KU LEUVEN

Hoe kwetsbaar is mijn industriële infrastructuur voor cyberaanvallers?

Bart Huyck
Hendrik Derre
Onderzoeksgroep E&A
KU Leuven Campus Gent

AGENTSCHAP INNOVEREN & ONDERNEMEN
EFRO EUROPEES FONDS VOOR REGIONALE ONTWIKKELING
Europese Unie
howest De Hogeschool West-Vlaanderen Lid van de Associatie Universiteit Gent
GHENT UNIVERSITY

KU LEUVEN

Hoe kwetsbaar is mijn industriële infrastructuur voor cyberaanvallers?

Bart Huyck
Hendrik Derre
Onderzoeksgroep E&A
KU Leuven Campus Gent

KU LEUVEN



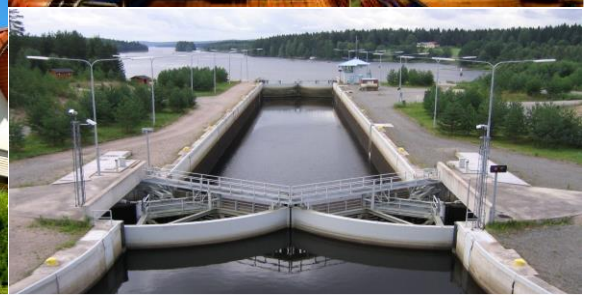








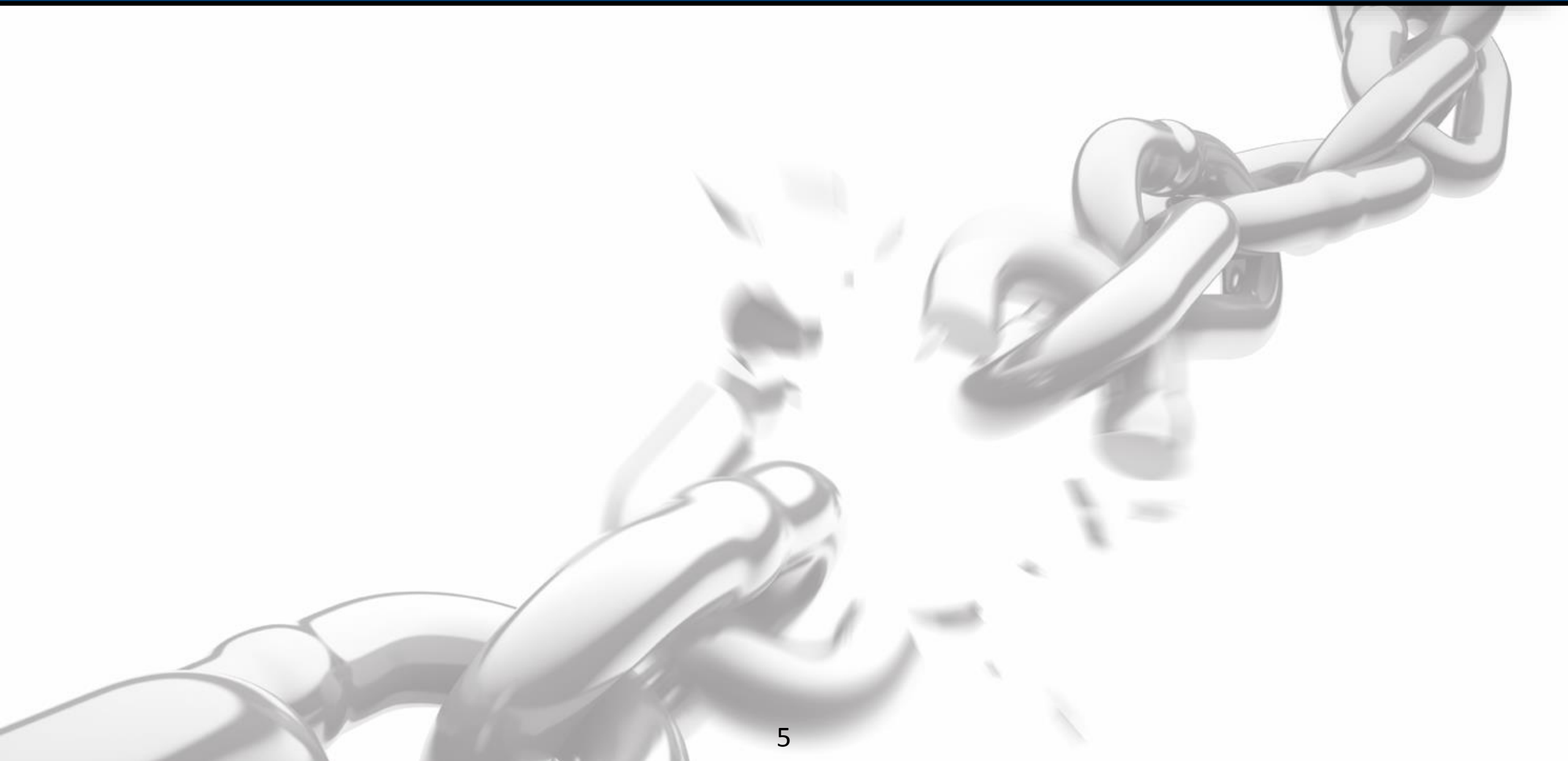


KU LEUVEN

Kwetsbaarheden industriële infrastructuur

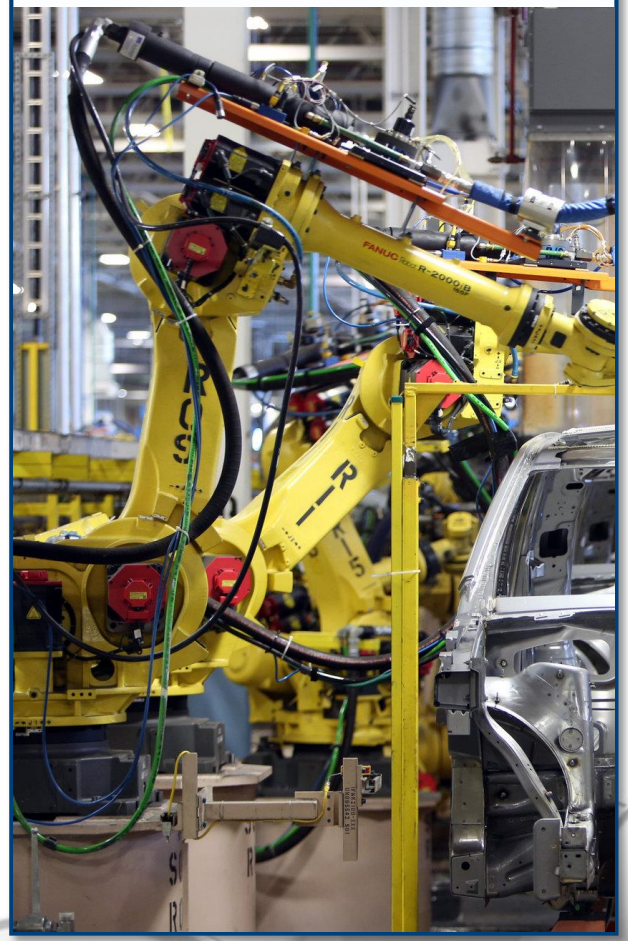
KU LEUVEN



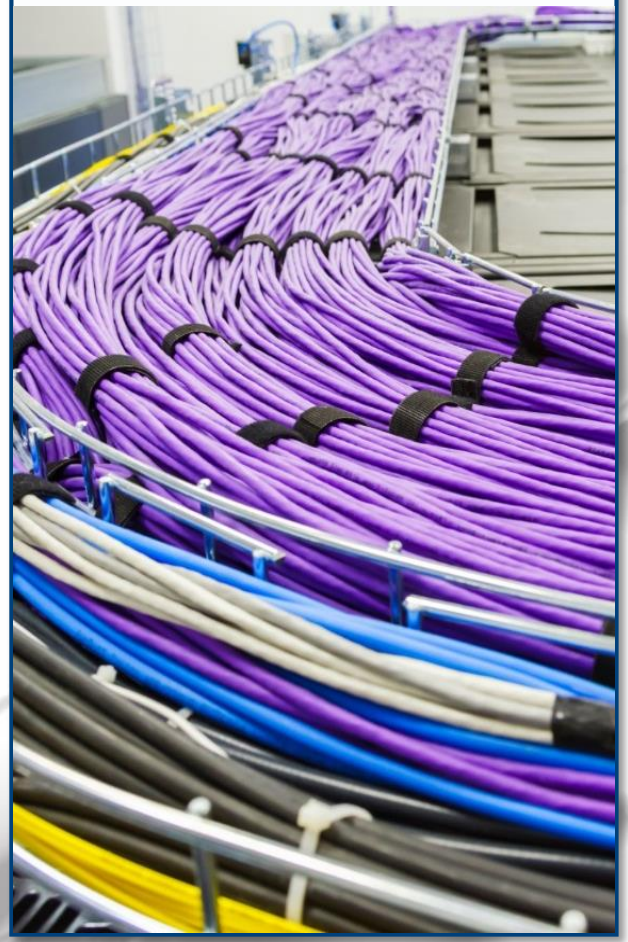
Kwetsbaarheden industriële infrastructuur

KU LEUVEN

Kwetsbare platformen



Kwetsbare Netwerken

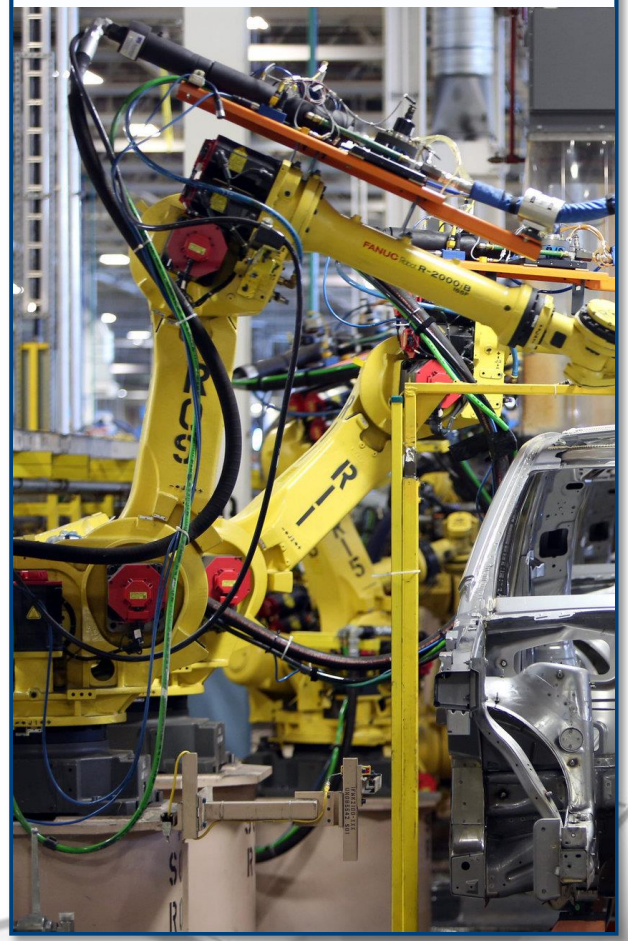


Zwakke procedures & beleid

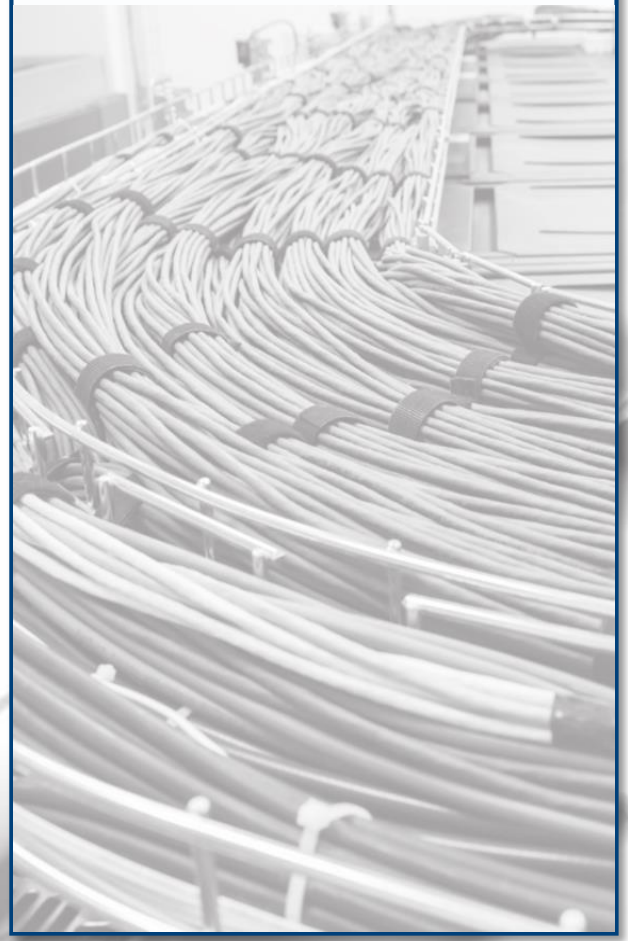
Kwetsbaarheden industriële infrastructuur

