OT & CYBERSECURITY CONFERENTIE

22 April 2026 • Amersfoort

Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

OT Coalitie

OT & CYBERSECURITY CONFERENTIE

OT hoeft niet verbonden te zijn!

Traditionele benaderingen voor OT-beveiliging schieten tekort wanneer staten cybermiddelen inzetten

Maurice Snoeren (maurice.snoeren@rwe.com)

Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

OT Coalitie

OT & CYBERSECURITY CONFERENTIE

Cyber was de oorlog die je niet ziet!

- Staten gebruiken cyber als officieel machtsinstrument
- Openlijke dreigingen richting kritische infrastructuur
- Cyber wordt gecombineerd met kinetische militaire operaties
- Aanvallen richten zich op maatschappelijke ontwrichting

OT & CYBERSECURITY CONFERENTIE

Cyber als strategisch wapen

- Onze grootste kwetsbaarheid is onze afhankelijkheid
- Cyberaanvallen worden ingezet om:
  - logistiek en communicatie te verstoren
  - militaire operaties te ondersteunen
  - politieke druk uit te oefenen
  - maatschappelijke ontwrichting te realiseren
- We vertrouwen op software en we weten niet volledig wat erin zit

OT als doelwit

De vraag is niet óf cyber impact heeft, maar wanneer en hoe groot

- OT stuurt kritische processen: energie, water, industrie, telecom
- Kritieke infrastructuur militair doelwit → OT automatisch ook
- Uitval heeft directe operationele en maatschappelijke impact
- Toenemende connectiviteit van OT
- Systemen ontworpen voor beschikbaarheid, niet security

Statelijke actoren

- Focus op OT en kritische infrastructuur
- Voorbereiding op sabotage bij geopolitieke escalatie
- Gebruik van legitieme tools en accounts
- Zero-days zijn geen uitzondering (~90 zero-days misbruikt 2025)
- AI gedreven (autonome) aanvallen

→ Vertrouwen op software is risico

Herstelcapaciteit?

- Aanvallers richten op maximale schade OT infrastructuur
- Kritische componenten hebben lange levertijden
- Sterke afhankelijkheid van internationale supply chains
- Focus moet verschuiven naar resilience & damage containment
- Security moet werken, zelfs als software faalt

OT & CYBERSECURITY CONFERENTIE

Hackdriehoek

OT & CYBERSECURITY CONFERENTIE

Hackdriehoek

géén controle

Bekende en onbekende kwetsbaarheden in software, processen en menselijk gedrag

Maatschappelijke ontwrichting en/of verstoren/sabotage kritische infrastructuur door OT-systemen aan te vallen.

Statelijke actoren die kwetsbaarheden benutten om bij de kroonjuwelen te komen

OT & CYBERSECURITY CONFERENTIE

Hackdriehoek

OT & CYBERSECURITY CONFERENTIE

Hackdriehoek

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

OT & CYBERSECURITY CONFERENTIE

Traditionele benaderingen voor OT-beveiliging

- Het kan niet uitvallen, want we hebben redundantie en veiligheidssystemen.
- De OT-omgeving is beschermd zolang je regelmatig updates en patches toepast.
- De OT-omgeving is niet verbonden met de buitenwereld.
- Beveiliging vaak gebaseerd op software, zoals firewalls, VPN's, etc.

Traditionele benaderingen voor OT-beveiliging

- Het kan niet [illegible] systemen.
- De OT-omgeving is beschermd zolang je regelmatig updates en patches toepast.
- De OT-omgeving is niet verbonden met de buitenwereld.
- Beveiliging vaak gebaseerd op software, zoals firewalls, VPN's, etc.

vertrouw niet alléén op software voor security én niet alle functionaliteiten hoeft verbonden te zijn!

