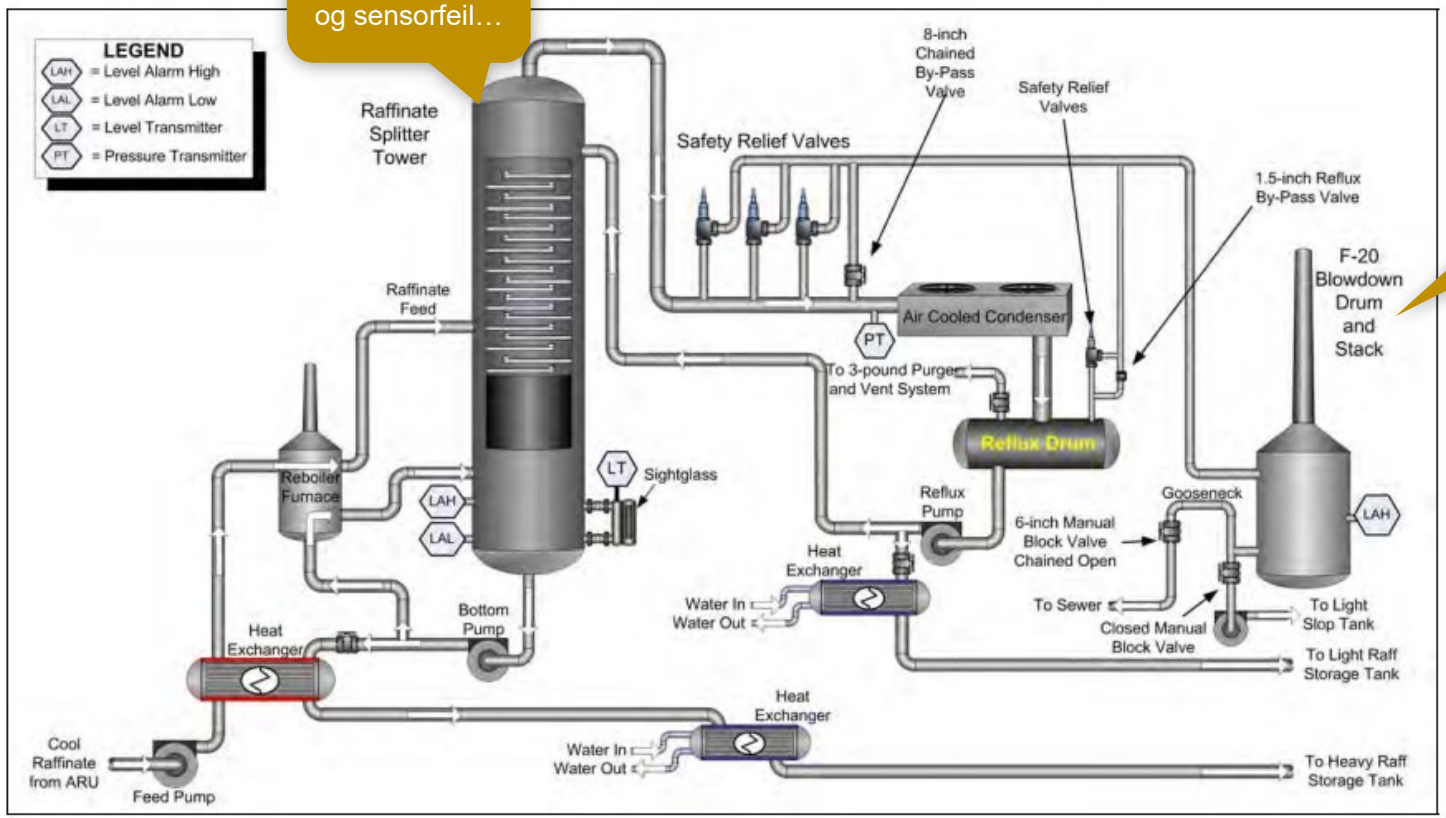


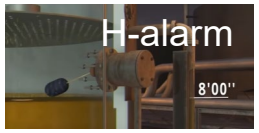
Figure 1. Raffinate section of the ISOM

Basert på BP ulykken (2005) https://www.csb.gov/bp-america-texas-city-refinery-explosion/

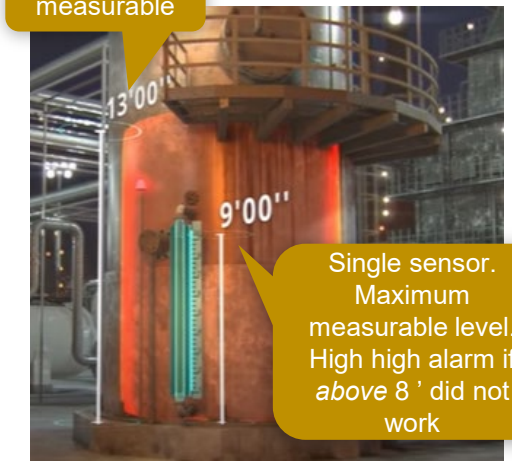
BP texas ulykken oppsummert

Practice

Procedure



Not measurable



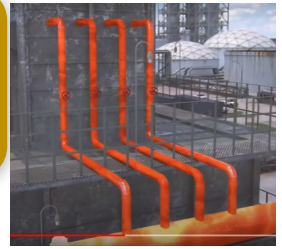
Single sensor. Maximum measurable level. High high alarm if *above* 8 ' did not work

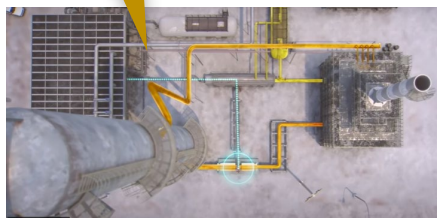
Night shift started to fill the Raffinate splitter tower. Common to do some overfilling,

Maximum (measurable) liquid level exceeded measurement range without any reporting (common deviating from prescribed procedure)

Furnace started according to procedure to heat liquid

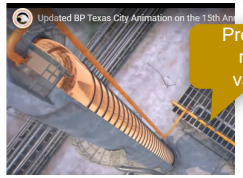
Lack of monitoring of flow in and out of tower





Day shift continued to fill and circulate liquid. Burner started to heat up the feed. Relied on level control using level control valve. Valve was left closed as the liquid still measured 9''.

Also, a series of organizational failures. Events caused by failed instrumentation hide to operators what was going on.



Pressure relief valves

Dangerous high level not discovered. Overfilling led to liquid into gas outlet with pressure relief valves.

Pressure relief valves all opened and liquids sent to liquid drum in flare system. High level alarm failed to alarm.

Liquid started to pour out of the flare tower, creating also a large flammable cloud

Heat from parked truck ignited the vapor, leading to explosion.

Vapor cloud spread to nearby areas with truck storage unit

Basert på BP ulykken (2005) https://www.csb.gov/bp-america-texas-city-refinery-explosion/

Spørsmålet er …

- Kunne denne ulykken skjedd i dag som et resultat av *et digitalt angrep*

Et digitalt angrep kunne ha…

.. Manipulert operatørskjermene slik at alt så normalt ut

…Manipulert for høyere temperatur i olje til varmeveksler

…Manipulert stopp av pumpe utløp bunnen

Manipulert sensoravlesning, endret på alarmsettpunkt

…Åpning av ventil som kan styres fra kontrollsystem

…Ikke visning av høytnivå i fakkeltank

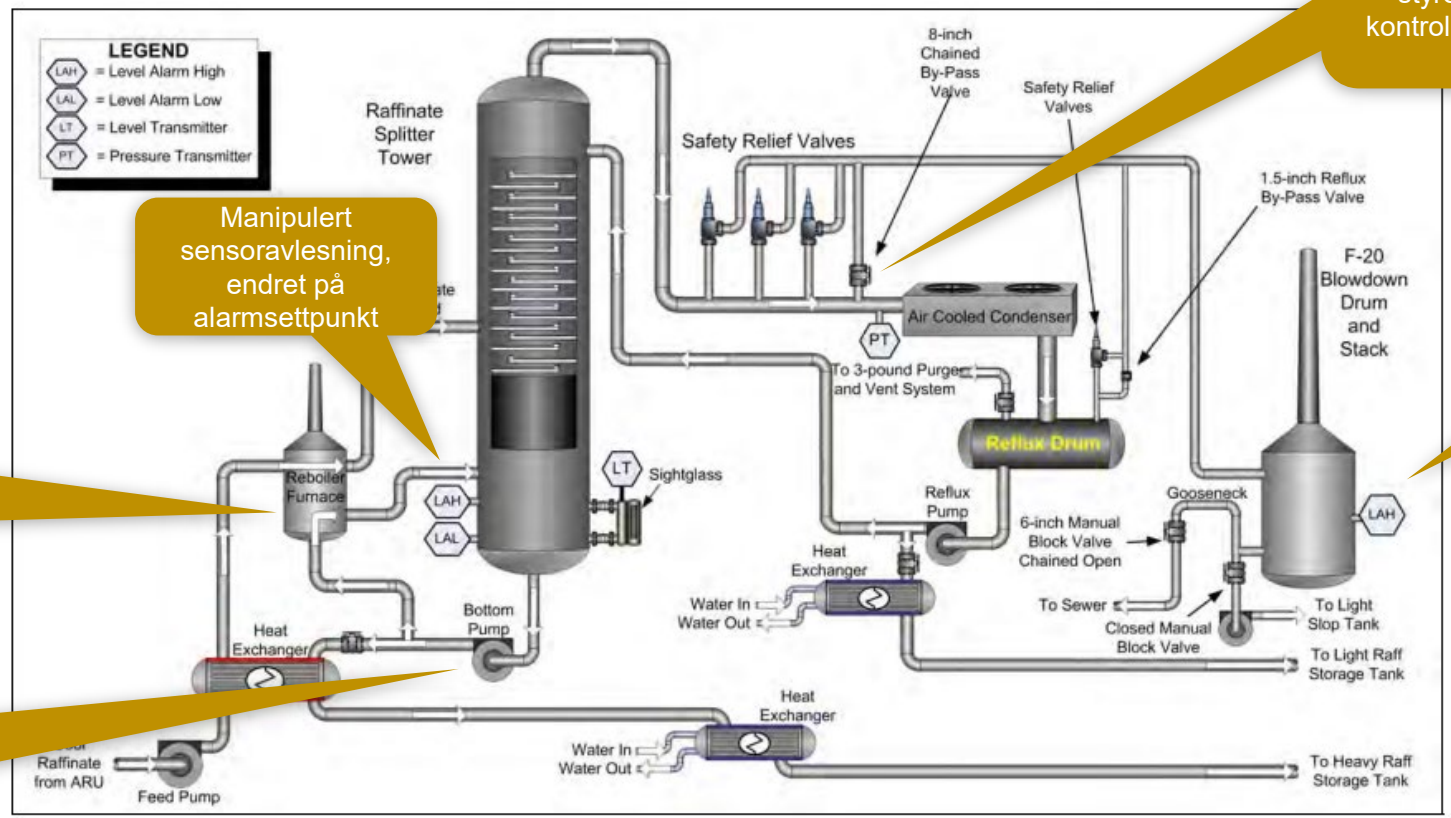
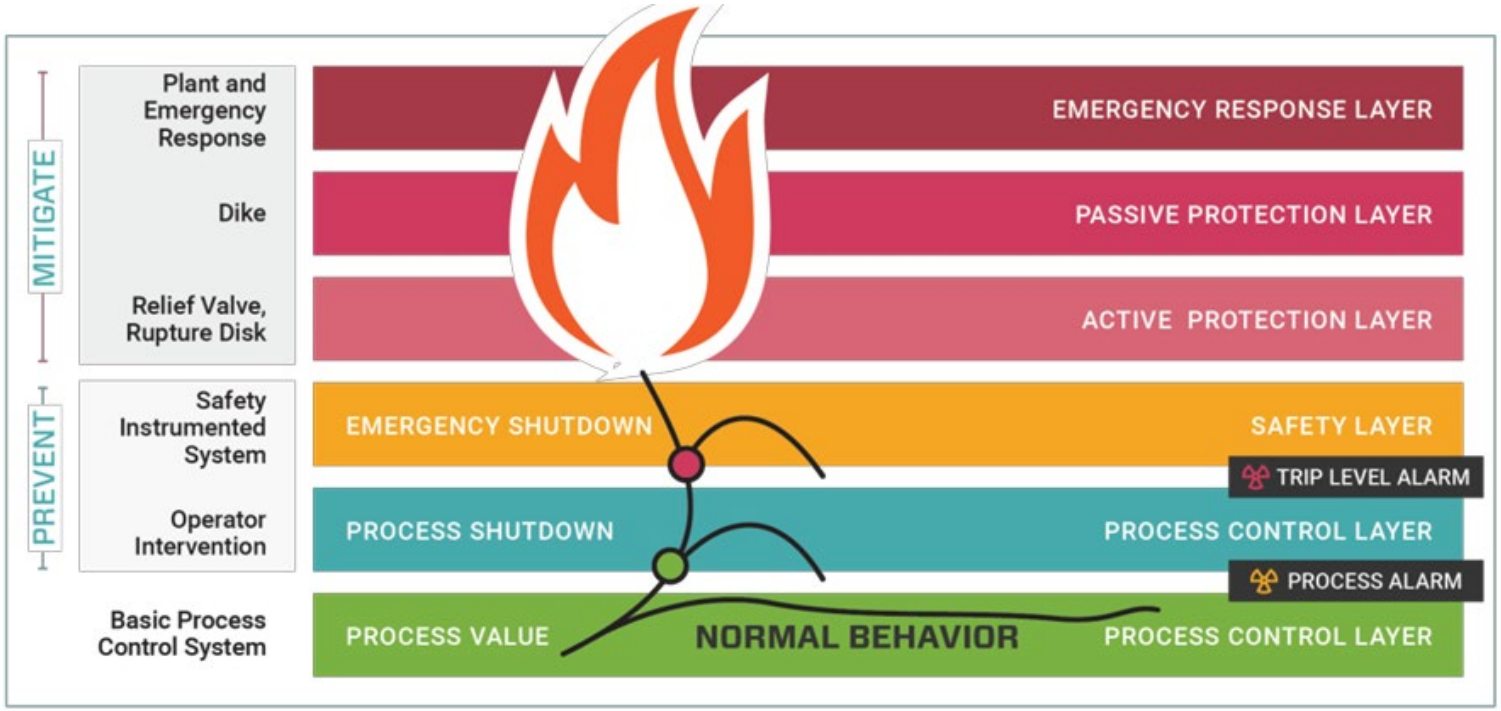


Figure 1. Raffinate section of the ISOM

Basert på BP ulykken (2005) https://www.csb.gov/bp-america-texas-city-refinery-explosion/