KU LEUVEN

Kwetsbare platformen

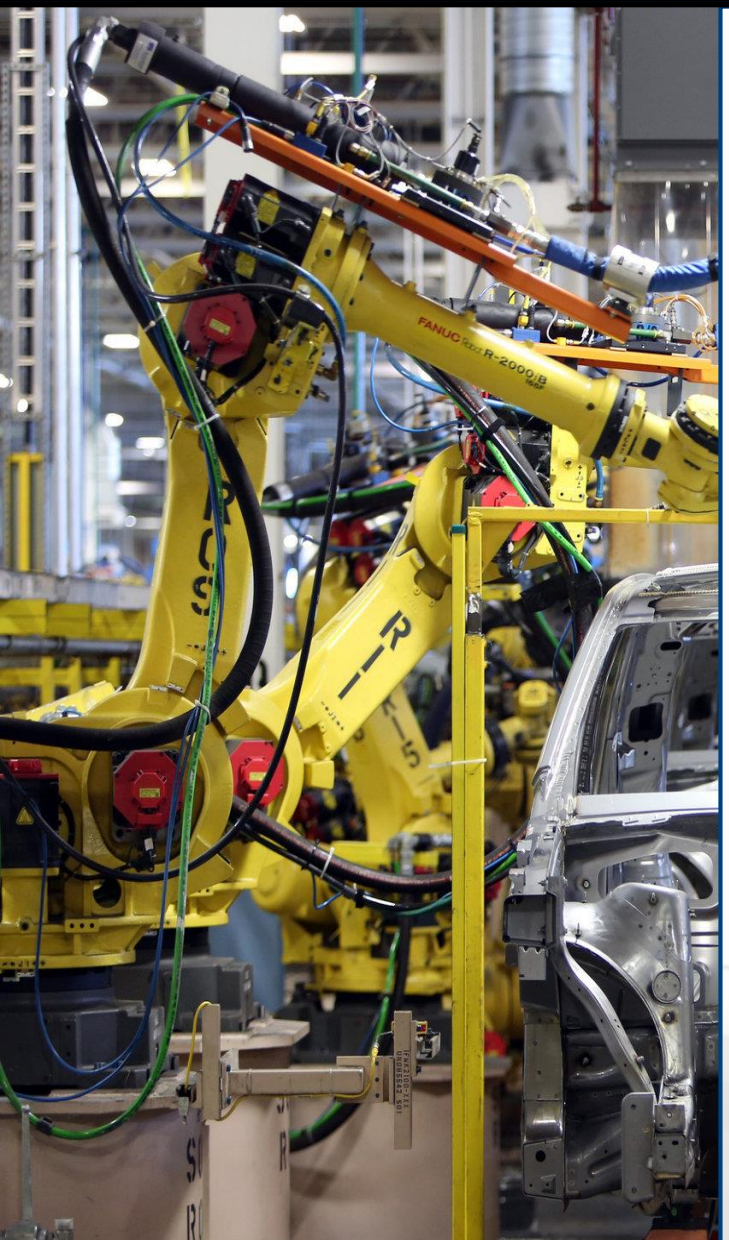


Kwetsbare Netwerken



Zwakke procedures & beleid

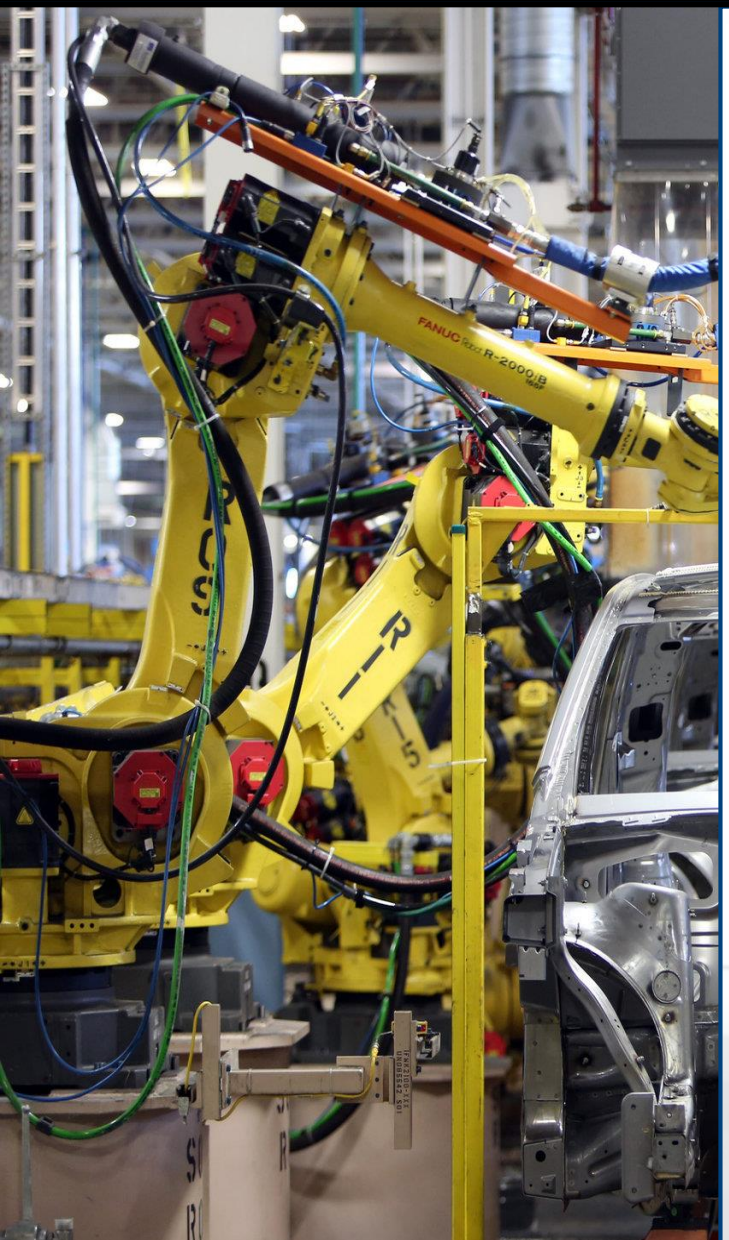
Kwetsbare Platformen



- Weinig tot geen aandacht voor security bij ontwikkeling
  - Keuze van gebruikte technologie
  - Security testen bij ontwikkeling?
- Weinig tot geen aandacht voor security bij implementatie
  - Default configuraties (inclusief default passwoorden)
- Levensduur van industriële componenten
  - Vaak onherstelbare kwetsbaarheden
  - Gebruik van niet meer ondersteunde software
- Niet of traag updaten van systemen

Kwetsbare Platformen

KU LEUVEN



ICS-CERT Monitor Newsletters

ICS-CERT publishes the Monitor Newsletter when an adequate amount of pertinent information has been collected. We provide this newsletter as a service to personnel actively engaged in the protection of critical infrastructure assets.