OT & CYBERSECURITY CONFERENTIE

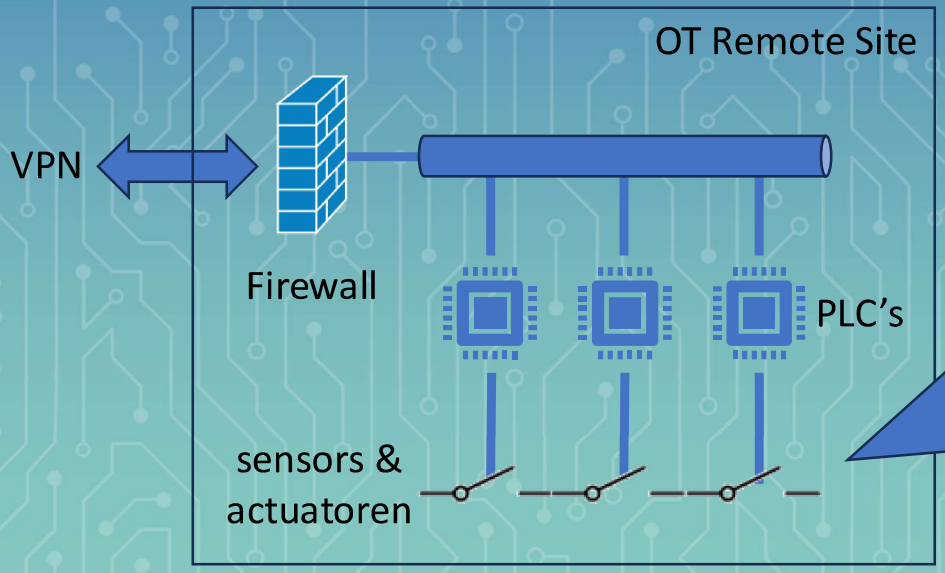
Een andere aanpak voor deze verbindingen is noodzakelijk

- Zorg dat een kwetsbaarheid niet meteen toegang geeft tot je OT asset
- Zorg dat OT assets géén blijvende schade op kunnen lopen
- Zorg voor beveiligingsmechanismen die op zich zelf staan
- Zorg voor weerbaarheid door snel te kunnen herstellen
- Zorg voor mogelijk herstel zonder automatiseringssysteem*
- Zorg voor security monitoring van deze verbindingen
- Negeer waarschijnlijkheid bij risico's met hoge maatschappelijke impact

* Voor zover dat mogelijk is

Voorbeeld hoe OT te verbinden

Een systeem is zó ontworpen en ingericht is dat, zelfs als het wordt gecompromitteerd, de impact beperkt blijft tot de strikt bedoelde functionaliteit.

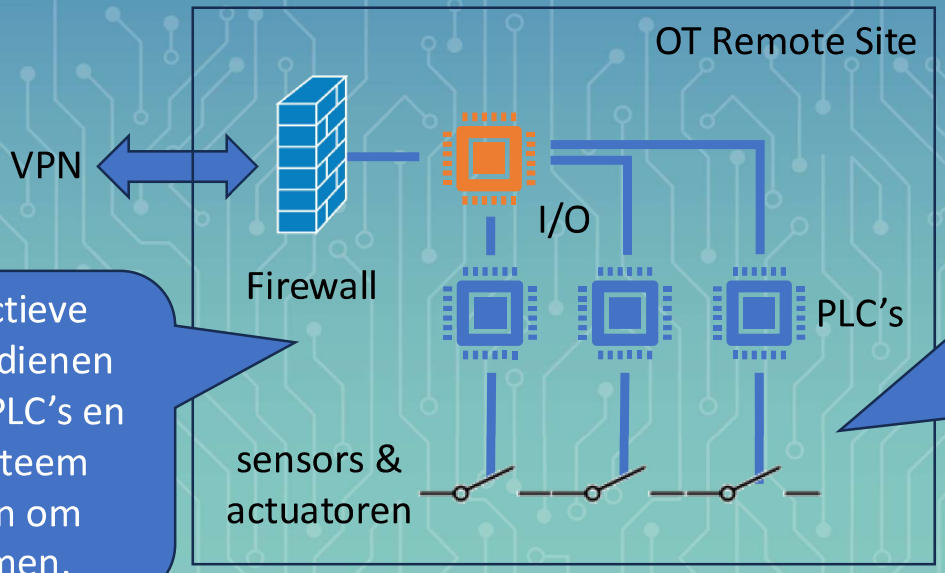


Traditionele aanpak met firewall en VPN. Er moet op afstand geschakeld worden. Bij compromitteren van de VPN kan de aanvaller alle achterliggende PLC's aanvallen door de kwetsbaarheden te misbruiken.

OT & CYBERSECURITY CONFERENTIE

Voorbeeld hoe OT te verbinden

Een systeem is zó ontworpen en ingericht is dat, zelfs als het wordt gecompromitteerd, de impact beperkt blijft tot de strikt bedoelde functionaliteit.