Angripere kan bevisst …

- Trigge unormale hendelser
- Koble ut eller gjøre sikkerhetsbarrierer mindre effektive
- Skape kombinasjoner av hendelser som er «usannsynlige»
- Fjerne eller redusere mulighet for manuell inngripen
- …

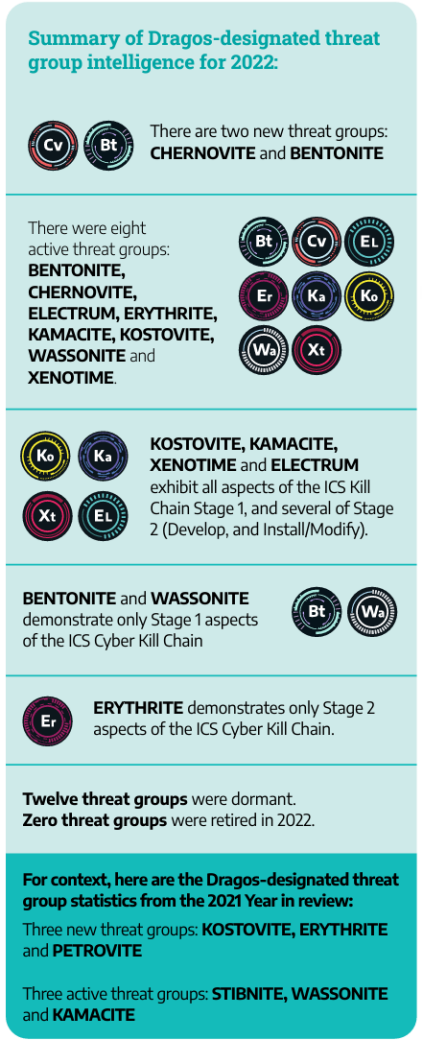


Kilde: https://www.dragos.com/wp-content/uploads/Past-and-Future-of-Integrity-Based-ICS-Attacks.pdf

Angrep og angrepsstrategi mot industrielle anlegg

Angriperen mot industrielle anlegg

- Ofte ressurssterke grupper med statlig finansiering og/eller involvering
- Ofte gitt navn av organisasjoner (som Dragos) som følger med på virksomheten
- Angrep planlegges og gjennomføres ofte av to typer angrepsgrupper – hver med sin spesialkompetanse:
  - «Stage 1»: De som er spesialister på å komme seg inn på kontornettet.
  - «Stage 2»: De som er spesialister på digitalt utstyr og nettverk på industrielle anlegg
- Angrep kan også planlegges indirekte – ved å infisere utstyr hos underleverandører
  - Virus kan overføres med infisert programvare i utstyr og verktøy
  - Virus kan implementeres i hardware «fysiske trojaner» (krever fysisk tilgang til design og fabrikasjon)

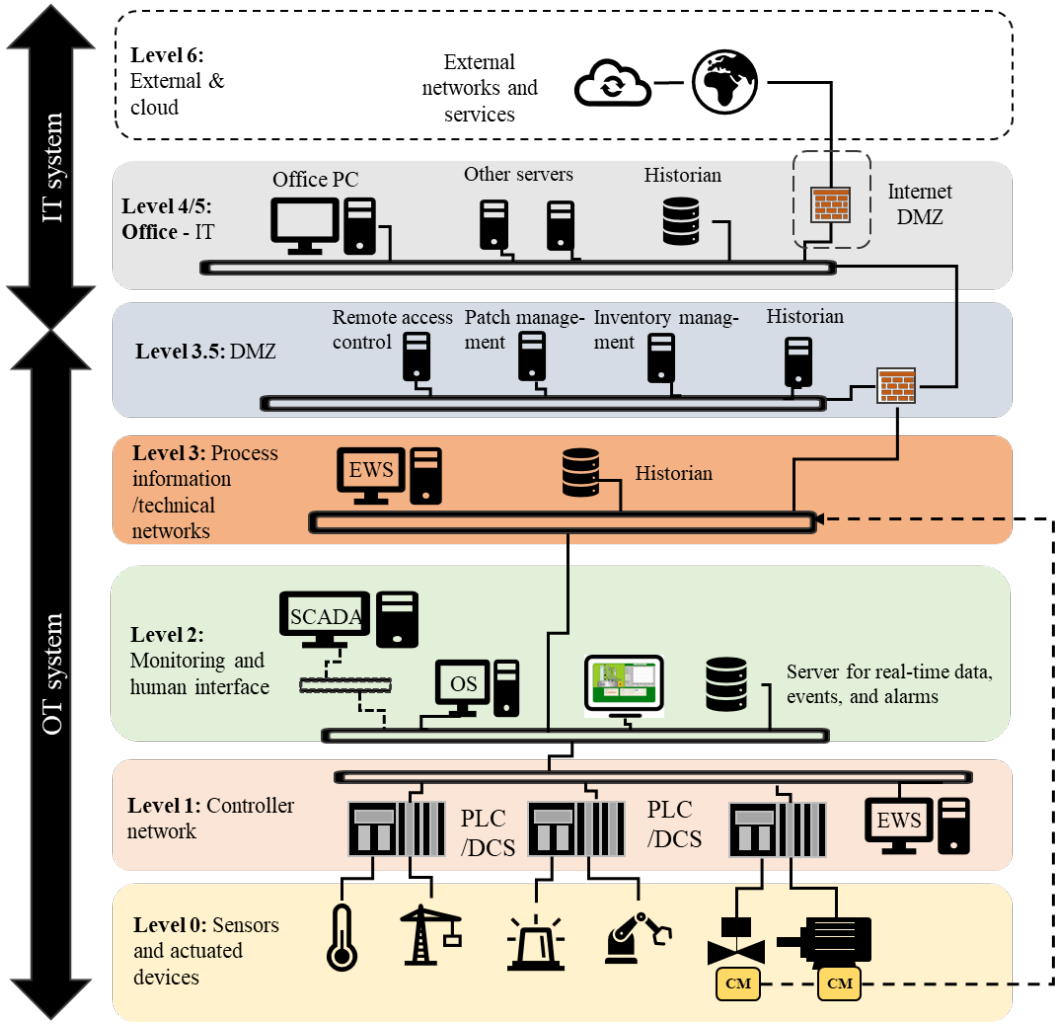


Angripere refereres til som «attacker», «adversary» eller «intruder». Samme betydning.

Kilde: https://www.dragos.com/year-in-review/#section-report . Se også: https://www.dragos.com/threat-groups/

Hvilke nettverk møter angriperne?

- Purdue referansearkitektur viser en typisk layout:
  - Lagvis – organisert etter hovedfunksjoner
  - Tydelig skille mellom IT-delen (Kontornettet) og OT-delen (fabrikken, anlegget)
  - Forbindelse mellom de to via en sikret sone (DMZ)
- I praksis finnes varianter av denne:
  - Tilpasset ulike anlegg
  - Utvikling av nettverk over tid (25 år) *kan* også medføre ukjente forbindelser…



Om Purdue modellen:
https://www.youtube.com/watch?v=c81YnS-Syik

OT: Operational Technology, DMZ: Demilitarized zone

OT sikkerhet vs IT sikkerhet

IT siden

- Eksponert mot internet «hele tiden»
- Stort sett oppdatert IT teknologi
- Kan patche (oppgradering som fjerner sårbarheter) uten større konsekvenser

OT-siden

- Ikke direkte eksponert
- Tilganger er styrt og kontrollert (remote access)
- OT utstyr over flere generasjoner – både nytt og gammelt (20 år +)
- Patching krevende – kan medføre produksjonsstans og midlertidig utkobling sikkerhetssystemer

Men jeg lager jo bare en liten komponent…

- Leveransekjedeangrep (supply chain attack) er en stor bekymring
- Klarer en angriper å plassere en sårbarhet i et produkt som senere installeres inngår i en eller flere leveranser kan gi større muligheter for å utføre skade i anleggene utstyret står (access vector/attack vector)
- At alle underleverandører og deres underleverandører osv har kontroll på cybersikkerhet er avgjørende


THE WALL STREET JOURNAL.

ZTE | WSJ
Compliance Creates Value
Why compliance culture should be at the heart of every business strategy.
DISCOVER MORE

PRO CYBER NEWS
SolarWinds Hack Forces Reckoning With Supply-Chain Security
Companies are re-evaluating how they vet vendors and pausing software updates

solarwinds
BIDEN HARRIS
Biden White House Faces Three Problems From Suspected Russian Hack

A suspected Russian cyberattack of the federal government has breached at least six cabinet-level departments. WSJ's Gerald F. Seib explains what the hack means for President-elect Joe Biden's national security efforts. Photo illustration: Laura Kammermann

By David Uberti and Kim S. Nash
Jan. 14, 2021 5:30 am ET | WSJ Pro

Har underleverandøren kontroll på softwareutvikling og softwarevedlikehold?

https://www.wsj.com/articles/solarwinds-hack-forces-reckoning-with-supply-chain-security-11610620200

Har underleverandøren kontroll på hele utviklingen av hardware/chips?

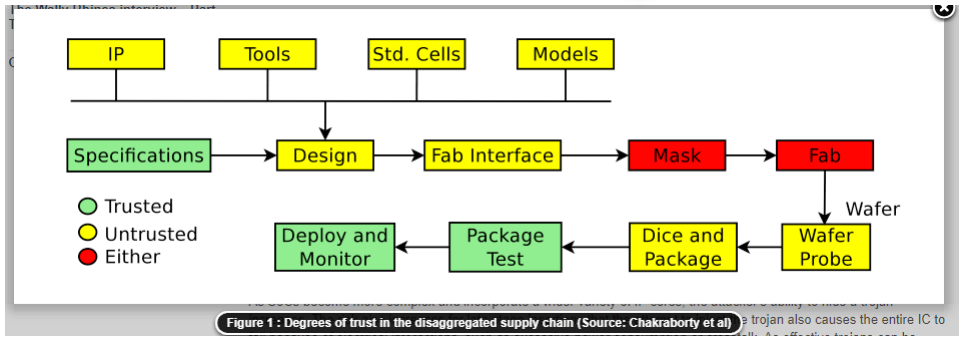


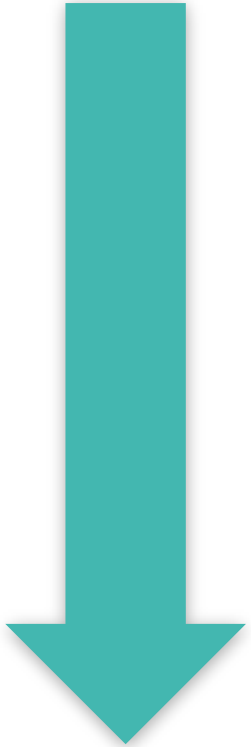
Figure 1 : Degrees of trust in the disaggregated supply chain (Source: Chakraborty et al)

https://www.techdesignforums.com/practice/guides/hardware-trojan-security-countermeasures/

Målet med angrepet

- Loss of:
  - View (operator screen, alarms)
  - Control (control logic, readings, actions, remove power supply…)
  - Safety (inhibit inputs, inhibit outputs, remove power supply (loosing readings)…)
- Denial of («Denial of service» - DOS):
  - View (intervene in what is available for view)
  - Control (intervene in communication/denial of service)
  - Safety (intervene in communication,…)
- Manipulation of:
  - View
  - Control
  - Sensors and instruments (change calibration parameters, settings,..)
  - Safety (e.g., change voting)

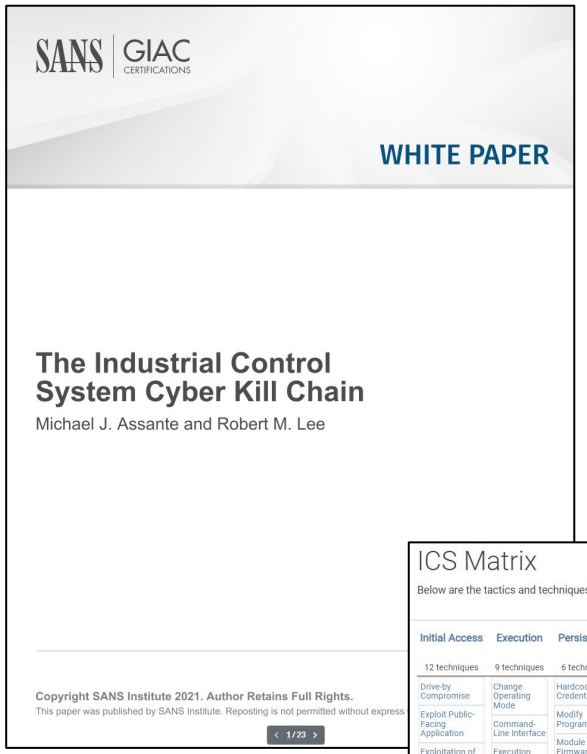
Kritikalitetsskala (?)



Sikkerhetssystemer vil ofte bidra til sikker tilstand i anlegget ved Loss of/bortfall og DOS, men mer uklart om sikker tilstand kan oppnås dersom systemene er manipulert

To kjente måter å beskrive angrepsstrategier

- ICS Cyber Kill Chain
- Mitre Attack matrix


SANS | GIAC CERTIFICATIONS

WHITE PAPER

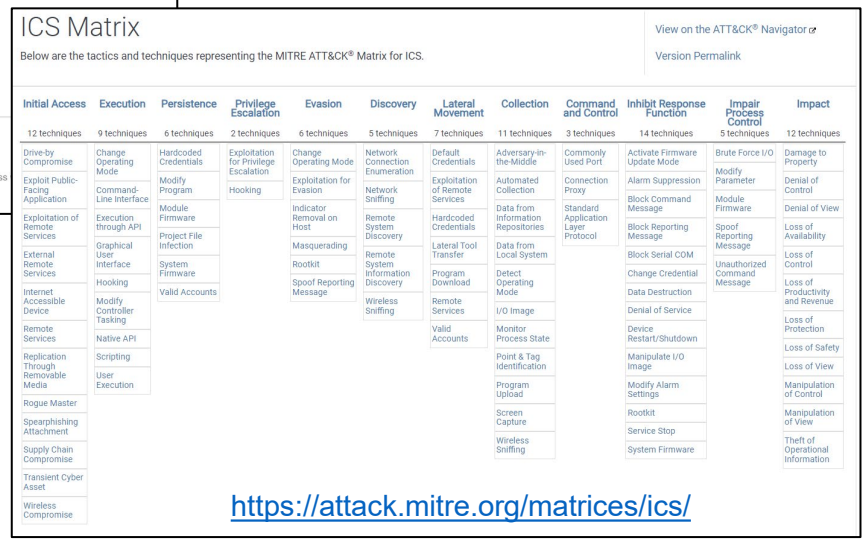
The Industrial Control System Cyber Kill Chain

Michael J. Assante and Robert M. Lee

Copyright SANS Institute 2021. Author Retains Full Rights.