Recent Product Releases

Alerts

ICS-ALERT-16-286-01 Sierra Wireless Mitigations Against Mirai Malware, October 12, 2016

ICS-ALERT-16-263-01 BINOM3 Electric Power Quality Meter Vulnerabilities, September 19, 2016

ICS-ALERT-16-256-01 FENIKS PRO Elnet Energy Meter Vulnerabilities, September 12, 2016

ICS-ALERT-16-256-02 Schneider Electric ION Power Meter CSRF Vulnerability, September 12, 2016

Advisories

View Advisories Feed

ICSA-16-301-01 Honeywell Experion PKS Improper Input Validation Vulnerability, October 27, 2016

ICSA-16-299-01 Siemens SICAM RTU Devices Denial-of-Service Vulnerability, October 25, 2016

ICSA-16-294-01 Moxa EDR-810 Industrial Secure Router Privilege Escalation Vulnerability, October 20, 2016

ICSA-16-292-01 Schneider Electric PowerLogic PM8ECC Hard-coded Password Vulnerability, October 18, 2016

ICSA-16-287-01 OSIsoft PI Web API 2015 R2 Service Account Permissions Vulnerability, October 13, 2016

ICSA-16-287-02 Siemens Automation License Manager Vulnerabilities, October 13, 2016

ICSA-16-287-03 Siemens SIMATIC STEP 7 (TIA Portal) Information Disclosure Vulnerabilities, October 13, 2016

ICSA-16-287-04 Rockwell Automation Stratix Denial-of-Service and Memory Leak Vulnerabilities, October 13, 2016

ICSA-16-287-05 Moxa ioLogik E1200 Series Vulnerabilities, October 13, 2016

ICSA-16-287-06 Fatek Automation Designer Memory Corruption Vulnerabilities, October 13, 2016

ICSA-16-287-07 Kabona AB WDC Vulnerabilities, October 13, 2016

ICSA-16-252-01 GE Bently Nevada 3500/22M Improper Authorization Vulnerability, October 6, 2016

ICSMA-16-279-01 Animas OneTouch Ping Insulin Pump Vulnerabilities, October 5, 2016

ICSA-16-278-01 INDAS Web SCADA Path Traversal Vulnerability, October 4, 2016

ICSA-16-278-02 Beckhoff Embedded PC Images and TwinCAT Components Vulnerabilities, October 4, 2016

ICSA-16-273-01 American Auto-Matrix Front-End Solutions Vulnerabilities, September 29, 2016

ICSA-16-271-01 Siemens SCALANCE M-800/S615 Web Vulnerability, September 27, 2016

ICSA-16-264-01 Moxa Active OPC Server Unquoted Service Path Escalation Vulnerability, September 20, 2016

ICSA-16-259-01 Yokogawa STARDOM Authentication Bypass Vulnerability, September 15, 2016

ICSA-16-259-02 ABB DataManagerPro Credential Management Vulnerability, September 15, 2016

ICSA-16-259-03 Trane Tracer SC Sensitive Information Exposure Vulnerability, September 15, 2016

ICSA-16-224-02 Rockwell Automation RSLogix 500 AND RSLogix Micro File Parser Buffer Overflow Vulnerability, September 15, 2016

ICSA-16-250-01 Siemens SIPROTEC 4 and SIPROTEC Compact Vulnerabilities, September 6, 2016

Other

Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies, September 13, 2016

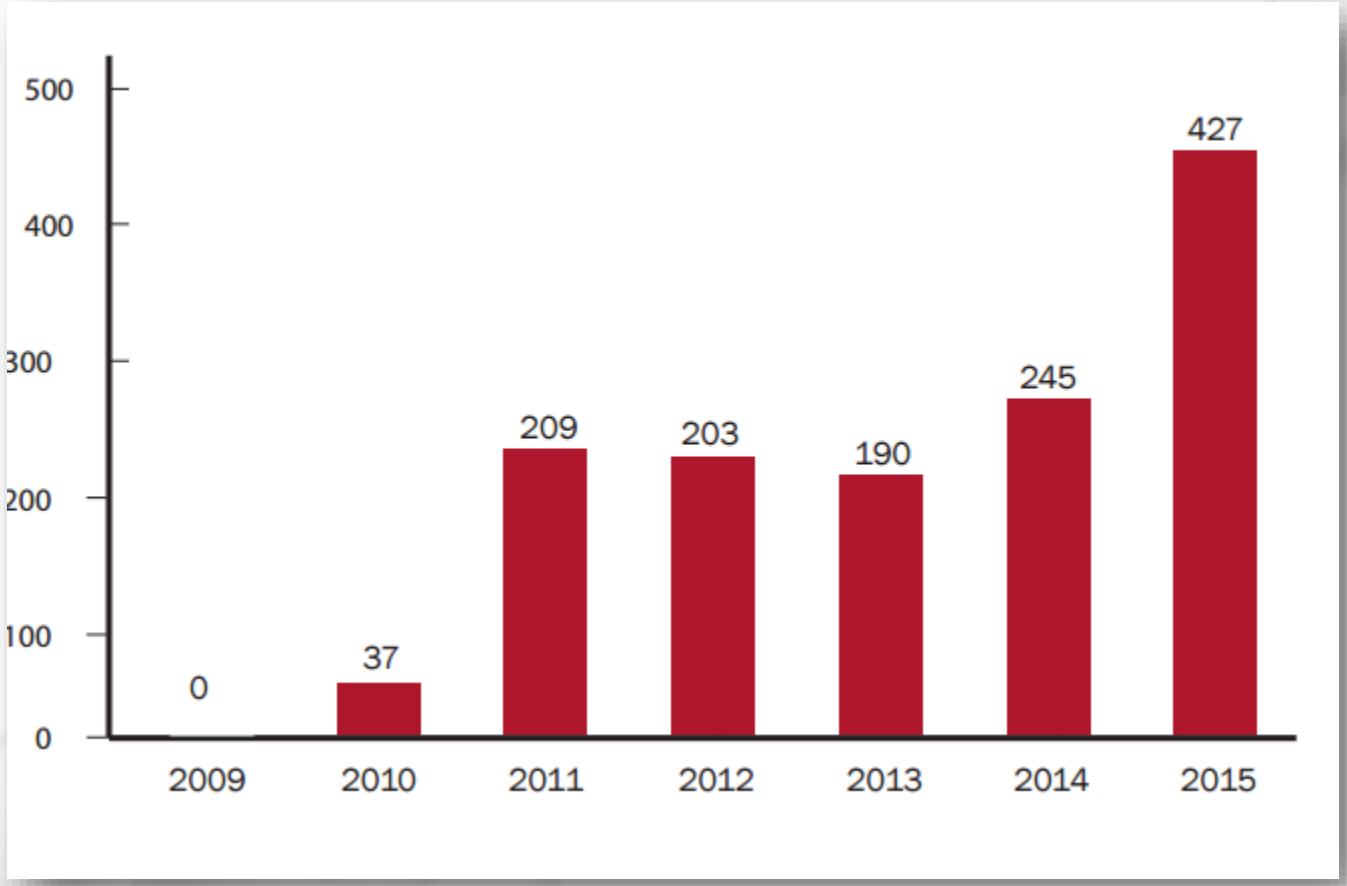
NCCIC/ICS-CERT FY 2015 Annual Vulnerability Coordination Report, September 28, 2016

