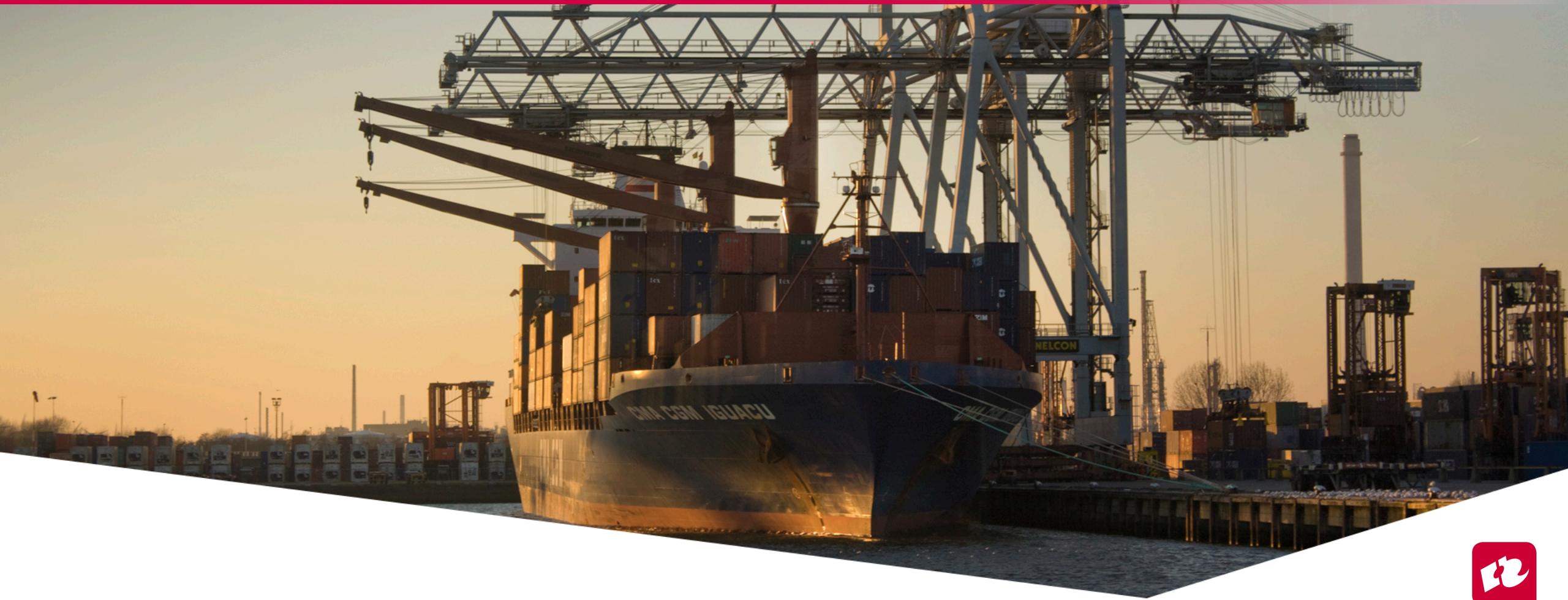


ICS Security

TINLAB 19-20



Security bij TINLAB

- Bredere blik op cybersecurity in wat meer obscure gebieden die vaak over het hoofd gezien worden...
- ...en waar we niet een heel vak aan kunnen wijden in het TI-curriculum
- Nu: Introductie in cybersecurity in kritieke infrastructuur
- Week 7: Vragenuurtje en evt. aangevraagde gerelateerde onderwerpen