This paper was published by SANS Institute. Reposting is not permitted without express

https://www.sans.org/white-papers/36297/


ICS Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for ICS.

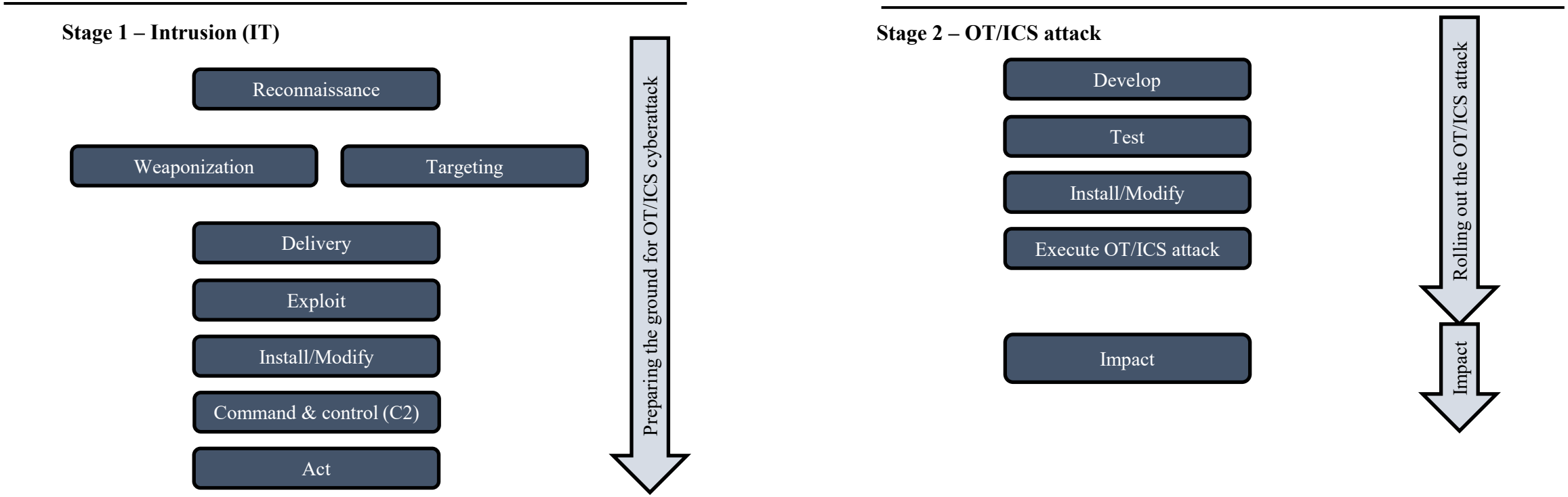
View on the ATT&CK® Navigator

Version Permalink

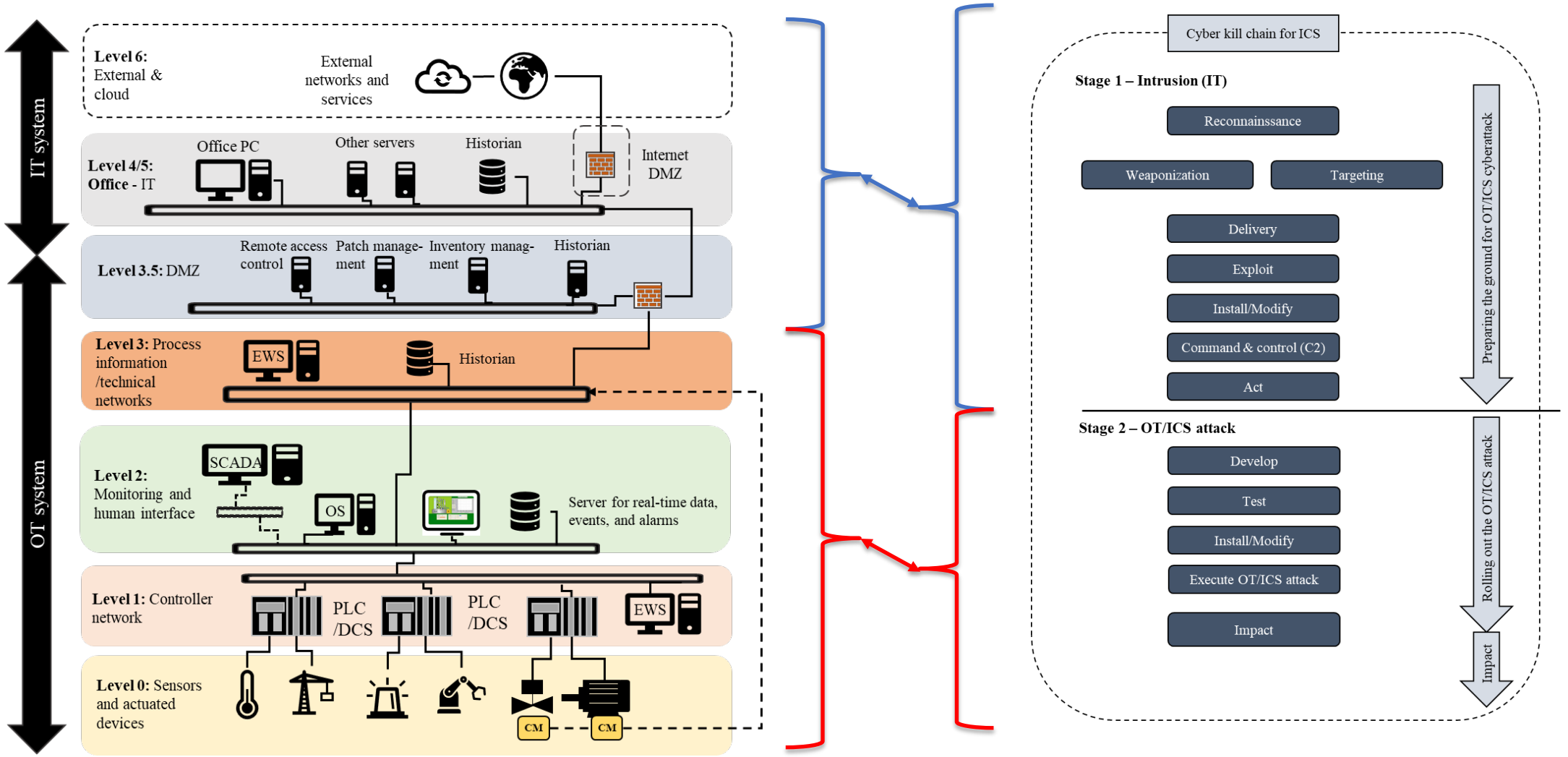
Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
12 techniques	9 techniques	6 techniques	2 techniques	6 techniques	5 techniques	7 techniques	11 techniques	3 techniques	14 techniques	5 techniques	12 techniques
Drive-by Compromise	Change Operating Mode	Hardcoded Credentials	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Adversary-in-the-Middle	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Command-Line Interface	Modify Program	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Automated Collection	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Execution through API	Module Firmware		Indicator Removal on Host	Remote System Discovery	Hardcoded Credentials	Data from Information Repositories	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
External Remote Services	Graphical User Interface	Project File Infection		Masquerading	Remote System Information Discovery	Lateral Tool Transfer	Data from Local System		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Hooking	System Firmware		Rootkit	Wireless Sniffing	Program Download	Detect Operating Mode		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	Modify Controller Tasking	Valid Accounts		Spoof Reporting Message		Remote Services	I/O Image		Change Credential		Loss of Productivity and Revenue
Replication Through Removable Media	Native API					Valid Accounts	Monitor Process State		Data Destruction		Loss of Protection
Rogue Master	Scripting						Point & Tag Identification		Denial of Service		Loss of Safety
Spearphishing Attachment	User Execution						Program Upload		Device Restart/Shutdown		Loss of View
Supply Chain Compromise							Screen Capture		Manipulate I/O Image		Manipulation of Control
Transient Cyber Asset							Wireless Sniffing		Modify Alarm Settings		Manipulation of View
Wireless Compromise									Rootkit		Theft of Operational Information
									Service Stop		
									System Firmware		

https://attack.mitre.org/matrices/ics/

Cyber killchain



Cyber kill chain for ICS



Kilde: https://www.sans.org/white-papers/36297/

Cyber kill chain

Stage 1 – Intrusion (IT)

Reconnaissance

Intruder gathers information about potential target, researches it using open tools like google and Shodan, and attempts to identify vulnerabilities in the target network

Intruder creates a suitable weapon by integrating a virus or worm that can steal credentials that give access to a network into e.g., files that can be delivered to or downloaded by targets

Weaponization

Targeting

Intruder prioritize targets and decides on appropriate tools

Delivery

Intruder transmits weapon to target (via email attachments, websites, USB,..). "Phishing".

The malware/virus exploits the vulnerability, meaning that e.g., by exploiting the acquired credentials

Exploit

Install/Modify

The malware/virus installs itself, alternatively uses/modifies an existing capability in the system that can be used for unauthorized purposes

The malware/exploited capability is used to establish a bi- or one way directional communication path.

Command & control (C2)

Use the bi- or one directional communication path to act: e.g., collect information, discover new systems to connect to/access, installation and execution of additional capabilities, collection of additional credentials, … installing anti-forensic techniques (to "on demand" hide/clean traces of their activities)

Act

Cyber killchain

Stage 2 – OT/ICS attack

Develop	*Intruder develops new capabilities tailored to ICS (OT). The capabilities are developed to achieve the ultimate goal of the attacks that can be: Loss of view and/or control, denial of view, control and/or safety, and manipulation of view, control, sensors/instruments and/or safety Not always ready when stage 1 attack is executed but developed using information acquired in stage 1. Could be to develop a capability to modify logic software using a program installed at the engineering station and to connect to the PLC that allows transfer of new programs. It may also involve capabilities for modifying parameters for e.g., configuration of sensors or actuated devices, and manipulating the readings/updates of real-time information at the operator stations.*
Test	*Intruder tests new capabilities as a validation of the planned attack, often using similar ICS equipment at own premises first, before testing inside the actual OT system. Includes also to test that the capabilities are not detected.*
Install/Modify	*Intruder installs or the malware/virus installs the final capabilities onto the target ICS equipment. This can involve*
Execute OT/ICS attack	*The capabilities are executed. For example, the new (unauthorized) version of the program logic is being run on the target PLC or the sensor is operating with new (unauthorized calibration data)*
Impact	*The impact of the capabilities are manifested and can range from minor disruptions to severe damages to the ICS or plant.*

Eksempel: Trisis angrepet (2017)

Designet for å skape en eksplosjon. Første angrep målrettet mot SIS.

Home › Security › Cyber attack on Saudi plant designed to cause explosion

SECURITY March 17, 2018

Cyber attack on Saudi plant designed to cause explosion

Details emerge of Triton attack against plant safety system which caused shutdown in August

By ITP Staff

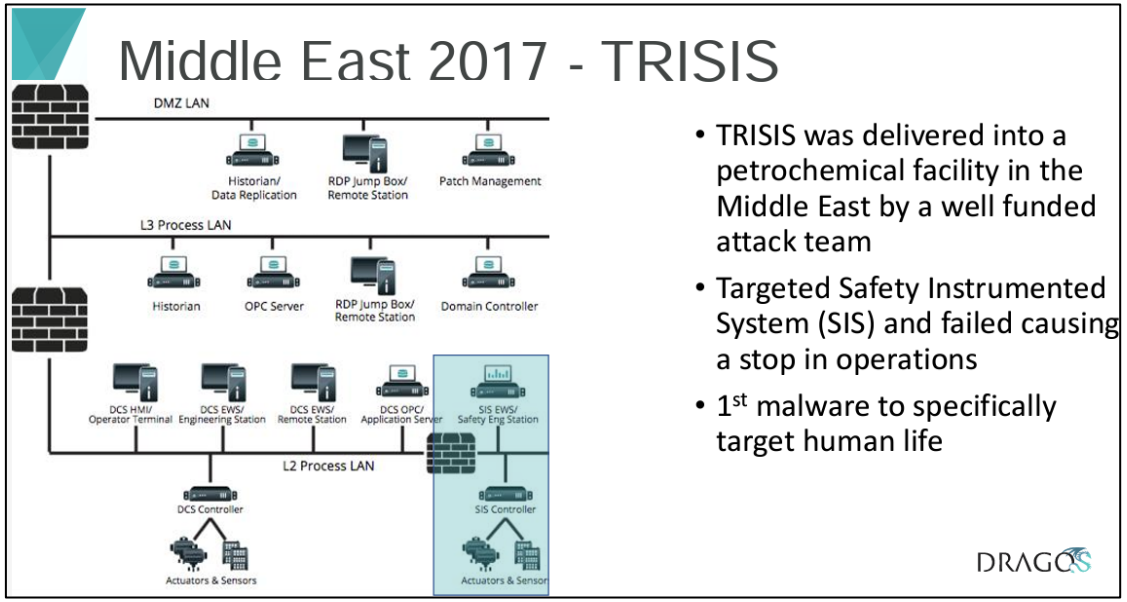
Cyber attack on Saudi plant designed to cause explosion

A cyberattack against a petrochemical company in Saudi Arabia could have caused serious physical damage, according to news reports.

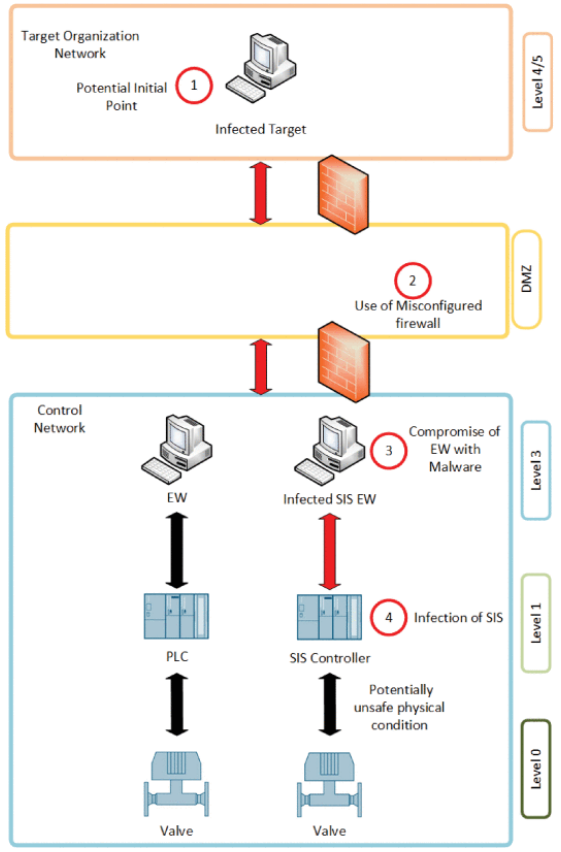
The attack, which was detected in August, appears to have been designed to cause safety controllers to stop working, which could have caused an explosion at the plant.