Follow ICS-CERT on Twitter: @icscert

ics-cert.us-cert.gov/

Kwetsbare Platformen

KU LEUVEN



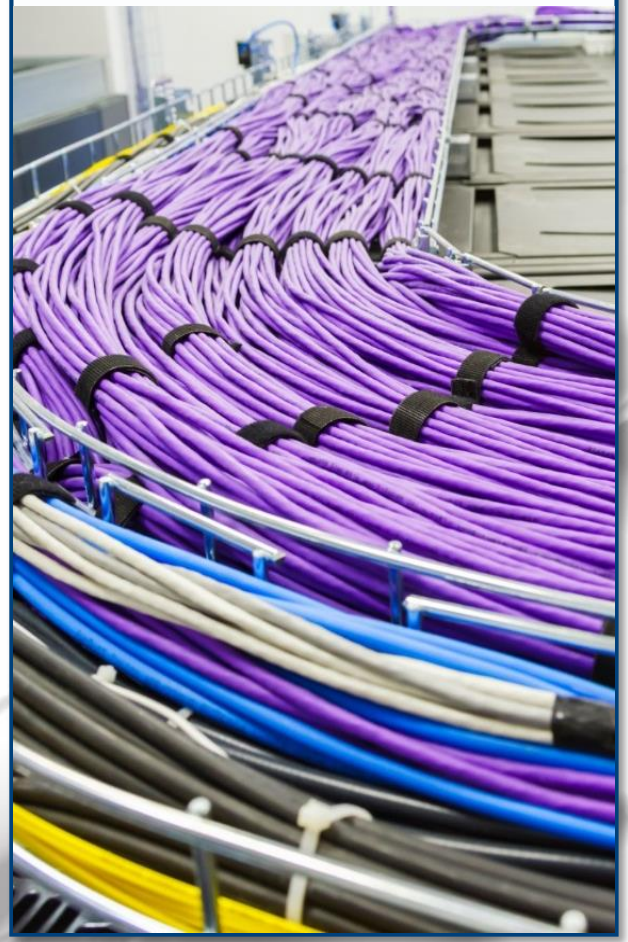
Number of vulnerabilities reported to ICS-CERT 2009 through FY 2015