Wat je gaat doen

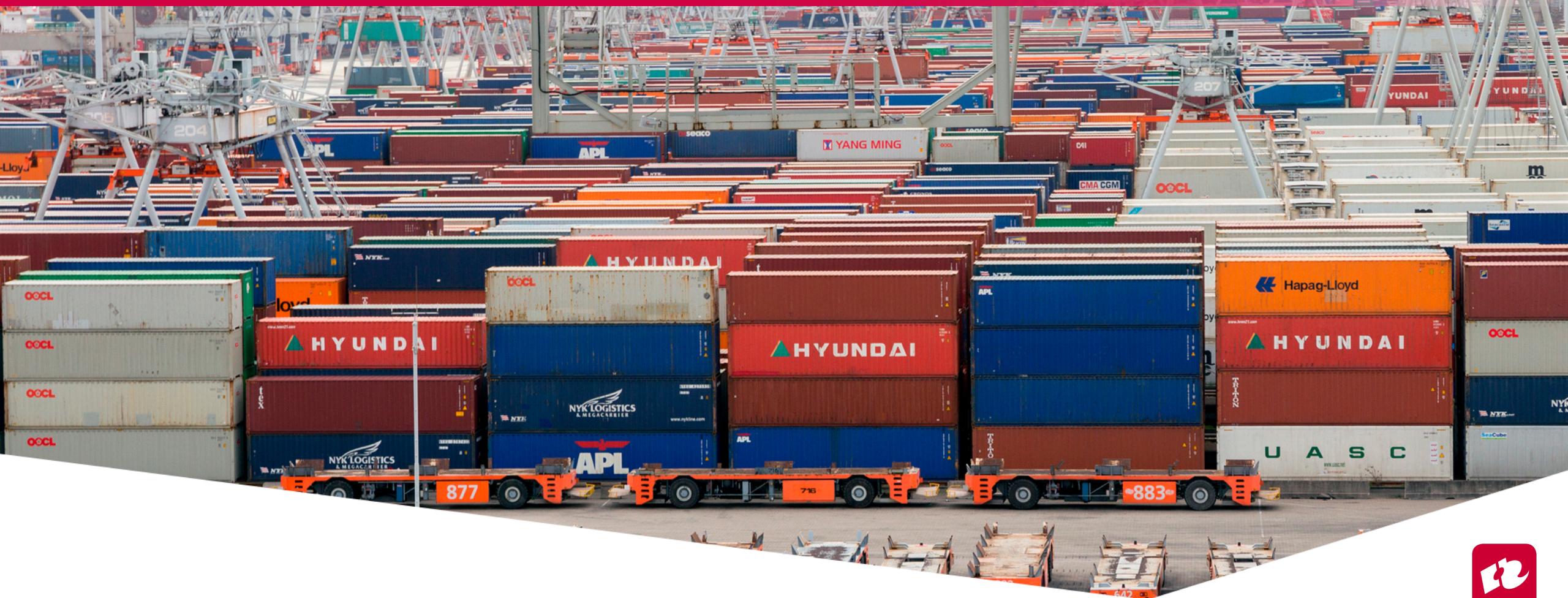
Doe onderzoek naar een real-life voorbeeld van een aanval op een ICS, vooral kijkend naar de technische details.

Zorg dat je verslag bevat hoe de aanval voorkomen had kunnen worden en hoe het opgelost is.

Schrijf een kort verslag en voeg het toe aan je opleverset.



ICwattes?



