



IACS & CYBERSECURITY CONFERENCE



April 15th 2025 • Amersfoort • The Netherlands



Het spoor cyberveilig

Lessons learned in de internationale spoorketen



IOIO
IOIO
Of in de
Spoorsector

Samenwerking

Innovatie

Lessons Learned

Samenvatting

Innovatie



IACS & CYBERSECURITY CONFERENCE



Apple Lisa launch

1983

Oplevering



iPod

2001

Modernisering



iPhone

2006

OBIS/RTM



iPhone12 Pro

2020



Vision Pro

2024

Vervanging



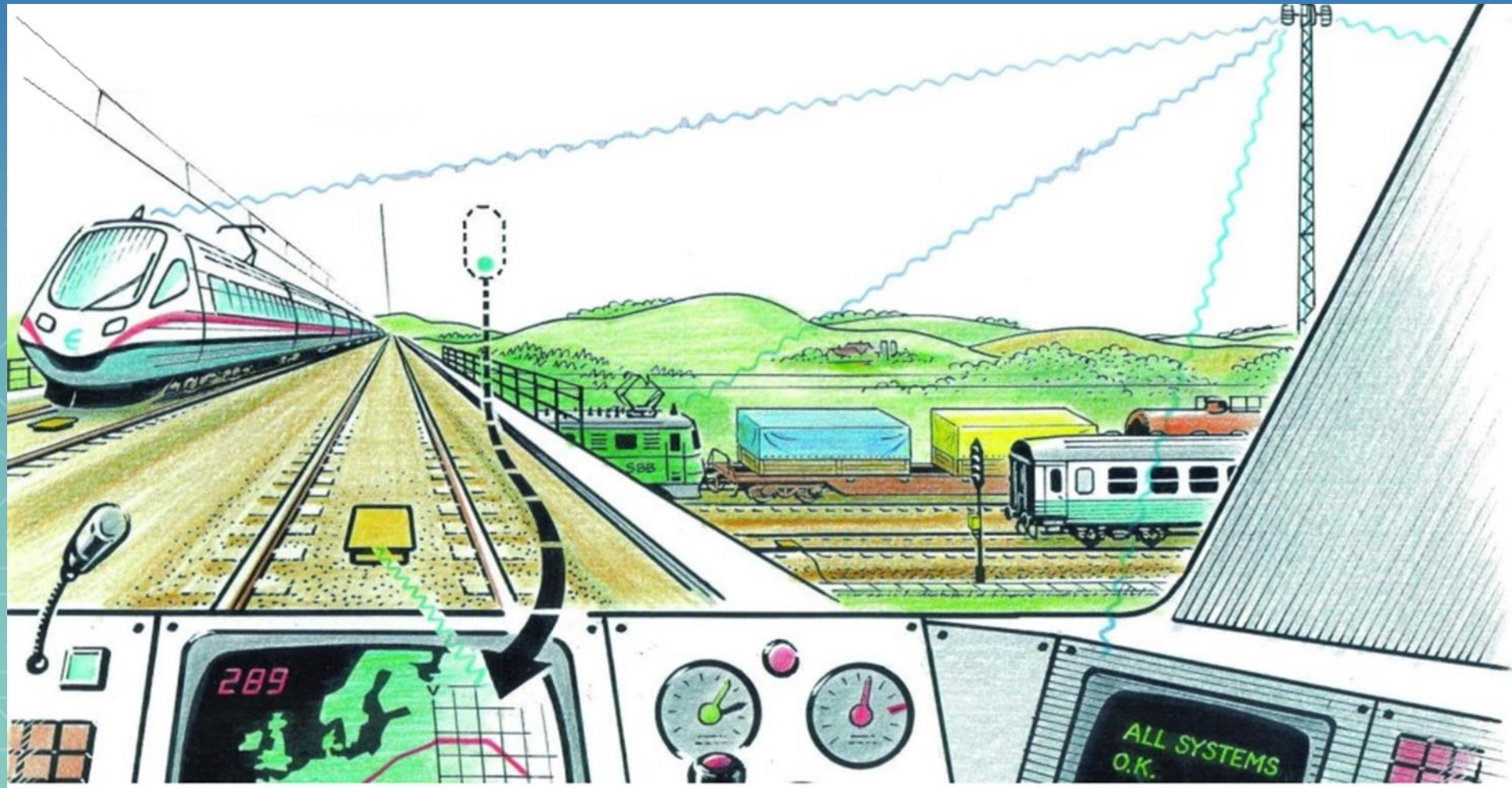
Data Authority for Digital Infrastructure
Ministry of Economic Affairs