Kwetsbaarheden industriële infrastructuur

KU LEUVEN

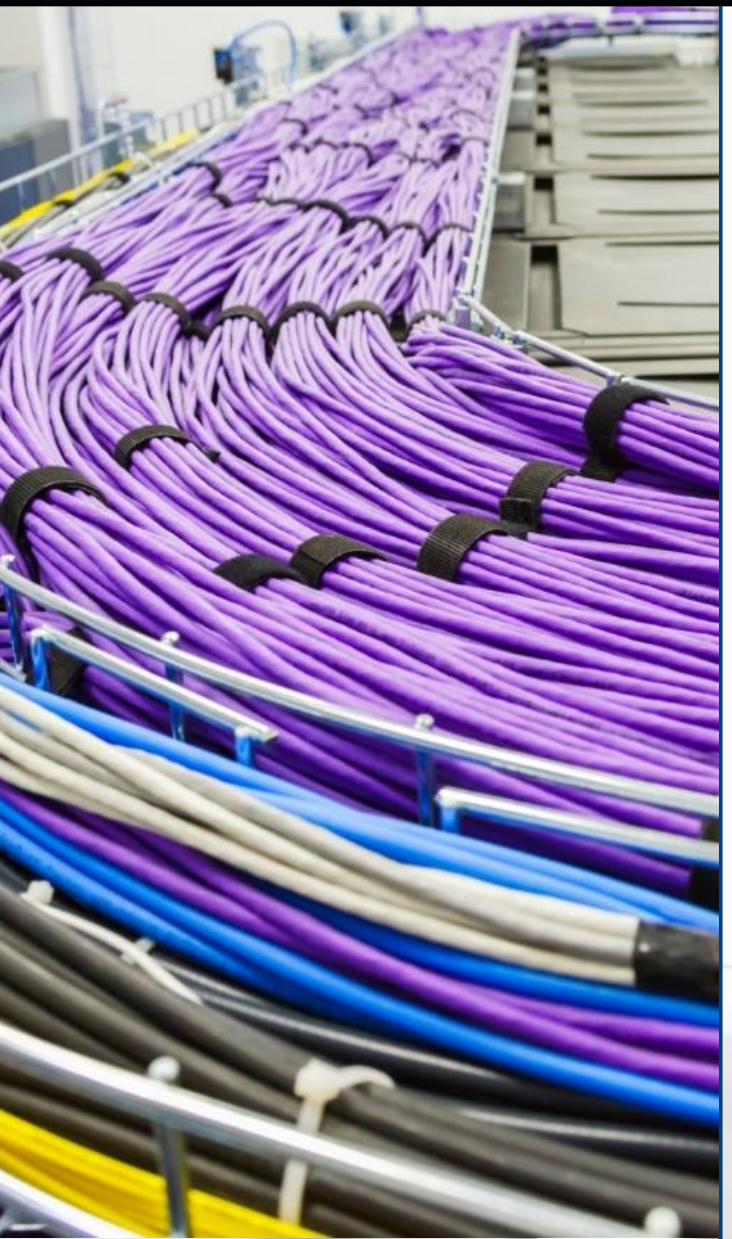
Kwetsbare platformen

Kwetsbare Netwerken



Zwakke procedures & beleid

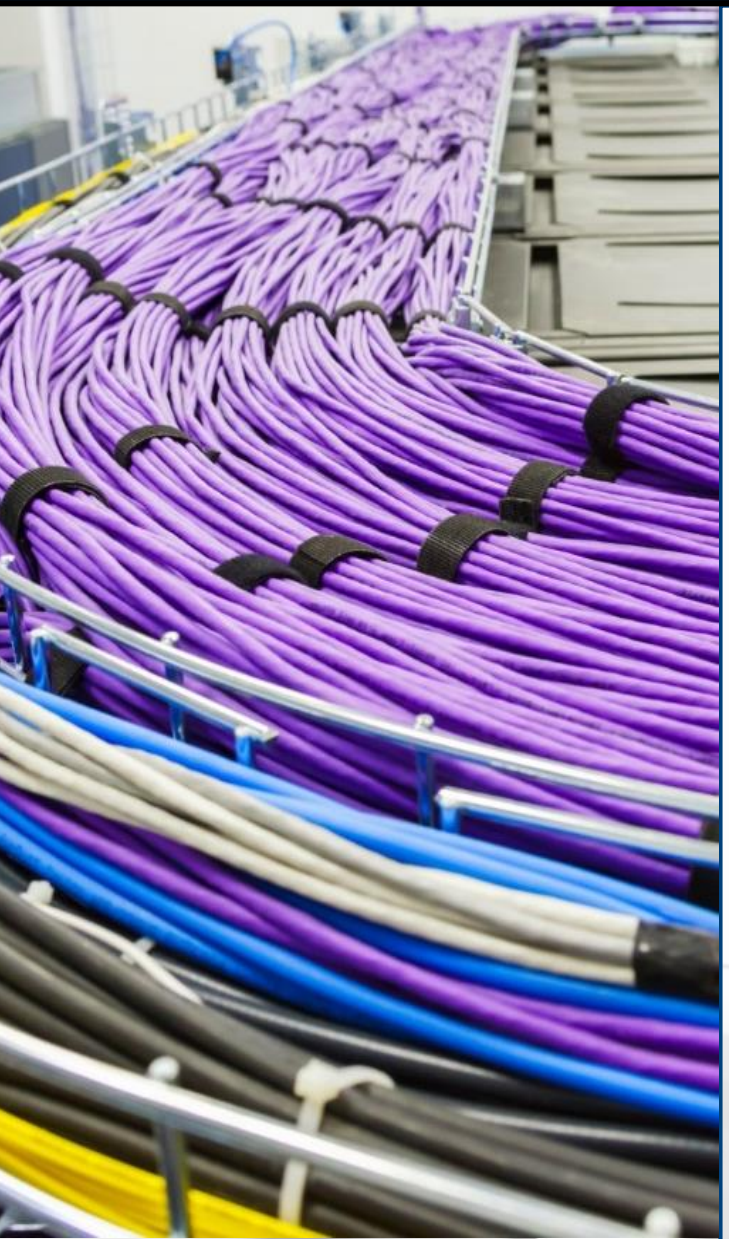
Kwetsbare Netwerken

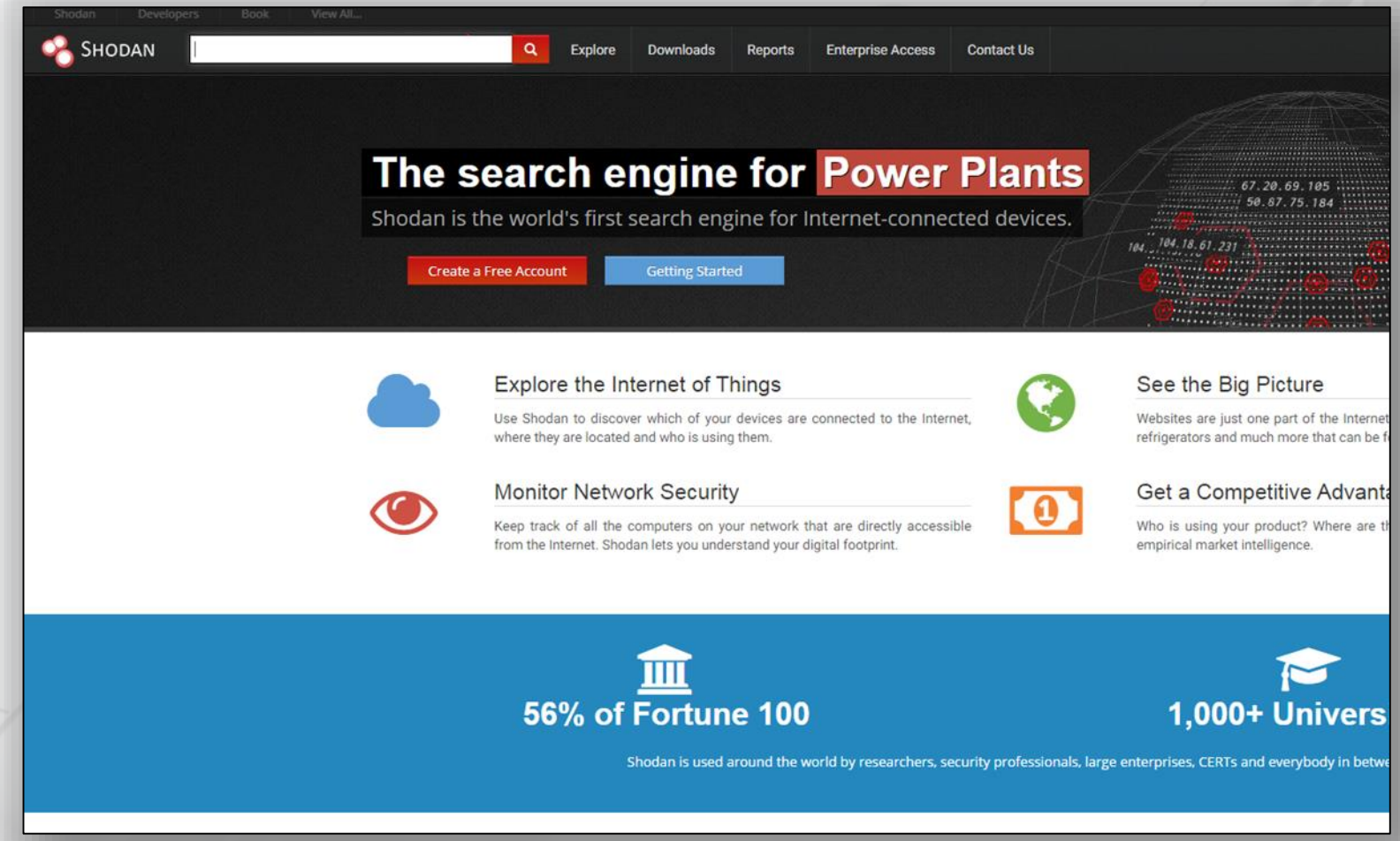


- Weinig tot geen aandacht voor security bij ontwikkeling
  - Kwetsbare Protocollen
  - Geen authenticatie
  - Geen encryptie
- Weinig aandacht voor security bij implementatie
  - Geen aangepaste netwerkarchitectuur
  - Geen security monitoring
- Onveilige toegang tot het netwerk
  - Ongedocumenteerde / tijdelijke connecties
  - Onveilige toegang van buitenaf