The attack apparently only failed due to a flaw in the coding of the malware, causing equipment to shut down instead.

Kilde: https://www.edgemiddleeast.com/security/616795-cyber-attack-on-saudi-plant-designed-to-cause-explosion



Kilde: https://www.dragos.com/resource/combating-threats-in-oil-and-gas-environments-with-the-dragos-platform/



Kilde: https://ieeexplore.ieee.org/document/9638617

Teknikker brukt ifbm Trisis/Triton

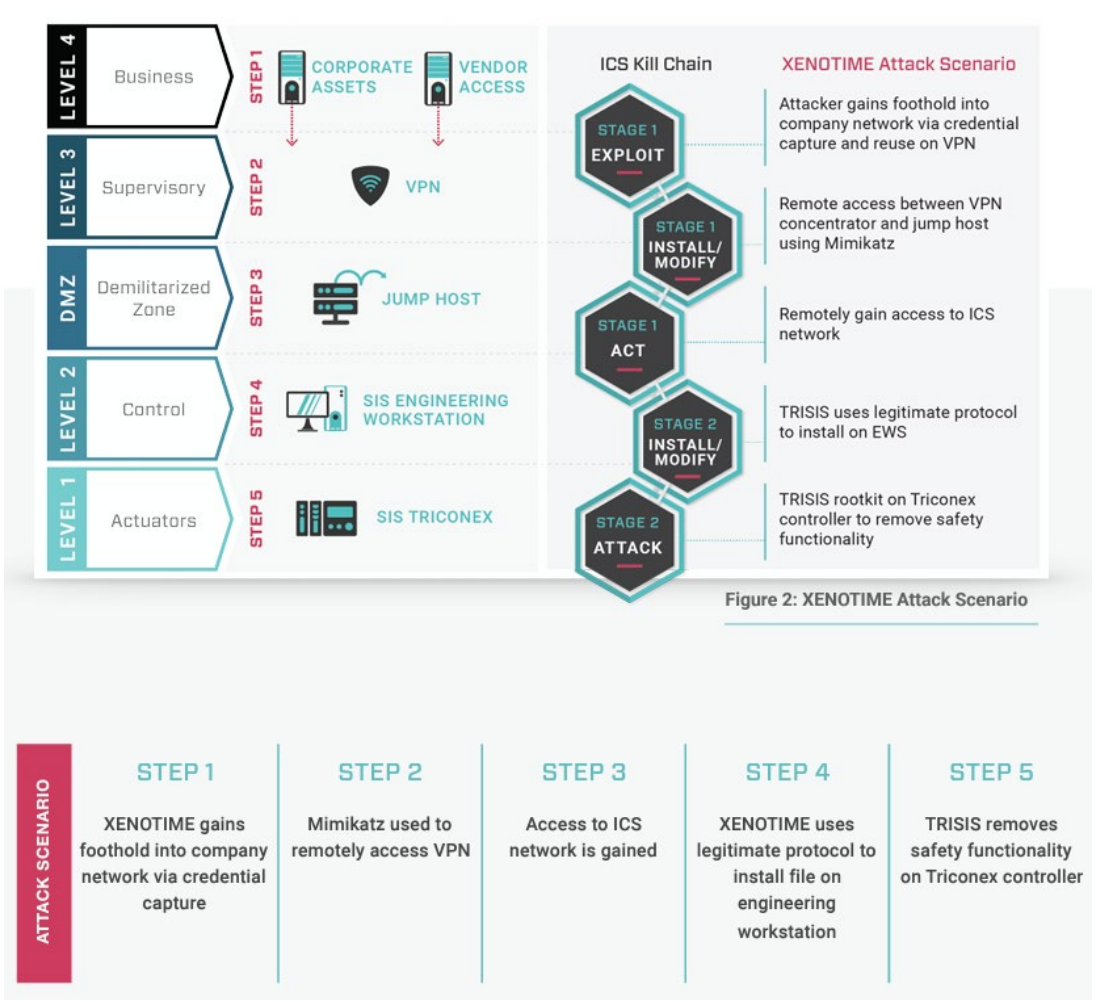


Figure 2: XENOTIME Attack Scenario


DRAGOS

DRAGOS CASE STUDY

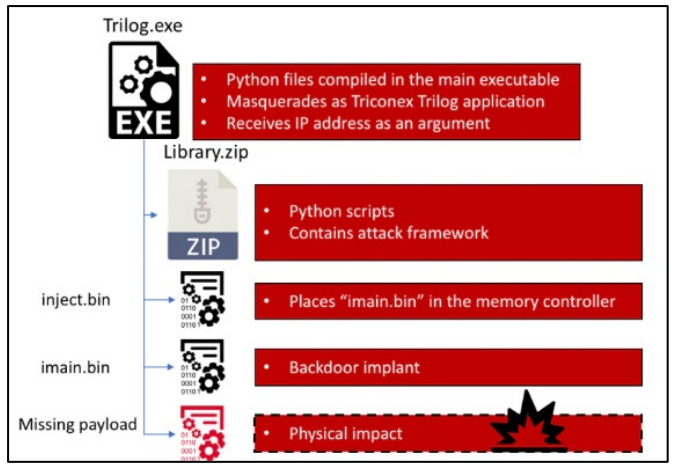
COMBATING THREATS IN OIL AND GAS ENVIRONMENTS WITH THE DRAGOS PLATFORM

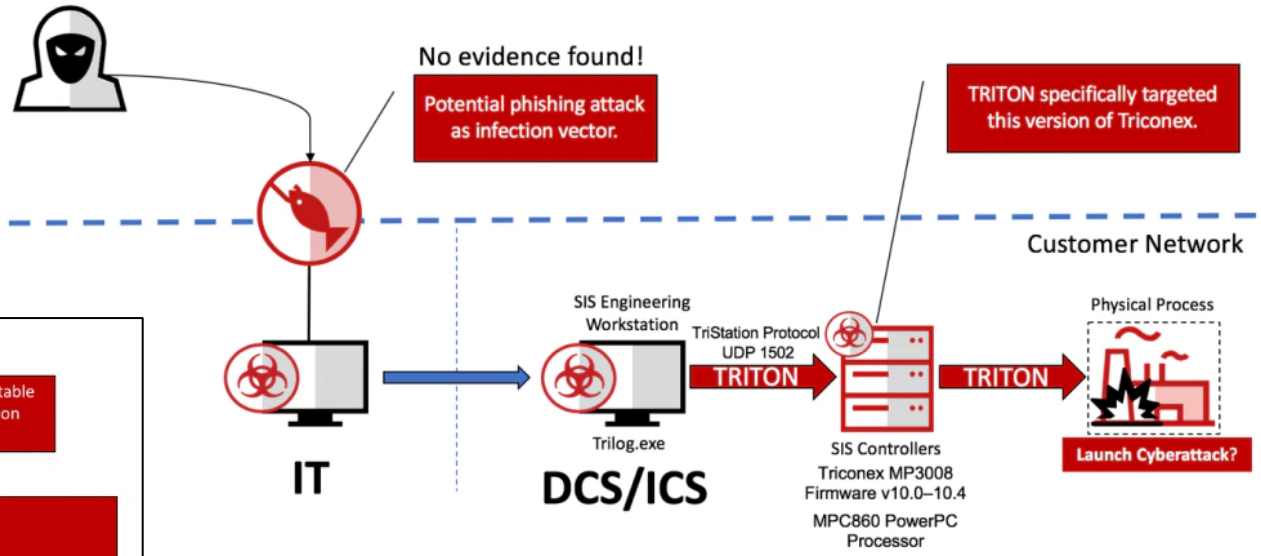
ABSTRACT

In 2018, a large North American oil refinery[1] suspected that its industrial control systems (ICS) environment had XENOTIME-related activity (the threat activity group behind the 2017 TRISIS attack on a Middle Eastern oil and gas facility) and engaged Dragos to investigate. This case study will examine the organization's challenges in securing its ICS environment prior to engaging Dragos, reveal the vulnerabilities facing this organization through a TRISIS threat scenario, and demonstrate how the Dragos Platform can help oil and gas organizations rapidly identify malicious behavior on their networks and respond before a significant compromise.

Kilde: https://www.dragos.com/resource/combating-threats-in-oil-and-gas-environments-with-the-dragos-platform/

Teknikker brukt ifbm Trisis/Triton





https://www.trellix.com/pt-br/about/newsroom/stories/research/triton-malware-spearheads-latest-generation-of-attacks-on-industrial-systems1.html

Det nyeste og mest avanserte virus for OT: PIPEDREAM

Events – en kjent konferanse innenfor ICS cybersikkerhet

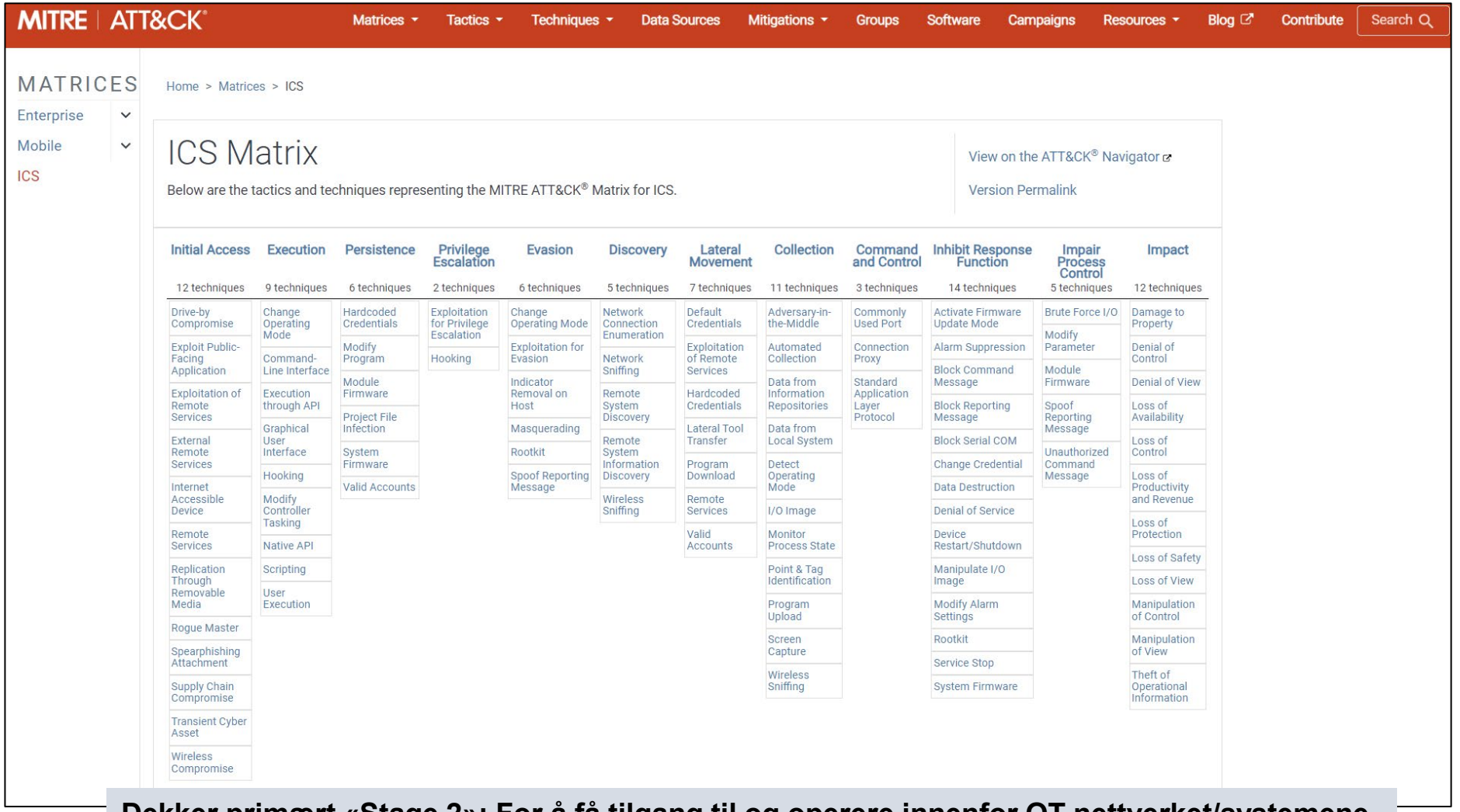
Se presentasjonen av Pipedream på https://www.youtube.com/watch?v=H82sbIwFxt4

I presentasjonen omtales:

- Hackergrupper som retter seg mot ICS
- ICS kill chain for ICS
- Purdue referansearkitektur
- Pipedream virus og funksjonalitet i denne
- Den litt latterlige skjorta som hentyder på hva Rob synes om de som driver med hacking

ICS: Industrial control systems

MITRE Att@ck matrix for ICS: Kilde til kunnskap om angrep



Dekker primært «Stage 2»: For å få tilgang til og operere innenfor OT nettverket/systemene

Kilde: https://attack.mitre.org/matrices/ics/

Internet accessible device

MITRE | ATT&CK

Matrices Tactics Techniques Data Sources Mitigations Groups Software Campaigns Resources Blog

ATT&CKcon 4.0 will be held on Oct 24-25 in McLean, VA. Click here for more details and to register.

TECHNIQUES

- Enterprise
- Mobile
- ICS
  - Initial Access
    - Drive-by Compromise
    - Exploit Public-Facing Application
    - Exploitation of Remote Services
    - External Remote Services
    - Internet Accessible Device
    - Remote Services
    - Replication Through Removable Media
    - Rogue Master
    - Spearphishing Attachment
    - Supply Chain Compromise
    - Transient Cyber Asset
    - Wireless Compromise
  - Execution
  - Persistence
  - Privilege Escalation
  - Evasion
  - Discovery
  - Lateral Movement
  - Collection
  - Command and Control
  - Inhibit Response Function
  - Impair Process Control
  - Impact

Home > Techniques > ICS > Internet Accessible Device

Internet Accessible Device

Adversaries may gain access into industrial environments through systems exposed directly to the internet for remote access rather than through External Remote Services. Internet Accessible Devices are exposed to the internet unintentionally or intentionally without adequate protections. This may allow for adversaries to move directly into the control system network. Access onto these devices is accomplished without the use of exploits, these would be represented within the Exploit Public-Facing Application technique.