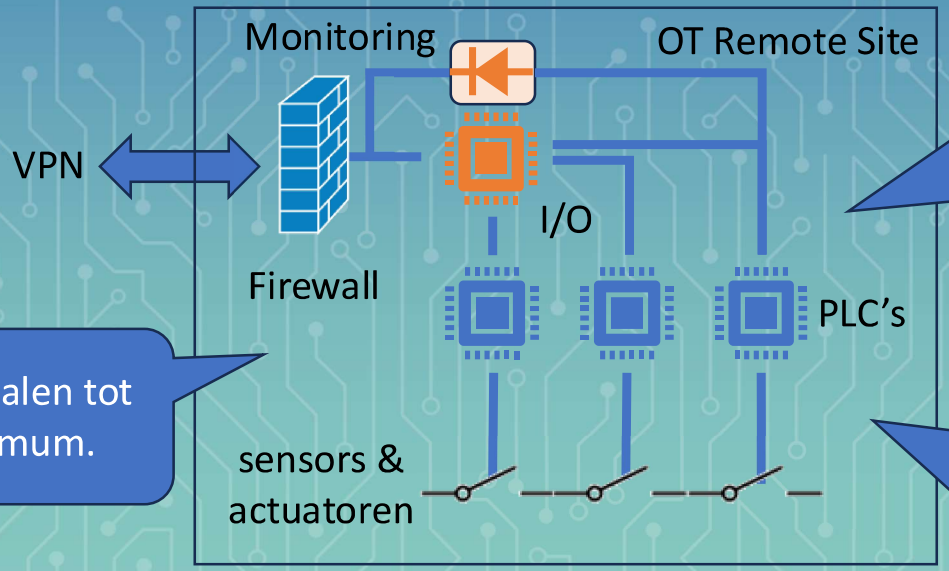
Foutieve of destructieve schakelhandelingen dienen door de logica in de PLC's en een apart safetysysteem afgevangen worden om schade te voorkomen.

Er moet op afstand geschakeld worden. Bij compromitteren van de VPN kan de aanvaller alleen schakelen en niet meer andere systemen aanvallen.

OT & CYBERSECURITY CONFERENTIE

Voorbeeld hoe OT te verbinden

Een systeem is zó ontworpen en ingericht is dat, zelfs als het wordt gecompromitteerd, de impact beperkt blijft tot de strikt bedoelde functionaliteit.



Proces en security monitoring met data-diodes zodat er geen extra aanvalsvector ontstaat.

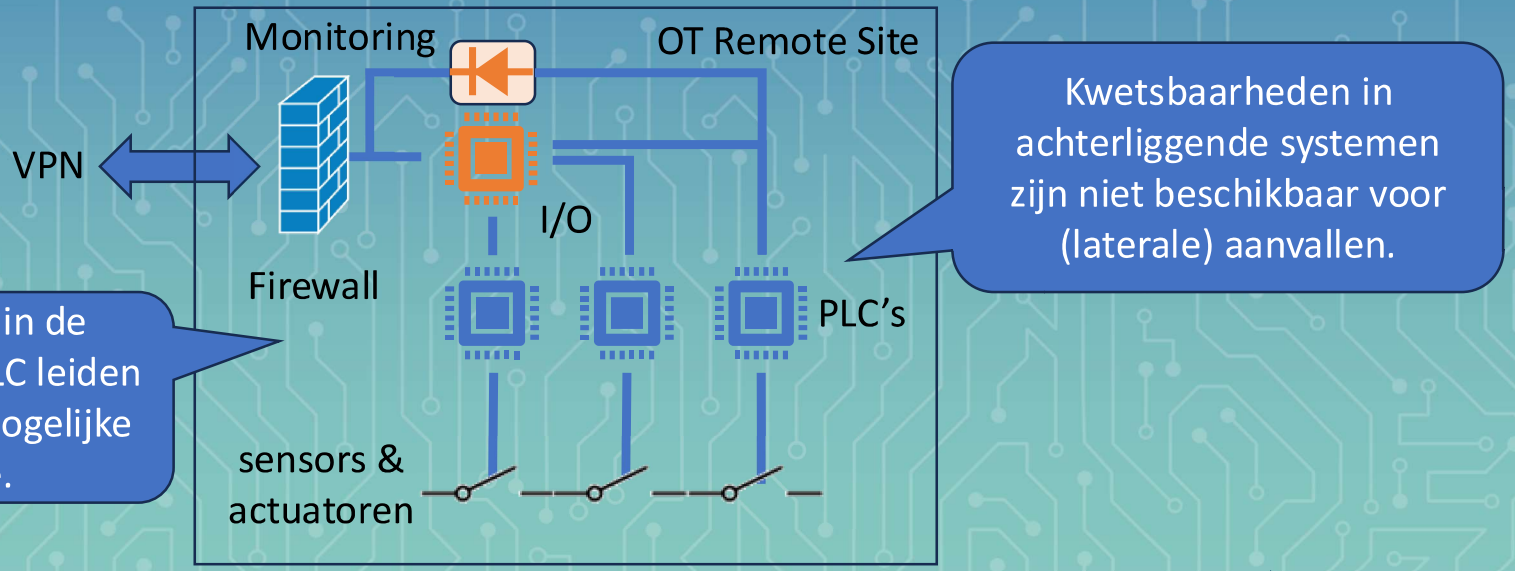
Beperk de stuursignalen tot het absolute minimum.