National Cyber Security Centre
Ministry of Justice and Security

IACS Coalition

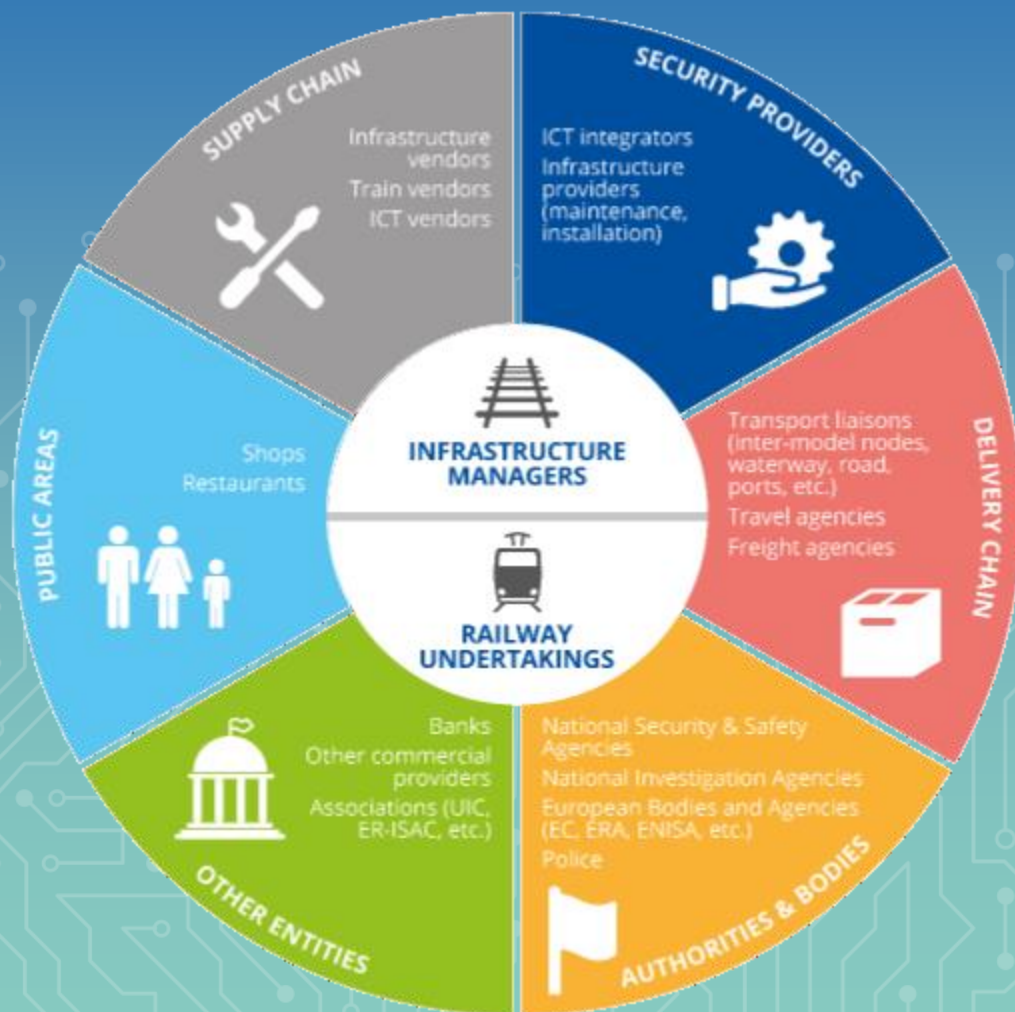


European Rail Traffic Management System





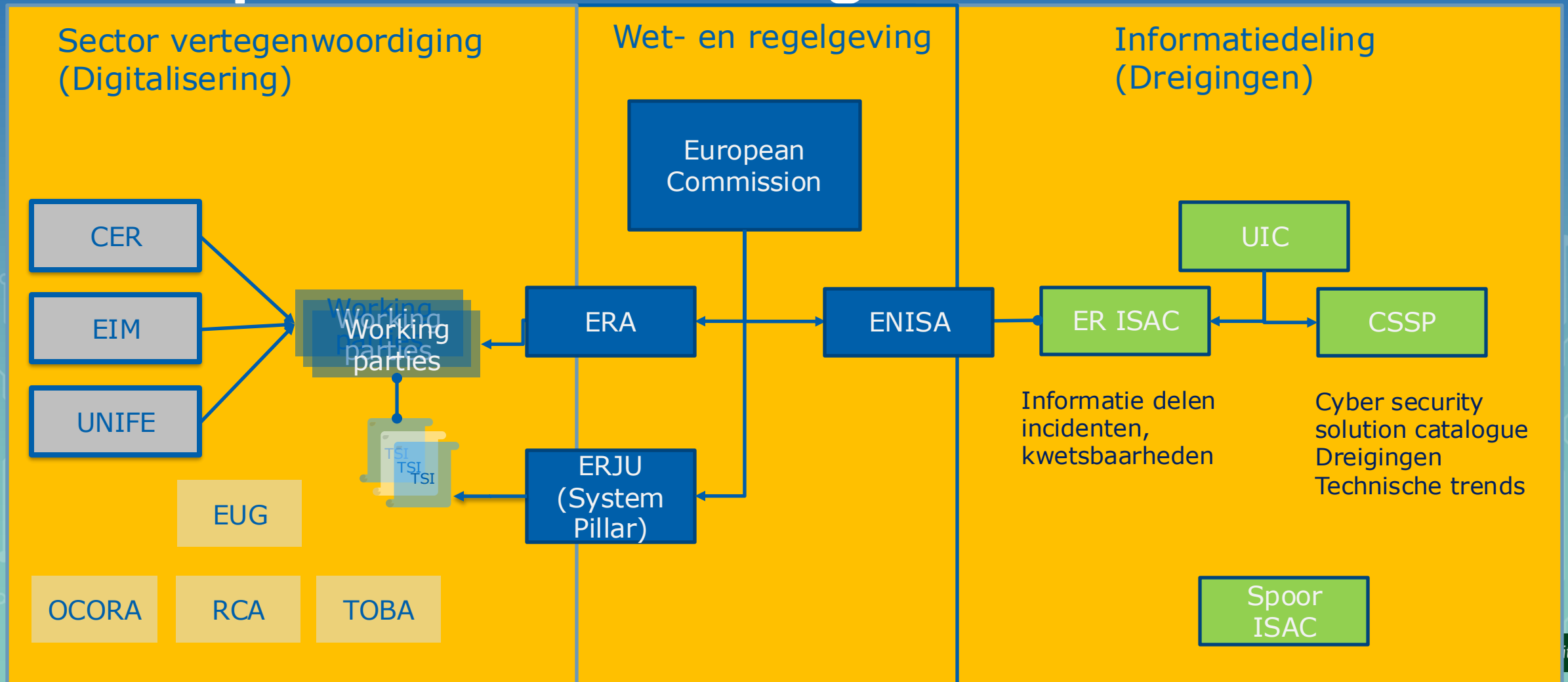
Het ecosysteem van de spoorsector



- Spoorwegondernemingen
- Infrastructuurmanagers
- Leveranciers van treinen
- Leveranciers van spoorwegsysteem
- ICT service providers
- Leveranciers van ICS/ OT assets
- Leveranciers van ICT assets