Adversaries may leverage built in functions for remote access which may not be protected or utilize minimal legacy protections that may be targeted. [1] These services may be discoverable through the use of online scanning tools.

In the case of the Bowman dam incident, adversaries leveraged access to the dam control network through a cellular modem. Access to the device was protected by password authentication, although the application was vulnerable to brute forcing. [1] [2] [3]

In Trend Micros manufacturing deception operations adversaries were detected leveraging direct internet access to an ICS environment through the exposure of operational protocols such as Siemens S7, Omron FINS, and EtherNet/IP, in addition to misconfigured VNC access. [4]

ID: T0883
Sub-techniques: No sub-techniques
Tactic: Initial Access
Platforms: Control Server, Data Historian, Field Controller/RTU/PLC/IED, Human-Machine Interface, Input/Output Server, Safety Instrumented System/Protection Relay
Version: 1.0
Created: 21 May 2020
Last Modified: 09 March 2023

Version Permalink

Mitigations

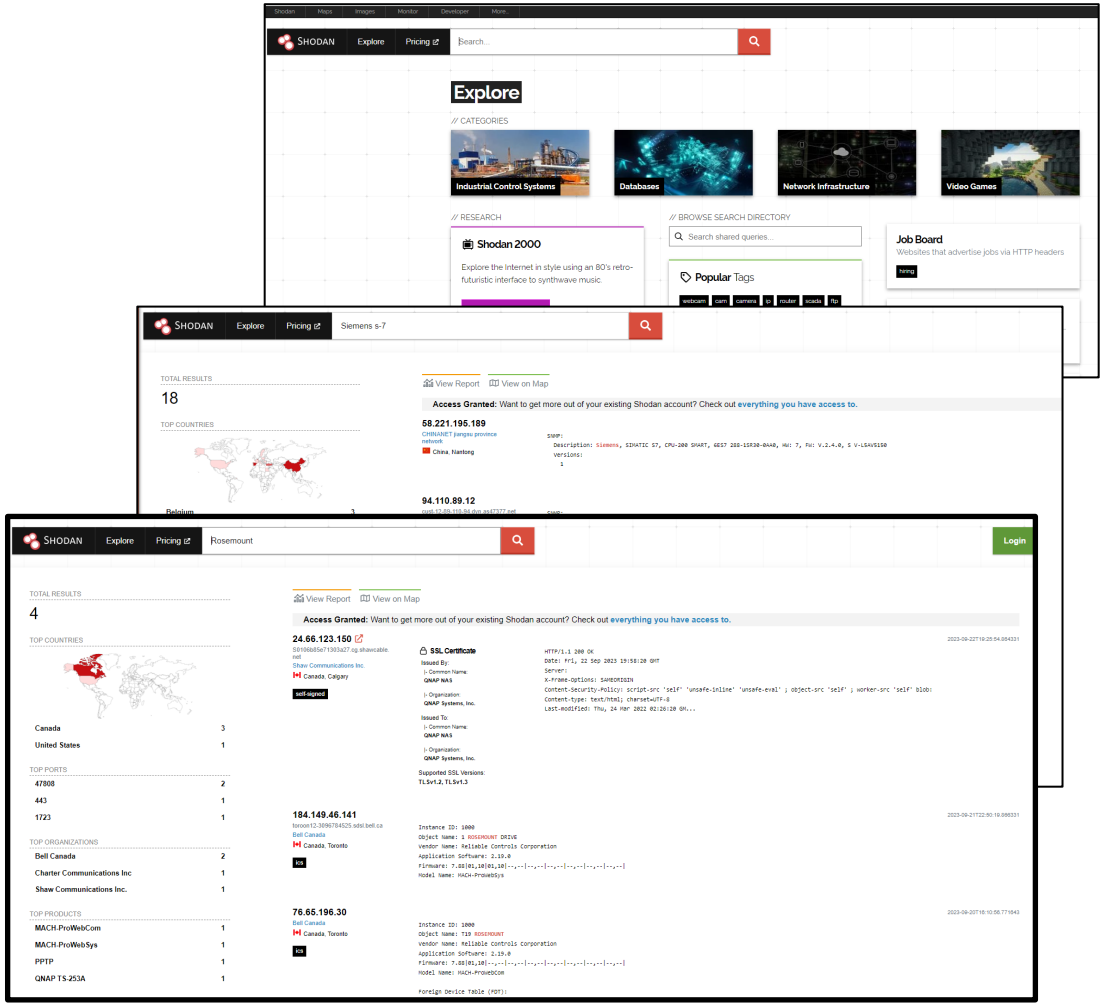
ID	Mitigation	Description
M0930	Network Segmentation	Deny direct remote access to internal systems through the use of network proxies, gateways, and firewalls. Steps should be taken to periodically inventory internet accessible devices to determine if it differs from the expected.

Detection

ID	Data Source	Data Component	Detects
DS0028	Logon Session	Logon Session Metadata	Monitor logon activity for unexpected or unusual access to devices from the Internet.
DS0029	Network Traffic	Network Traffic Content	Monitor for unusual logins to Internet connected devices or unexpected protocols to/from the Internet. Network traffic content will provide valuable context and details about the content of network flows.
		Network Traffic Flow	Monitor for unexpected protocols to/from the Internet. While network traffic content and logon session metadata may directly identify a login event, new Internet-based network flows may also be a reliable indicator of this technique.

References

1. NCCIC 2014, January 1 Internet Accessible Control Systems At Risk Retrieved. 2019/11/07
2. Danny Yadron 2015, December 20 Iranian Hackers Infiltrated New York Dam in 2013 Retrieved. 2019/11/07
3. Mark Thompson 2016, March 24 Iranian Cyber Attack on New York Dam Shows Future of War Retrieved. 2019/11/07
4. Stephen Hilt, Federico Maggi, Charles Perine, Lord Remorin, Martin Rsler, and Rainer Vosseler Mark Thompson 2016, March 24 Iranian Cyber Attack on New York Dam Shows Future of War Retrieved. 2019/11/07 Caught in the Act: Running a Realistic Factory Honeypot to Capture Real Threats Retrieved. 2021/04/12



Shodan er en nettside der en kan finne utstyr direkte eksponert på nett

Supply chain compromise

MITRE | ATT&CK®

Matrices | Tactics | Techniques | Data Sources | Mitigations | Groups | Software | Campaigns | Resources | Blog | Co

ATT&CKcon 4.0 will be held on Oct 24-25 in McLean, VA. Click here for more details and to register.

TECHNIQUES

- Enterprise
- Mobile
- ICS
  - Initial Access
    - Drive-by Compromise
    - Exploit Public-Facing Application
    - Exploitation of Remote Services
    - External Remote Services
    - Internet Accessible Device
    - Remote Services
    - Replication Through Removable Media
    - Rogue Master
    - Spearphishing Attachment
    - Supply Chain Compromise
    - Transient Cyber Asset
    - Wireless Compromise
  - Execution
  - Persistence
  - Privilege Escalation
  - Evasion
  - Discovery
  - Lateral Movement
  - Collection
  - Command and Control
  - Inhibit Response Function
  - Impair Process Control
  - Impact

Home > Techniques > ICS > Supply Chain Compromise

Supply Chain Compromise

Adversaries may perform supply chain compromise to gain control systems environment access by means of infected products, software, and workflows. Supply chain compromise is the manipulation of products, such as devices or software, or their delivery mechanisms before receipt by the end consumer. Adversary compromise of these products and mechanisms is done for the goal of data or system compromise, once infected products are introduced to the target environment.

Supply chain compromise can occur at all stages of the supply chain, from manipulation of development tools and environments to manipulation of developed products and tools distribution mechanisms. This may involve the compromise and replacement of legitimate software and patches, such as on third party or vendor websites. Targeting of supply chain compromise can be done in attempts to infiltrate the environments of a specific audience. In control systems environments with assets in both the IT and OT networks, it is possible a supply chain compromise affecting the IT environment could enable further access to the OT environment.

Counterfeit devices may be introduced to the global supply chain posing safety and cyber risks to asset owners and operators. These devices may not meet the safety, engineering and manufacturing requirements of regulatory bodies but may feature tagging indicating conformance with industry standards. Due to the lack of adherence to standards and overall lesser quality, the counterfeit products may pose a serious safety and operational risk. [1]

Yokogawa identified instances in which their customers received counterfeit differential pressure transmitters using the Yokogawa logo. The counterfeit transmitters were nearly indistinguishable with a semblance of functionality and interface that mimics the genuine product. [1]

F-Secure Labs analyzed the approach the adversary used to compromise victim systems with Havex. [2] The adversary planted trojanized software installers available on legitimate ICS/SCADA vendor websites. After being downloaded, this software infected the host computer with a Remote Access Trojan (RAT).

ID: T0862

Sub-techniques: No sub-techniques

Tactic: Initial Access

Platforms: Control Server, Data Historian, Field Controller/RTU/PLC/IED, Human-Machine Interface, Input/Output Server, Safety Instrumented System/Protection Relay

Version: 1.1

Created: 21 May 2020

Last Modified: 09 March 2023

Version Permalink

Procedure Examples

ID	Name	Description
S0093	Backdoor.Oldrea	The Backdoor.Oldrea RAT is distributed through trojanized installers planted on compromised vendor sites. [2]
G0035	Dragonfly	Dragonfly trojanized legitimate ICS equipment providers software packages available for download on their websites.[3]
G0088	TEMP.Veles	TEMP.Veles targeted several ICS vendors and manufacturers. [4]

Mitigations

ID	Mitigation	Description
M0947	Audit	Perform audits or scans of systems, permissions, insecure software, insecure configurations, etc. to identify potential weaknesses. Perform periodic integrity checks of the device

Endpoint Protection

View Only

Community Home | Threads | Library | Events | Members

BACK TO LIBRARY

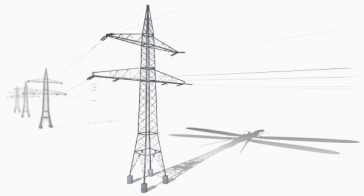
Dragonfly: Western Energy Companies Under Sabotage Threat

2 Recommend

Jun 30, 2014 08:58 AM

A L Johnson

Statistics
0 Favorited
9 Views
0 Files
0 Shares
0 Downloads



An ongoing cyberespionage campaign against a range of targets, mainly in the energy sector, gave attackers the ability to mount sabotage operations against their victims. The attackers, known to Symantec as Dragonfly, managed to compromise a number of strategically important organizations for

Tools employed

Dragonfly uses two main pieces of malware in its attacks. Both are remote access tool (RAT) type malware which provide the attackers with access and control of compromised computers. Dragonfly's favored malware tool is Backdoor.Oldrea, which is also known as Havex or the Energetic Bear RAT. Oldrea acts as a back door for the attackers on to the victim's computer, allowing them to extract data and install further malware.

Oldrea appears to be custom malware, either written by the group itself or created for it. This provides some indication of the capabilities and resources behind the Dragonfly group.

Once installed on a victim's computer, Oldrea gathers system information, along with lists of files, programs installed, and root of available drives. It will also extract data from the computer's Outlook address book and VPN configuration files. This data is then written to a temporary file in an encrypted format before being sent to a remote command-and-control (C&C) server controlled by the attackers.

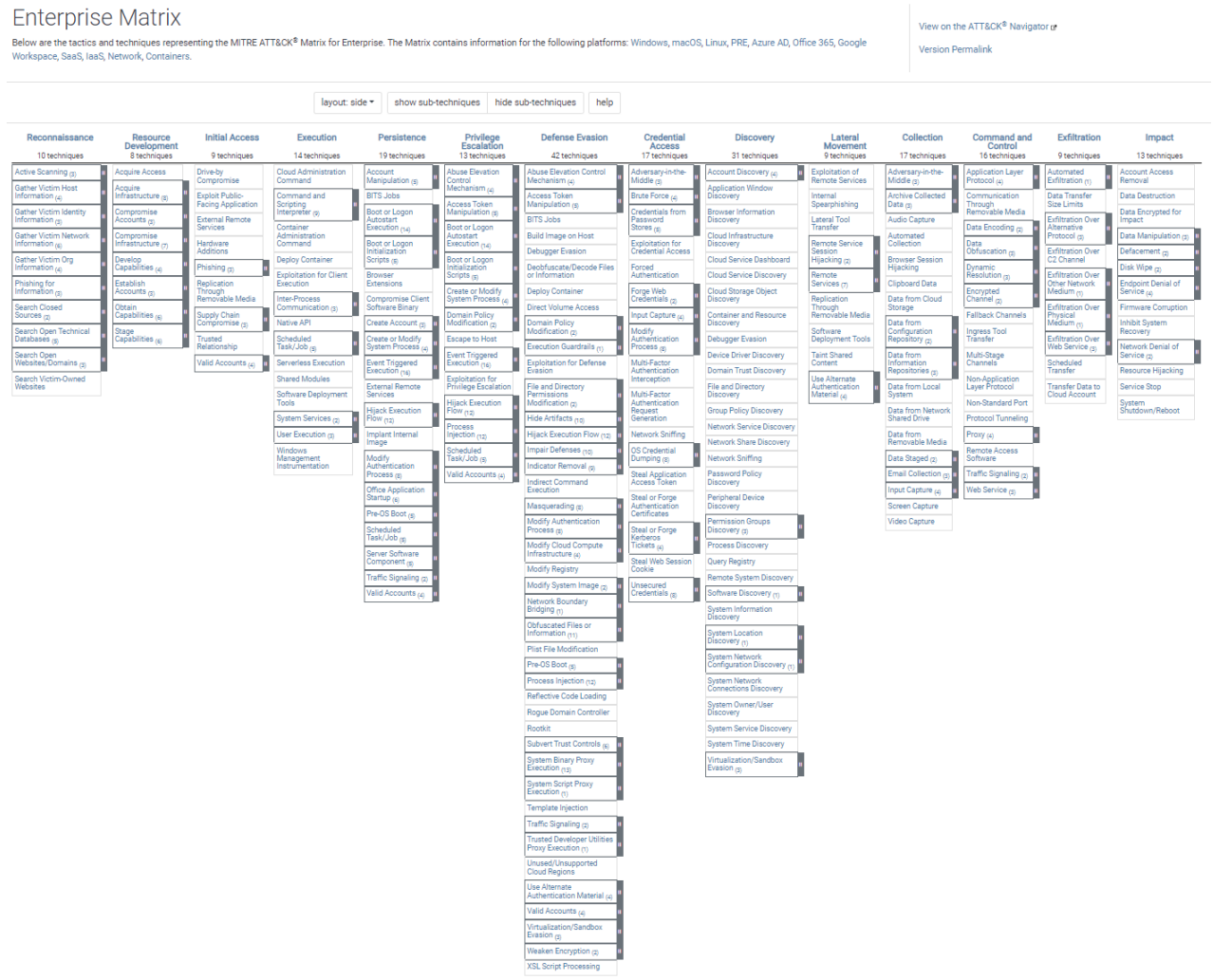
The majority of C&C servers appear to be hosted on compromised servers running content management systems, indicating that the attackers may have used the same exploit to gain control of each server. Oldrea has a basic control panel which allows an authenticated user to download a compressed version of the stolen data for each particular victim.