Zorg voor de mogelijkheid om handmatig in te grijpen voor snel herstel.

OT & CYBERSECURITY CONFERENTIE

Voorbeeld hoe OT te verbinden

Een systeem is zó ontworpen en ingericht is dat, zelfs als het wordt gecompromitteerd, de impact beperkt blijft tot de strikt bedoelde functionaliteit.

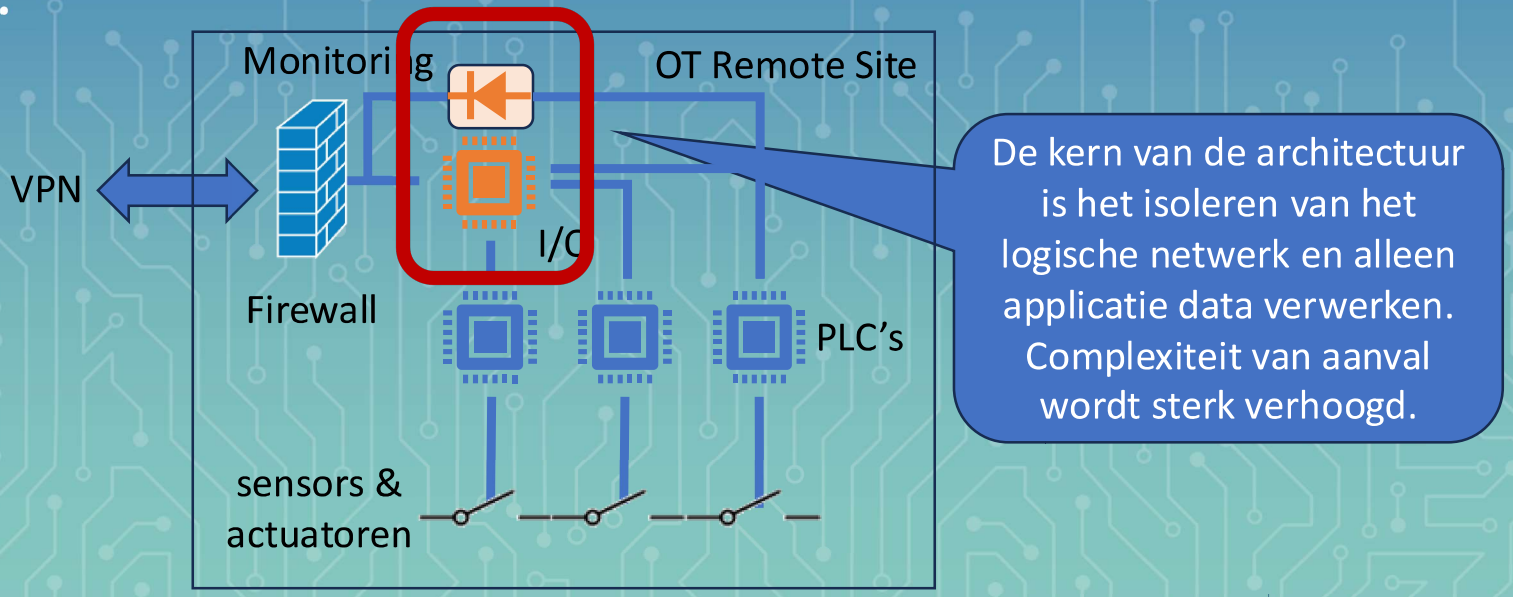


Kwetsbaarheden in achterliggende systemen zijn niet beschikbaar voor (laterale) aanvallen.