Kwetsbare Netwerken

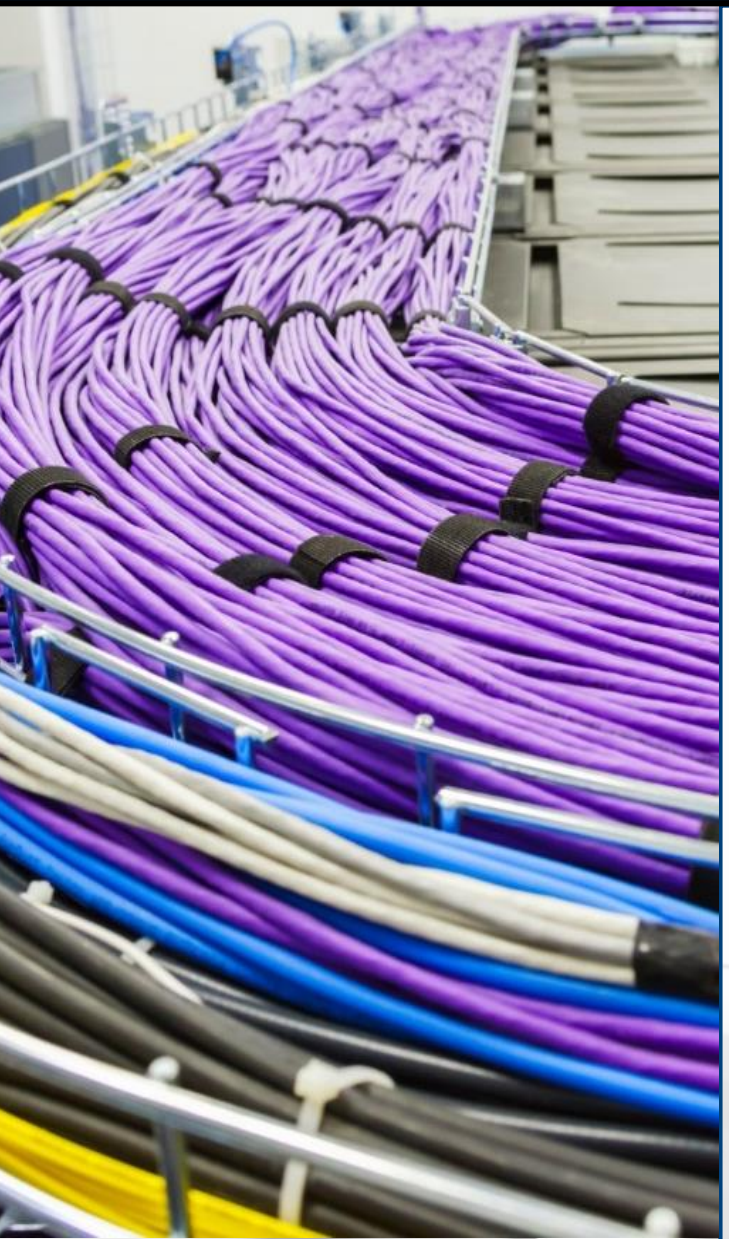
KU LEUVEN





Kwetsbare Netwerken

KU LEUVEN

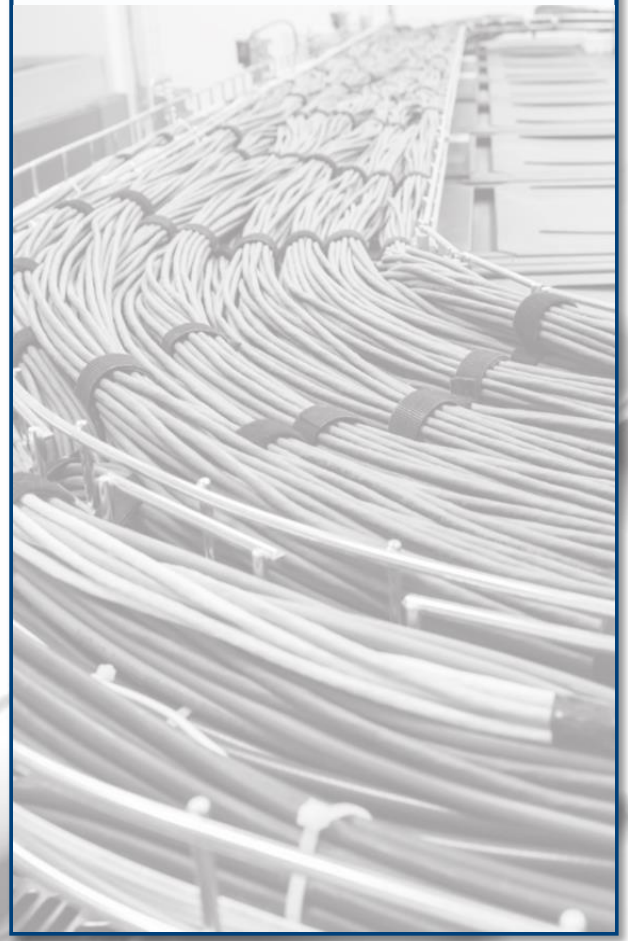


Kwetsbaarheden industriële infrastructuur

KU LEUVEN

Kwetsbare platformen

Kwetsbare Netwerken



Zwakke procedures & beleid

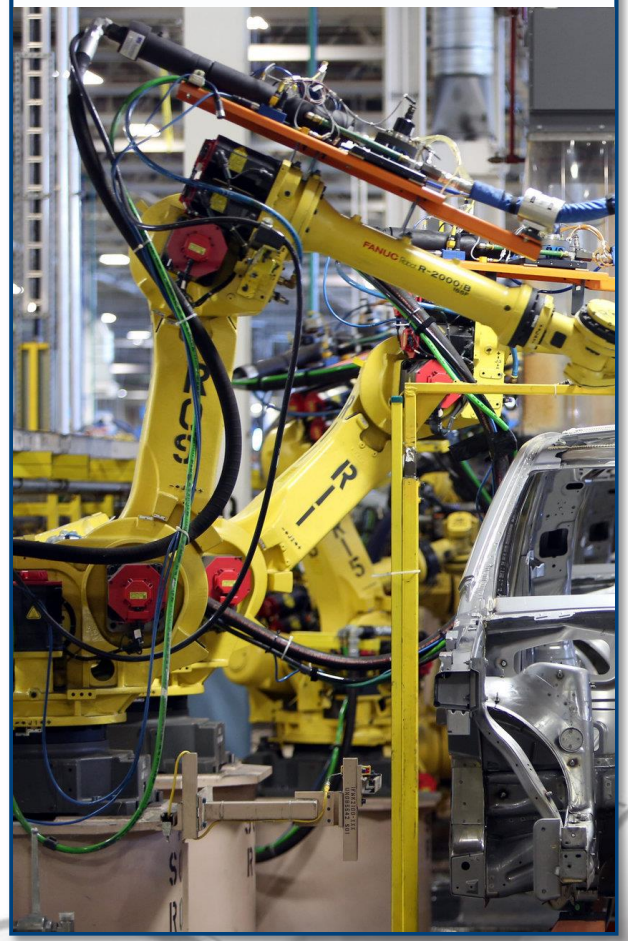
Zwakke procedures & beleid

- Geen, onvolledig of onaangepast veiligheidsbeleid
  - Gedocumenteerde ICS security beleid?
  - Administratief kader voor security?