The second main tool used by Dragonfly is Trojan.Karagany. Unlike Oldrea, Karagany was available on the underground market. The source code for version 1 of Karagany was leaked in 2010. Symantec believes that Dragonfly may have taken this source code and modified it for its own use. This version is detected by Symantec as Trojan.Karagany!gen1.

Karagany is capable of uploading stolen data, downloading new files, and running executable files on an infected computer. It is also capable of running additional plugins, such as tools for collecting passwords, taking screenshots, and cataloging documents on infected computers.

Symantec found that the majority of computers compromised by the attackers were infected with Oldrea. Karagany was only used in around 5 percent of infections. The two pieces of malware are similar in functionality and what prompts the attackers to choose one tool over another remains unknown.

MITRE Att@ck matrix for enterprise: Stage 1



Kilde: https://attack.mitre.org/matrices/ics/

Generelt og aktuelle strategier for Stage 1

Standarder bruk i industrien

Kjente standarder brukt i industrien

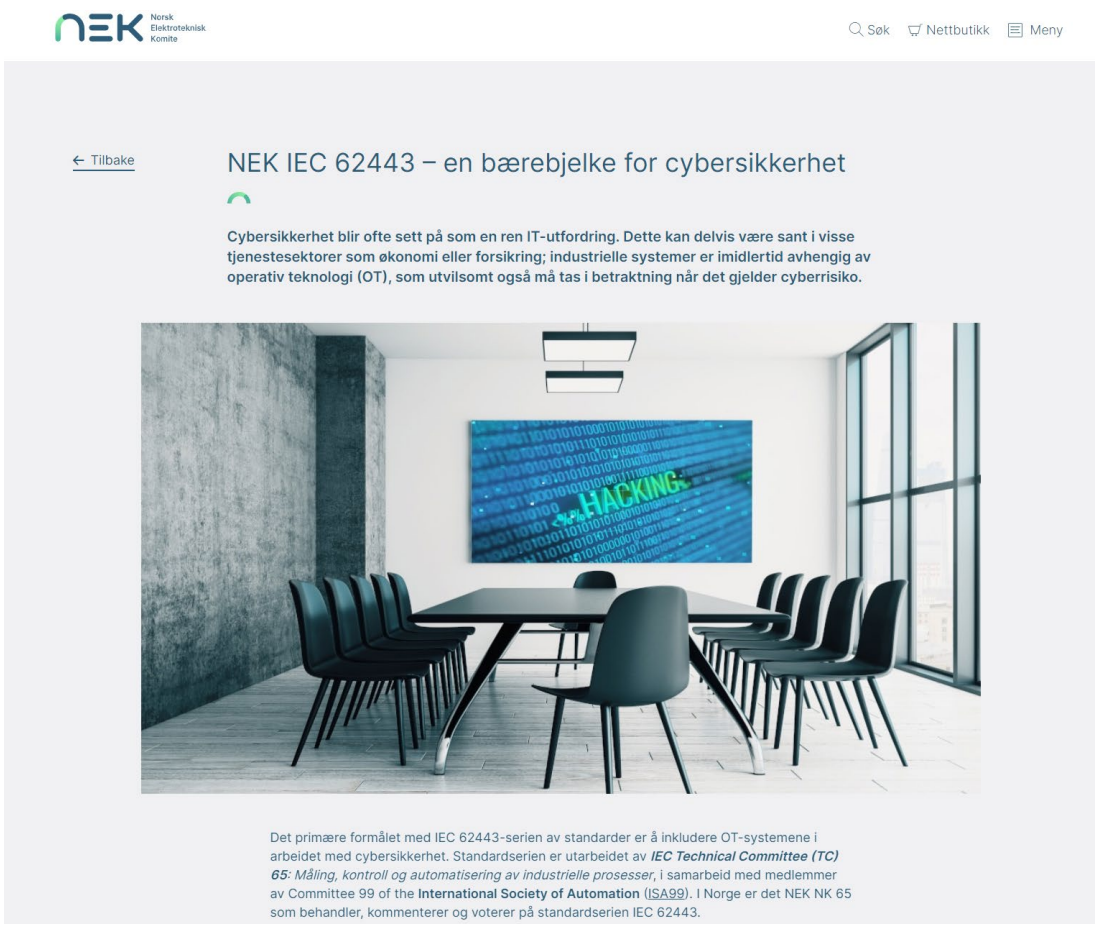
Standarder mest brukt

- **IEC 62443**
  (tilgjengelig via https://i.ntnu.no/wiki/-/wiki/Norsk/Standarder)
- **NIST cybersecurity framework**
  https://www.nist.gov/cyberframework

Andre standarder

- NIST guide to Industrial Control Systems (ICS) Security (https://csrc.nist.gov/pubs/sp/800/82/r2/final)
- ISA TR 84.00.09 Cybersecurity for SIS: https://www.isa.org/products/isa-tr84-00-09-2017-cybersecurity-related-to-the-f
- DNV GL RP G108 – Guideline on the application of IEC 62443 https://www.dnv.com/cybersecurity/recommended-practices/dnv-rp-g108-cyber-security-in-the-oil-and-gas-industry-based-on-IEC-62443.html
- Other guidelines from DNV
- Offshore Norway retningslinje 104: https://offshorenorge.no/retningslinjer/arkiv/helse-arbeidsmiljo-og-sikkerhet/104-anbefalte-retningslinjer-krav-til-informasjonssikkerhetsniva-i-ikt-baserte-prosesskontroll--sikkerhets--og-stottesystemer-ny-revisjon-pr-05.12.2016/
- Flere standarder og retningslinjer enten publisert eller under utvikling av IEC for å dekke ulike bransjer:
  - IEC TS 62351 – Security aspects for power systems
  - IEC TR 63074 – Security aspects of machinery control systems
  - IEC TR 63069 – Framework for functional safety and security
  - ISO/IEC 27036

IEC 62443



https://www.nek.no/2020/09/28/nek-iec-62443-en-baerebjelke-for-cybersikkerhet/

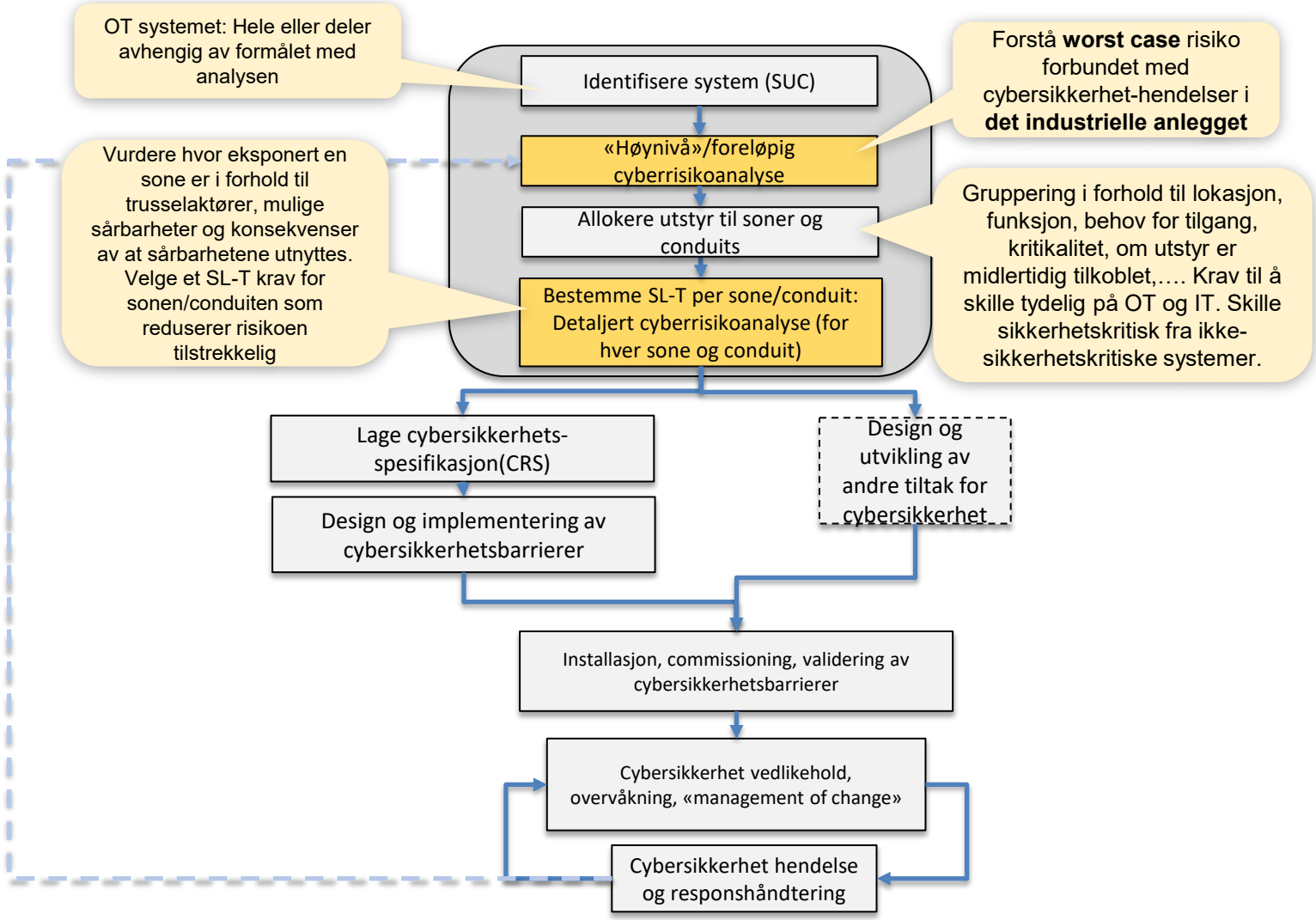
IEC 62443 er en standard som består av flere deler (standarder):

- Generelle krav (NEK IEC 62443-1. * – en del av fire publisert)
- Policy og prosedyrer (NEK IEC 62443-2. * – tre deler av fire er publisert)
- Systemkrav (NEK IEC 62443-3. * – alle tre delene publisert)
- Komponentkrav (NEK IEC 62443-4. * – begge deler er publisert)

IEC 62443 – cybersikkerhet livssyklus

- Krav til å gjennomføre cyberrisikoanalyser
- Risikoanalyser basert på etablerte prinsipper i ISO 27005, den generelle standarden for IT security risikoanalyser
- Denne resulterer i:
  - Soneinndeling og conduits (Forbindelser mellom soner)
  - Tilhørende Security level (SL) krav (1-4)

Kilde med flere detaljer: IEC 62443-3-2



Cyber risiko

Risiko (generelt) forbundet med en bestemt farlig hendelse (HE - Hazardous event) uttrykkes ofte som:

Risk = P x C

P: Probability/likelihood/frequency of HE
C: Consequence, often worst case, if HE not handled

Ideen bak Consequence-driven Cyber-Informed Engineering (CCE)

Kan delvis påvirkes ved å re-designe anlegget

Hvilke konsekvenser er det for mennesker, miljø og andre kritiske verdier

Likelihood / sannsynlighet

Cyber risk = Trussel x Sårbarhet x Konsekvens

Hvor eksponert er man?

Hvilke sårbarheter har man?

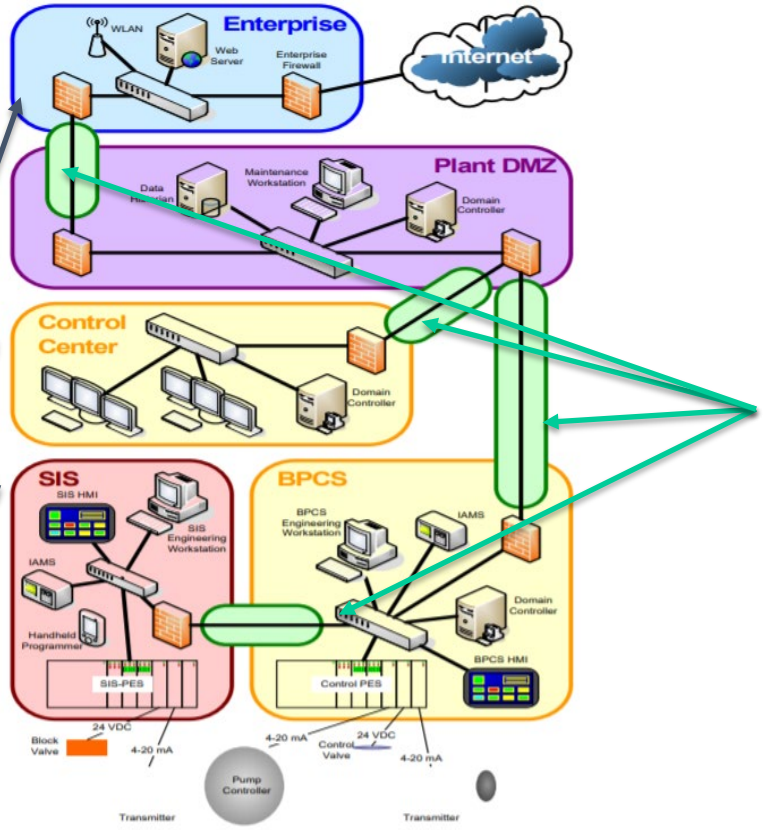
Ikke så enkelt å påvirke. Delvis observerbart

Kan påvirkes (kontrollerbart og observerbart)