Kwetsbaarheden in de firewall en koppel PLC leiden niet meteen naar mogelijke grote schade.

Voorbeeld hoe OT te verbinden

Een systeem is zó ontworpen en ingericht is dat, zelfs als het wordt gecompromitteerd, de impact beperkt blijft tot de strikt bedoelde functionaliteit.



OT & CYBERSECURITY CONFERENTIE

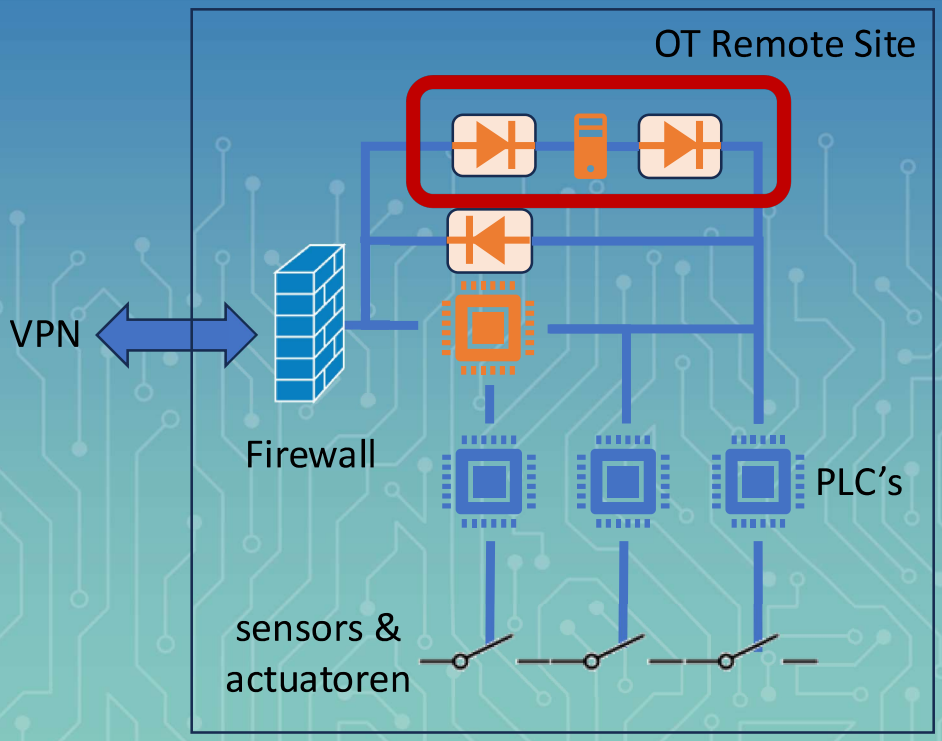
Uitdagingen

- Traditionele IT-aanpak domineert nog steeds voor OT verbindingen
- Beperkte kennis en onbegrip m.b.t. data-diode technology
- Restrisico's dienen nog steeds gemitigeerd te worden
- Het gaat niet over preventie, maar over weerbaarheid, herstelbaarheid en verhogen aanvalscomplexiteit
- Logische netwerkscheiding lijkt lastig, maar is écht mogelijk
- Remote toegang en updates blijft een uitdaging, maar is ook zeker mogelijk

OT & CYBERSECURITY CONFERENTIE

Remote toegang en updates onderzoek

- Logische netwerkisolatie blijft
- Één aanvalsvector (software)
- Belang van human-in-the-loop
- Onafhankelijk controle systeem
- Zelf in control: Geen vendor lock-in
- Rest risico: Kwaadwillende update en toegang



OT & CYBERSECURITY CONFERENTIE

Samenvatting

- OT hoeft niet verbonden te zijn!
- Cyber wordt zichtbaar ingezet door staten
- OT is een doelwit voor verstoring en ontwrichting
- Statelijke actoren manipuleren software
- Focus op weerbaarheid en beperken schade
- Voor OT-beveiliging minder afhankelijk van software
- Dwing voor OT-verbinding alleen de benodigde functionaliteit af
- Logische netwerkscheiding: Het is uitdagend, maar het kan écht!

OT & CYBERSECURITY CONFERENTIE

OT hoeft niet verbonden te zijn!

Traditionele benaderingen voor OT-beveiliging schieten tekort wanneer staten cybermiddelen inzetten

Maurice Snoeren (maurice.snoeren@rwe.com)

Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

OT Coalitie