Europese samenwerking





Noodzaak tot samenwerking in de sector

Spoor digitaliseert, is verbonden, complex en veiligheid staat centraal

Toename in cyber dreiging

Nieuwe, uitdagende cyber wetgeving

We moeten duurzaam een cyber secure cultuur implementeren en verbeteren in onze sector, aangezien:

1. We deze uitdagingen alleen gezamenlijk kunnen aangaan → **The bad people collaborate, so the good people have to collaborate as well!**
2. We moeten samen de horizontale wetgeving efficiënt en succesvol toepassen en input leveren voor specifieke wetgeving om te zorgen dat deze passend en bruikbaar is.



Gemeenschappelijke aandachtspunten

- 25 gemeenschappelijke punten onder meer over NIS2 en CRA, ook cybersecurity versus safety en personeel.
- Om samenwerking op gang te brengen, focus op twee:

Stelsel uitbreidingen

**Classificatie van systemen en componenten
onder de CRA**



IACS & CYBERSECURITY CONFERENCE



Cyber Security deliverables



UNISIG subset 146 & 147
TSI CCS 2023



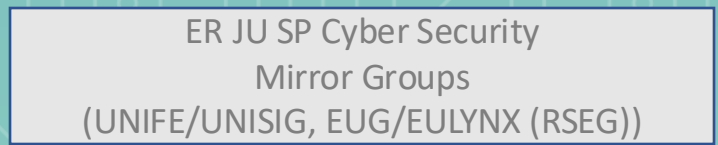
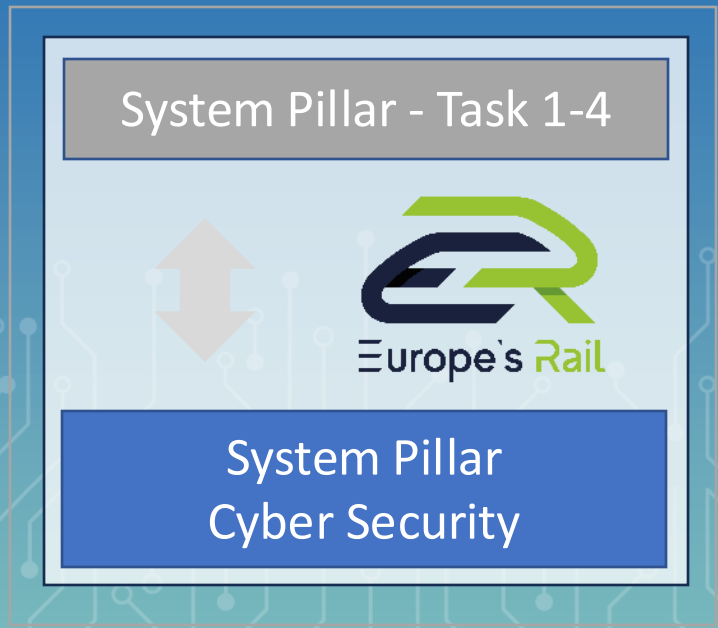
Baseline 4 R2 – Detailed
security requirements



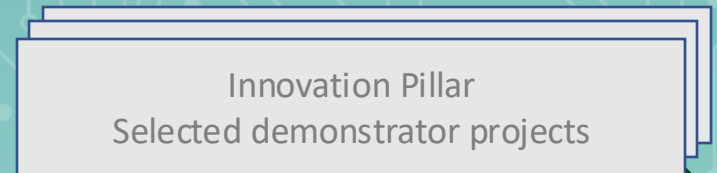
ESCG
Security Measures



42 input documents

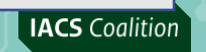


Shared Cybersecurity Services Spec (03/25)
Secure Component Spec (03/25)
Secure Communication Spec (03/25)
Secure Program Requirements (03/25)