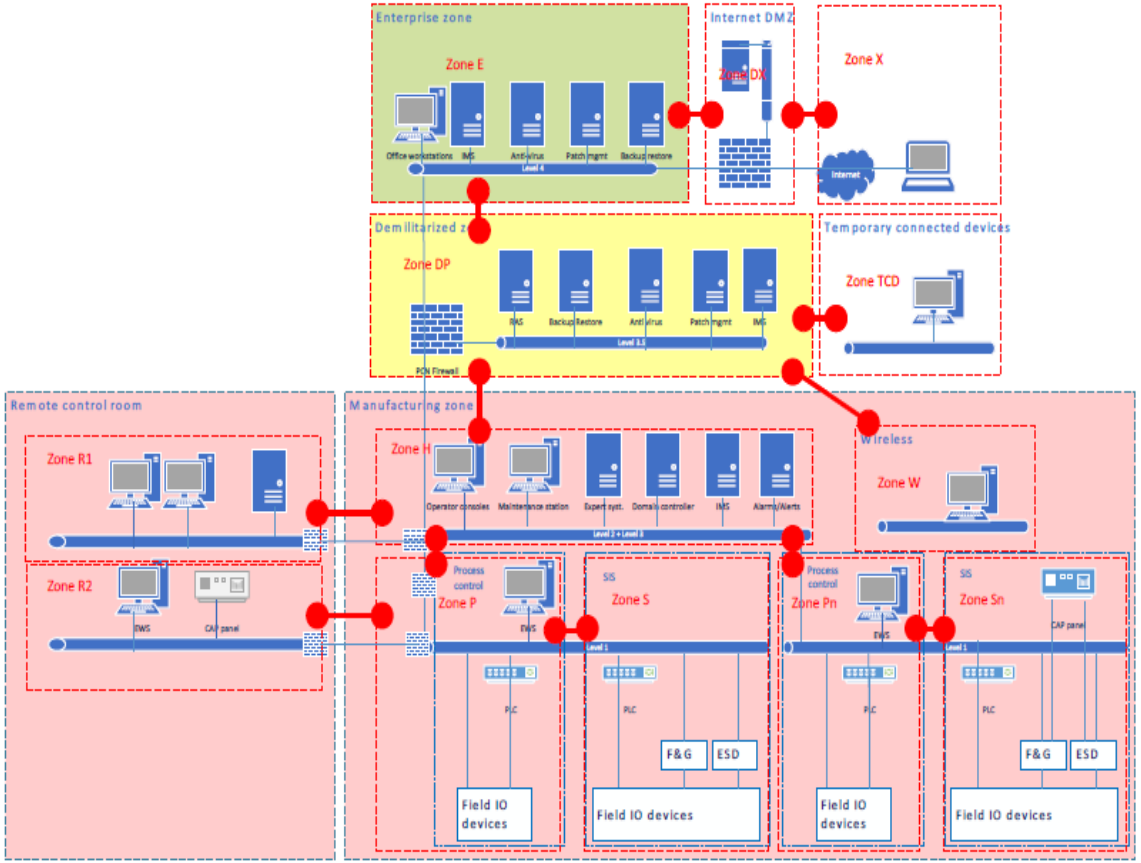
Cyber risk: Threat x vulernability x conseqeunce (Kilde: CCE book https://www.amazon.com/Countering-Cyber-Sabotage-Consequence-Driven-Cyber-Informed/dp/036749115X)

IEC 62443 – soner og conduits

Soner



Conduit



Eksempel fra DNV RP G108

Security level (SL)

- Security level:
  - Deles inn i fire nivå – SL 1 til SL 4

  Kan tolkes som:
  - Systemnivå: Uttrykk for hvor **effektivt/pålitelig** cybersikkerhetstiltak (security level measure/ countermeasure) – hver for seg eller samlet for en sone/conduit
  - Utstyrsnivå: Uttrykk for beskyttelsen som gis for **implementerte egenskaper for et utstyr plassert i en sone/conduit**.

- Selv ved en avansert trusselaktør vil ikke alle soner få krav om SL-4. Man må se på hvordan sonen er beskyttet av tiltak i andre soner.

- Det skilles mellom tre typer SL, der av SL-T som bestemmes i cyberrisikoanalysen.

SL-T	Description
1	Capability of the security level measure (SLM) to protect against causal or coincidental violation
2	Capability of the security level measure (SLM) to protect against intentional violations using simple means of low resources, generic skills and low motivation
3	Capability of the security level measure (SLM) to protect against intentional violations using sophisticated measures with moderate resources, IACS (OT) specific skills and moderate motivations
4	Capability of the security level measure (SLM) to protect against intentional violations using sophisticated measures with extended resources, IACS (OT) specific skills and moderate motivations

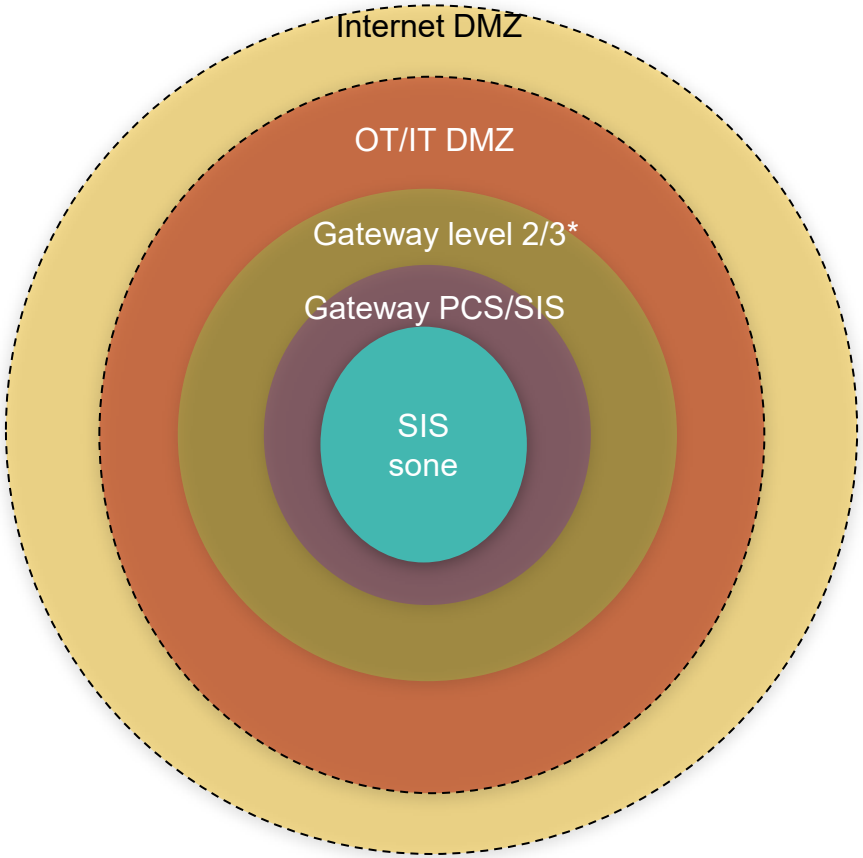
SL-T: Target for a zone or conduit

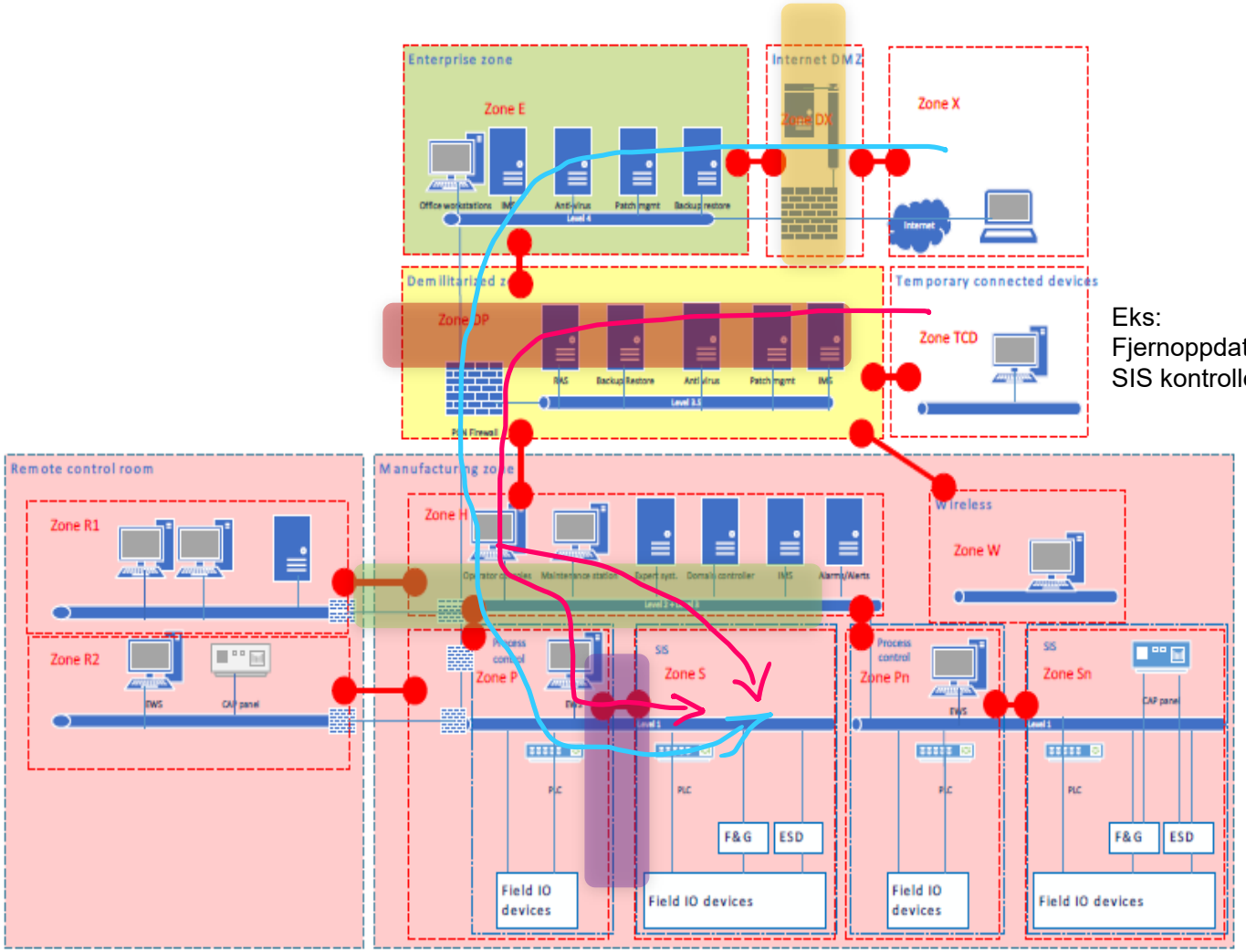
SL-A: SL level *achieved* for the zone or conduit

SL-C: The highest SL *capability* of individual devices (i.e, configurable)

IEC 62443-3-2 (annex A)

SL-T krav til soner – lagvis beskyttelse





Eks:
Fjernoppdatering
SIS kontroller

*Referer til Purdue referansearkitektur

IEC 62443 – eksempler på vurdering av cyberrisiko

Table B.1 – Example of a 3 x 5 risk matrix

		Severity		
		A	B	C
Likelihood	5	High	High	Med-high
	4	High	Med-high	Medium
	3	Med-high	Medium	Med-low
	2	Medium	Med-low	Low
	1	Med-low	Low	Low

Table B.2 – Example of likelihood scale

Likelihood scale	Guideword	Likelihood description	Frequency-based guidance
1	Certain	Almost certain	$>10^{-1}$ per year (High demand)
2	Likely	Likely to occur	10^{-1} to 10^{-3} per year (Low demand)
3	Possible	Quite possible or not unusual to occur	10^{-3} to 10^{-4} per year
4	Unlikely	Conceivably possible, but very unlikely to occur	10^{-4} to 10^{-5} per year
5	Remote	So unlikely that it can be assumed it will not occur	$<10^{-5}$ per year

Table B.3 – Example of consequence or severity scale

	Operational			Financial			HSE		
Category	Outage at one site	Outage at multiple sites	National infrastructure and services	Cost (Million USD)	Legal	Public confidence	People onsite	People offsite	Environment
A (High)	>7 days	>1 day	Impacts multiple sectors or disrupts community services in a major way	>500	Felony criminal offense	Loss of brand image	Fatality	Fatality or major community incident	Citation by regional agency or long-term significant damage over large area
B (Medium)	<2 days	>1 hour	Potential to impact sector at a level beyond the company	>5	Misdemeanor criminal offense	Loss of customer confidence	Loss of work day or major injury	Complaints or local community impact	Citation by local agency
C (Low)	<1 day	<1 hour	Little to no impact to sectors beyond the individual company. Little to no impact on community.	<5	None	None	First aid or recorda-ble injury	No complaints	Small, contained release below reportable limits

IEC 62443 – Å komme fra risikomatrisen til et SL-T krav

- Ofte deler ikke selskaper sine detaljerte risikomatriser
- Få eksempler på matriser der SL-T krav er gitt
- Som et eksempel kan vi anta at utstyr i sonen/conduit får:
  - High: SL-T 4
  - Med-high: SL-T 3
  - Medium: SL-T2
  - Med-low: SL T1
  - Low: Ikke krav til SL nivå. Risikoen er tilstrekkelig lav i utgangspunktet

Table B.1 – Example of a 3 x 5 risk matrix

		Severity		
		A	B	C
Likelihood	5	High	High	Med-high
	4	High	Med-high	Medium
	3	Med-high	Medium	Med-low
	2	Medium	Med-low	Low
	1	Med-low	Low	Low

Eksempel på SL-T krav

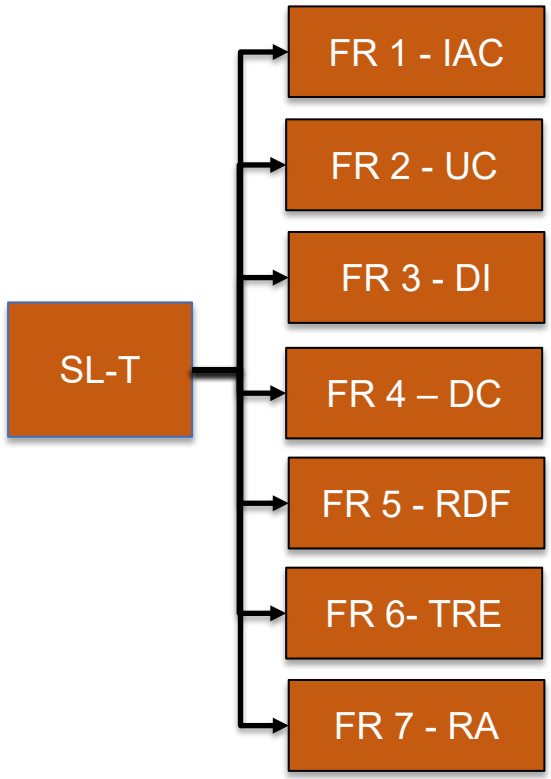
Ikke en ferdig etablert praksis i industrien, men her er noen eksempler:

- DMZ/Remote Access sone: SL-T 4
- Prosesskontroll- Remote Read-only HMI SL-T 3
- Prosesskontroll – EWS* SL-T 2 + disconnected / sterkere conduit
- Prosesskontroll - HMI SL-T 2
- Prosesskontroll - Logic solvers SL-T 1 + sterkere conduits
- SIS – EWS SL-T 3 + disconnected / sterkere conduits
- SIS – HMI SL-T 3 + disconnected / sterkere conduits
- SIS – Logic solvers SL-T 1 + sterkere conduits

Kilde: Kenneth Titlestad, Sopra Steria

Betydningen av et SL-T krav til sonen/conduit

- For utstyr i sonen og conduit må en vurdere implementering av krav knyttet til FR1- til FR-7
- Ikke alt utstyr vil implementere alle krav, men utstyr i sonen skal samlet sett oppnå kravene



Identifisering og autentisering: Forhindre uautorisert tilgang mennesker, software, utstyr når de forespør å koble seg til. Kan gis som individ, rolle, eller annet.