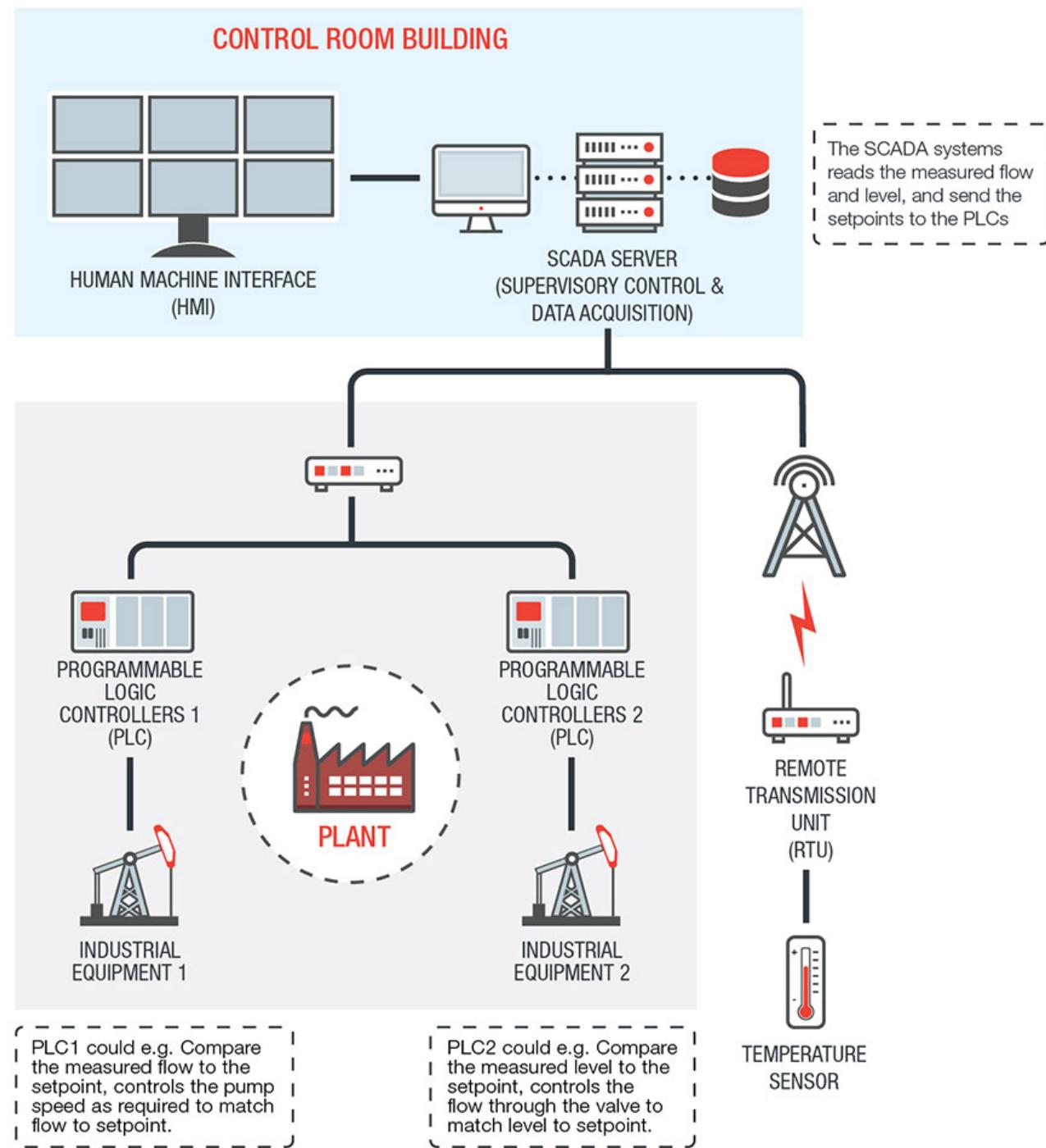
SCADA
PLC
DCS
IACS
PAC
RTU
IED



Industrial Control Systems (ICS)

- Verzamelterm voor verschillende soorten systemen voor het besturen van industriële processen
- Bestaan uit verschillende devices (zoals PLC's) en hebben een Human-Machine Interface (HMI) voor monitoring en controle
- Bekendste voorbeeld: SCADA





Wat maakt deze systemen zo anders?

Samengevat:

“Normale IT-systemen”	Industriële Controlesystemen
Minder kritieke operaties, delays zijn minder erg. Hogere throughput.	Real-time operaties, delays/latency zijn niet acceptabel. Matige throughput
Confidentiality en Integrity (doorgaans) boven Availability	Availability boven Confidentiality en Integrity
Kortere lifetime (3-5 jaar). Meer veranderlijk (denk aan updates).	Langere lifetime (10-15 jaar). Meer statisch.
Standaard (open) communicatieprotocollen en apparatuur	Veel proprietary apparatuur en netwerken

Voor een completer overzicht: [NIST SP 800-82](#): hoofdstuk 2.4 (tabel 2.1)



Vroeger...

- Domme systemen die offline draaien
- Niet flexibel
 - *Bij veranderingen: kabels naar de controlekamer trekken*
- Veelal geïsoleerde, proprietary systemen



Nu...

- Van centrale controle naar *distributed control* met systemen die naar de controlekamer rapporteren
- Steeds meer integratie met (open) industriestandaarden in de IT
- (iets minder) domme systemen die online draaien



Security issues

- ICS leunen vaak op “security by obscurity”
- Legacy communicatieprotocollen zonder security
- Configuratiefouten
 - *ICS niet goed gesegmenteerd binnen bedrijfsnetwerk*
 - *Toegang vanaf het internet met inadequate authenticatie*
 - ...
- Grote afstanden en afgelegenheid van (delen van) een systeem



Verschillen in securityoverwegingen

- ICS werken in de fysieke wereld – meer risico op letsel en serieuze schade aan milieu, economie, etc.
- Integriteit en continuïteit van ICS moet altijd behouden blijven – ook tijdens cyberaanvallen
- IT securitypraktijken kunnen niet altijd 1 op 1 op (veelal legacy) ICS toegepast worden (bijv. encryptie)
- Bij afgelegen onderdelen speelt fysieke beveiliging een grote rol



Hoe het fout kan gaan

- Bijkomende schade door onbedoelde infectie met (non-specifieke) malware
 - *Zotob (2005)*
 - *NotPetya (2017)*



Hoe het fout kan gaan

- Gerichte aanvallen, zoals:
 - *Stuxnet (2010)*
 - *Crash Override/Industroyer (2016)*
 - *Triton/Trisis (2017)*



Maatregelen

- ICS beginnen meer op “gewone” IT te lijken – ook qua security
- Netwerksegregatie
- Monitoring & logging
- Multi-factor authentication
- Principle of Least Privilege (POLP)





overtref jezelf