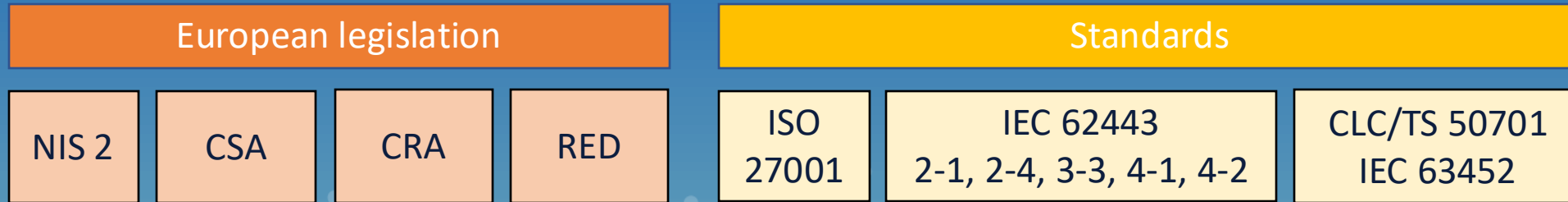
Dutch Authority for Digital
Infrastructure
Ministry of Economic Affairs

National Cyber Security Centre
Ministry of Justice and Security





Europe Cybersecurity Compliance



Target: compliance and full tracing

ER JU System Pillar Cyber Security specifications

Secure Component Spec

Shared Cybersecurity Service Spec

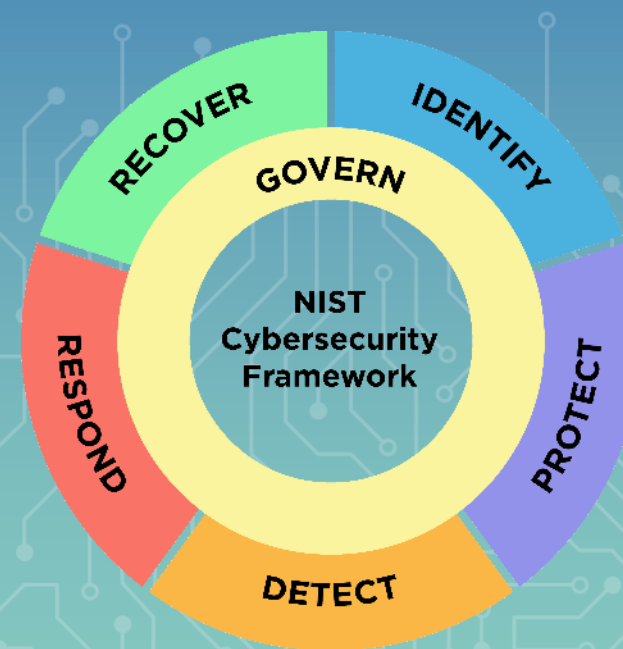
Secure Communication
Spec

Security Program Requirements (Application Guidelines)



Innovation and lessons learned

- Aan de hand van NIST Cyber Security Framework 2.0
- Hoe krijg je security embedded
- Where do we go from here? (*Marillion*)





Everybody's favorite: NIST - Govern

- NS is ISO55000 gecertificeerd (kwaliteitsysteem)
- Materieel Park Plan (MPP) - Vlootmanager
- Strategisch Asset Management Plan (SAMP) – Netwerk Ontwerp
- Levensloopplan (LLP) per serie - Materieelmanager



NIST - Identify

- SAMP: Alle materieelseries waar NS de ECM-1 rol heeft, heeft een actuele cyberrisico-analyse.
- SAMP: Alle materieelseries waar NS de ECM-1 rol heeft en significante impact op de operatie kan veroorzaken, heeft een cyberherstelplan.
- Materieelmanager verantwoordelijk, beschijft planning in LLP.
 - Bewaakt door vlootmanager



NIST - Identify

- Cyberrisico's plotten op NS Risico-matrix
 - Materieelmanager kan beslissen "Fix ik als eerste cyber of de rem".