Iverksette og overvåke de rettigheter en bruker har fått: Forhindre uautorisert adgang til å utføre aksjoner

Dataintegritet: Forhindre mulighet til å endre på data og kode/manipulering av data som deles mellom systemer og kode.

Datakonfidensialitet: Forhindre mulighet for å se/tappe/stjele innhold i data, knyttet spesielt til

Begrenset unødvendig dataflyt: Forhindre at data ikke flyter til autoriserte aktører, ved bruk av hensiktsmessig segregering.

Rask nok respons ved oppdagede hendelser/brudd security tiltak: Sikre at cybersikkerhetsbrudd varsles og tas aksjon på i rett tid.

Ressurstilgang: Sikre nettverksressurser mot denial of service (DoS) og sikre kontrollere og utstyr dersom hendelser inntreffer (recovery, automatisk reinstallering,…)

IEC 62443 – eksempler på SL krav per FR (sone/conduit)

SR 3.2:
The control system should use **protection mechanisms** to prevent, detect, mitigate and report instances of detected malicious code (for example, viruses, worms, Trojan horses and spyware) transported by electronic mail, electronic mail attachments, Internet access, removable media (for example, universal serial bus (USB) devices, diskettes or compact disks), PDF documents, web services, network connections and infected laptops or other common means.

Detection mechanisms should be able to detect integrity violations of application binaries and data files. Techniques may include, but are not limited to, binary integrity and attributes monitoring, hashing and signature techniques. Mitigation techniques may include, but are not limited to, file cleaning, quarantining, file deletion, host communication restriction and IPSs.

Prevention techniques may include, but are not limited to, application blacklisting and whitelisting techniques, removable media control, sandbox techniques and specific computing platforms mechanisms such as restricted firmware update capabilities, No Execute (NX) bit, data execution prevention (DEP), address space layout randomization (ASLR), stack corruption detection and mandatory access controls. See 10.4, SR 6.2 – Continuous monitoring for an associated requirement involving control system monitoring tools and techniques.

Table B.1 *(3 of 4)*

SRs and REs		SL 1	SL 2	SL 3	SL 4
FR 3 – System integrity (SI)					
SR 3.1 – Communication integrity	7.3	✓	✓	✓	✓
SR 3.1 RE 1 – Cryptographic integrity protection	7.3.3.1			✓	✓
SR 3.2 – Malicious code protection	7.4	✓	✓	✓	✓
SR 3.2 RE 1 – Malicious code protection on entry and exit points	7.4.3.1		✓	✓	✓
SR 3.2 RE 2 – Central management and reporting for malicious code protection	7.4.3.2			✓	✓
SR 3.3 – Security functionality verification	7.5	✓	✓	✓	✓
SR 3.3 RE 1 – Automated mechanisms for security functionality verification	7.5.3.1			✓	✓
SR 3.3 RE 2 – Security functionality verification during normal operation	7.5.3.2				✓
SR 3.4 – Software and information integrity	7.6		✓	✓	✓
SR 3.4 RE 1 – Automated notification about integrity violations	7.6.3.1			✓	✓
SR 3.5 – Input validation	7.7	✓	✓	✓	✓
SR 3.6 – Deterministic output	7.8	✓	✓	✓	✓
SR 3.7 – Error handling	7.9		✓	✓	✓
SR 3.8 – Session integrity	7.10		✓	✓	✓
SR 3.8 RE 1 – Invalidation of session IDs after session termination	7.10.3.1			✓	✓
SR 3.8 RE 2 – Unique session ID generation	7.10.3.2			✓	✓
SR 3.8 RE 3 – Randomness of session IDs	7.10.3.3				✓
SR 3.9 – Protection of audit information	7.11		✓	✓	✓
SR 3.9 RE 1 – Audit records on write-once media	7.11.3.1				✓
FR 4 – Data confidentiality (DC)					
SR 4.1 – Information confidentiality	8.3	✓	✓	✓	✓
SR 4.1 RE 1 – Protection of confidentiality at rest or in transit via untrusted networks	8.3.3.1		✓	✓	✓
SR 4.1 RE 2 – Protection of confidentiality across zone boundaries	8.3.3.2				✓
SR 4.2 – Information persistence	8.4		✓	✓	✓
SR 4.2 RE 1 – Purging of shared memory resources	8.4.3.1			✓	✓
SR 4.3 – Use of cryptography	8.5	✓	✓	✓	✓
FR 5 – Restricted data flow (RDF)					
SR 5.1 – Network segmentation	9.3	✓	✓	✓	✓
SR 5.1 RE 1 – Physical network segmentation	9.3.3.1		✓	✓	✓
SR 5.1 RE 2 – Independence from non-control system networks	9.3.3.2			✓	✓
SR 5.1 RE 3 – Logical and physical isolation of critical networks	9.3.3.3				✓

Kilde: IEC 62443-3-3

SR 3.2 – RE 1:
The control system shall provide the capability to employ malicious code protection mechanisms at **all entry and exit points**.

SR 3.2 – RE 2:
The control system shall provide the capability to **manage** malicious code protection mechanisms.
Note: Such mechanisms are commonly provided by endpoint infrastructure centralized management or **SIEM solutions**.

IBM forklarer SIEM

Security information and event management, or SIEM, is a security solution that helps organizations recognize and address potential security threats and vulnerabilities before they have a chance to disrupt business operations. SIEM systems help enterprise security teams detect user behavior anomalies and use artificial intelligence (AI) to automate many of the manual processes associated with threat detection and incident response.

The original SIEM platforms were log management tools, combining security information management (SIM) and security event management (SEM) to enable real-time monitoring and analysis of security-related events, as well as tracking and logging of security data for compliance or auditing purposes. (Gartner coined the term SIEM for the combination of SIM and SEM technologies in 2005.)

Over the years, SIEM software has evolved to incorporate user and entity behavior analytics (UEBA), as well as other advanced security analytics, AI and machine learning capabilities for identifying anomalous behaviors and indicators of advanced threats. Today SIEM has become a staple in modern-day security operation centers (SOCs) for security monitoring and compliance management use cases.

IEC 62443 – eksempler på SL krav per FR (komponent)

Fire typer komponenter:

- Software applikasjoner (SA)
- Embedded devices (ED)
- Host device (HD)
- Network device (ND)

Krav som gjelder de enkelte er angitt som:

- SAR
- EDR
- HDR
- NDR

R står for «Requirements»

SRs and REs	SL 1	SL 2	SL 3	SL 4
EDR 2.13 – Use of physical diagnostic and test interfaces		✓	✓	✓
RE (1) Active monitoring			✓	✓
HDR 2.13 – Use of physical diagnostic and test interfaces		✓	✓	✓
RE (1) Active monitoring			✓	✓
NDR 2.13 – Use of physical diagnostic and test interfaces		✓	✓	✓
RE (1) Active monitoring			✓	✓
FR 3 – System integrity (SI)				
CR 3.1 – Communication integrity	✓	✓	✓	✓
RE (1) Communication authentication		✓	✓	✓
SAR 3.2 – Protection from malicious code	✓	✓	✓	✓
EDR 3.2 – Protection from malicious code	✓	✓	✓	✓
HDR 3.2 – Protection from malicious code	✓	✓	✓	✓
RE (1) Report version of code protection		✓	✓	✓
NDR 3.2 – Protection from malicious code	✓	✓	✓	✓
CR 3.3 – Security functionality verification	✓	✓	✓	✓
RE (1) Security functionality verification during normal operation				✓
CR 3.4 – Software and information integrity	✓	✓	✓	✓
RE (1) Authenticity of software and information		✓	✓	✓

HDR 3.2:
Host devices need to support the use of malicious code protection (against, for example, viruses, worms, Trojan horses and spyware). The product supplier should **qualify and document the configuration of protection from malicious code mechanisms so that the primary mission of the control system is maintained**.

RE (1): The host device shall automatically report the software and file versions of protection from malicious code in use (as part of overall logging function).

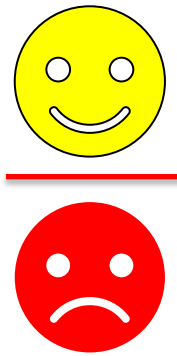
IEC 62443 – Handler ikke bare om tekniske egenskaper

Maturity level (modenhetsnivå):

- Gjelder for organisasjoner og prosesser
- Deles inn i fire nivå ML 1- ML 4
- Sammenstilt med SL – A så vil man få et uttrykk for samlet beskyttelsesnivå (security program rating – SPR)

Som selskap ønsker du ***ikke*** være på ML1 eller ML 2

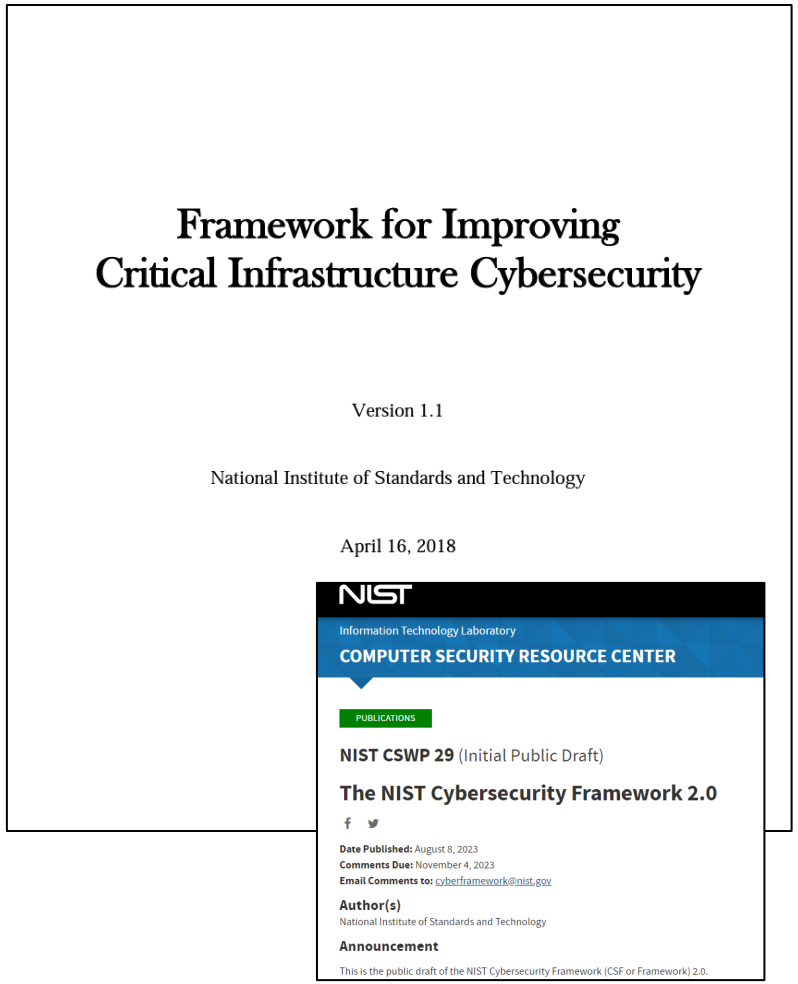
ML	Description
1	Organizational security measures (OSMs) are practiced in an ad-hoc manner and often undocumented (or not fully documented) manner.
2	Documentation exists that describes the OSMs and how to manage the delivery and performance of the practice. There may be a significant delay between the definition and practice of the OSM.
3	OSMs are repeatably practiced over time according to written documentation
4	Using suitable process key performance indicators, the effectiveness/and or performance improvements of the practice of the OSMs can be demonstrated



ML/SL	1	2	3	4
4	SPR1	SPR2	SPR3	SPR4
2	SPR1	SPR2	SPR3	SPR4
2	SPR1	SPR1	SPR2	SPR3
1	SPR0	SPR0	SPR1	SPR2

NIST cybersecurity framework

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO



Framework for Improving Critical Infrastructure Cybersecurity

Version 1.1

National Institute of Standards and Technology

April 16, 2018

NIST

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

PUBLICATIONS

NIST CSWP 29 (Initial Public Draft)

The NIST Cybersecurity Framework 2.0

Date Published: August 8, 2023
Comments Due: November 4, 2023
Email Comments to: cyberframework@nist.gov

Author(s)
National Institute of Standards and Technology

Announcement
This is the public draft of the NIST Cybersecurity Framework (CSF or Framework) 2.0.

https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework

Seminar 4 - gruppeoppgaver

Anta at PSD systemet er implementert i en egen SIS sone på nivå 0/1 i Purdue referansearkitekturen.

1. Forklar hvilke faktorer som inngår i cyberrisikobegrepet og hvilke av disse cybersikkerhetstiltak og krav i IEC 62443 generelt retter seg mot.
2. Forklar forskjellen mellom SL-T, SL-A og SL-C og eksemplifisert forskjellen ifbm PSD logikksystemet (PLCen). Se IEC 62443-3-2, annex A.
3. Anta SL-T 3 krav til engineering work station (EWS) som brukes for å oppdatere programvaren som kjører på PSD-systemet
   a) Forklar kort *ett* krav per FR-kategori, gjerne med eksempler på teknikker om dette er gitt (IEC 62443-3-3, for mer utdypning av tematikken kravene tar opp, så kan man søke i MITRE attack matrisen, NIST clossary, eller generell googling))
   b) Gi et eksempel på hvordan brudd/ikke implementert krav kan bidra til tap eller endret funksjonsevne til PSD SIF
   c) Velg ut 2-3 av kravene du har dekket og pek på hvilke teknikker de beskytter mot i MITRE attack-matrisens oversikt over angrepsteknikker
4. Forsøk å matche kravene fra forrige oppgave med angrepsteknikker de skal beskytte mot i MITRE attack matrisen.

Uavhengig av PSD SIFen:

5. Reflekter over egen rolle som ingeniør for å ivareta cybersikkerhet i en fremtidig jobbsituasjon (selvvalgt)