A7	B7	C7	D7	E7	F7
A6	B6	C6	D6	E6	F6
A5	B5	C5	D5	E5	F5
A4	B4	C4	D4	E4	F4
A3	B3	C3	D3	E3	F3
A2	B2	C2	D2	E2	F2
A1	B1	C1	D1	E1	F1



NIST - Protect / Detect / Respond

- Security Appliance
- Aansluiten bij bestaande response processen
 - (Digitale) storingen handelen we al af
 - Classificatie naar impact (veiligheidsstoringen) doen we al
 - Escalaties en mandaten zijn al ingericht



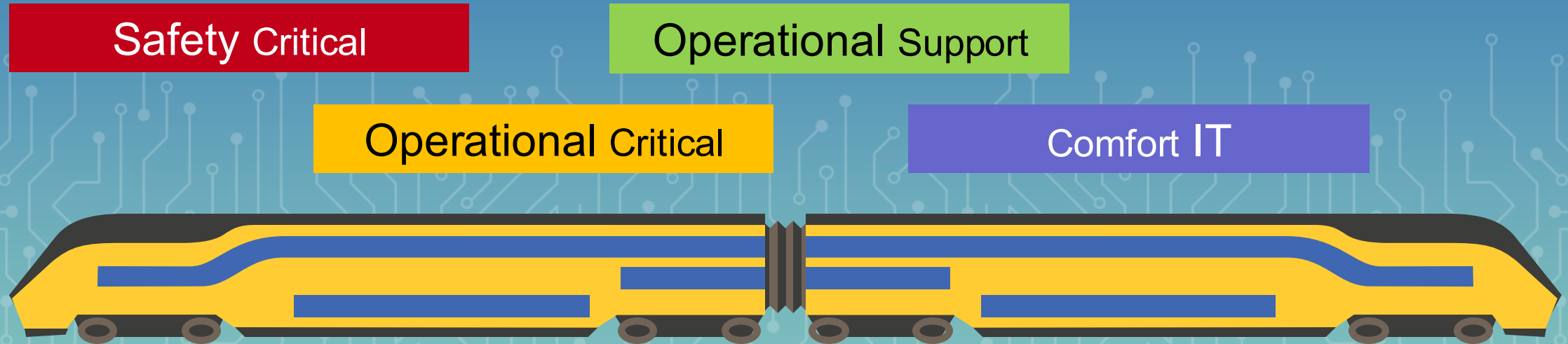
Security Appliance

- Firewall / intrusion detection / anomaly detection aan boord
- Hardware en software apart aanbesteed
 - Trein-gecertificeerde hardware
 - COTS security software





Security Appliance – Firewall



- Beheer Security Appliance in de Treindigitalisering-organisatie



Security Appliance – IDS

- Aansluiten bij NS SOC
 - Gebruik bestaande processen en organisatie
- Escalatie en opvolging in de lijn (NS Techniek)
- SOC levert kennis van events / malware om impact te bepalen



Security Appliance – Rode knoppen

- Strategie gericht op containment
 - Vastgelegd in playbooks / afhandelsscenario's
- Gemandateerde acties op materieel (geeft snelheid)
 - Wifi in de trein uit
 - IT/OT scheiden
 - Boord/Wal verbinding uit



Recover

- SAMP: Relevante treinseries hebben een getest herstelplan.
- Hoe doe je dat?
 - Wisseldelen?
 - Factory reset?
 - Hoe voorkom je herbesmetting?



Recover

- SAMP: Relevante treinseries hebben een getest herstelplan.
- Hoe herstel je 1 trein?
- Hoe herstel je 100 Treinen?
- Hoe verschilt dat per serie?





Recover

- Plannen voor herstel essentiële systemen
- En testen, testen, testen
- Te allen tijden een veilig inzetbare trein





Oefenen – oefenen – oefenen

- Kan op vele manieren
- Gebruik ieder incident voor aandacht, maar hou het realistisch...

NIGHTSLEEPER



DAYDREAMER











318

8

V

317

Samenvatting

-  Samenwerking is noodzakelijk
-  Lange tijdlijnen regelgeving, maar wel grote impact
-  Integreer zoveel mogelijk: bedrijfsproces of IT proces
-  Zet in op marktconforme oplossingen



Vragen