  - Security audits voor ICS omgeving?
- Gebrek aan training en awareness
- Wat te doen bij een aanval?
  - Hoe detecteren?
  - Welke procedures voor operatoren? Wie verwittigen?
  - Disaster recovery plan?

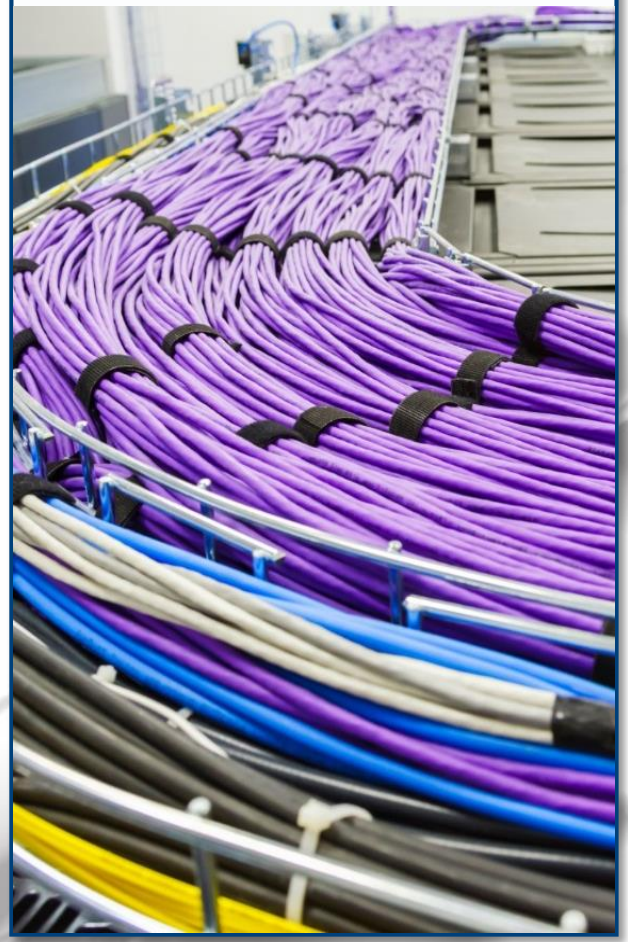
Kwetsbaarheden industriële infrastructuur

KU LEUVEN

Kwetsbare platformen



Kwetsbare Netwerken



Zwakke procedures & beleid

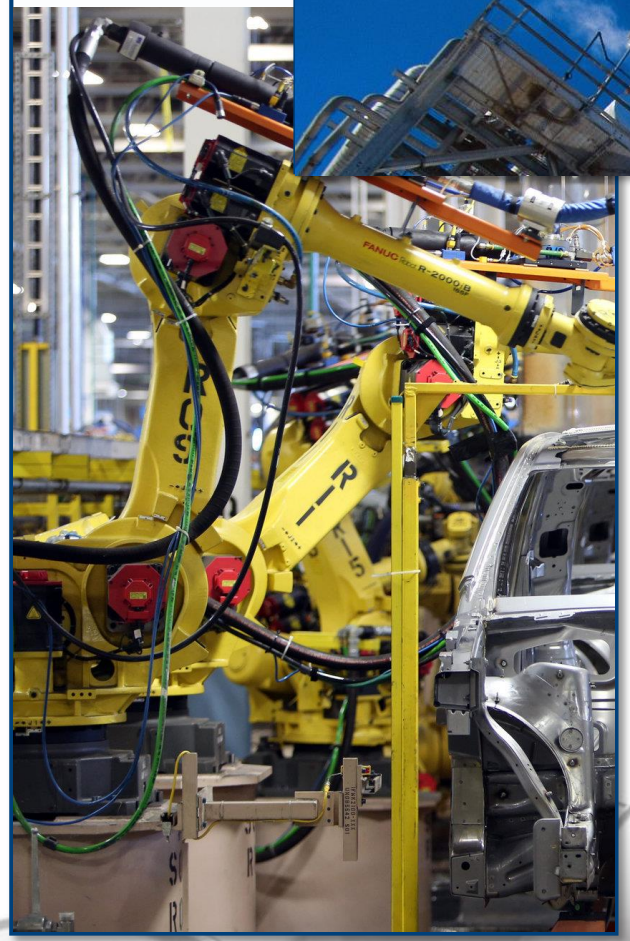
Kwetsbaarheden industriële infrastructuur

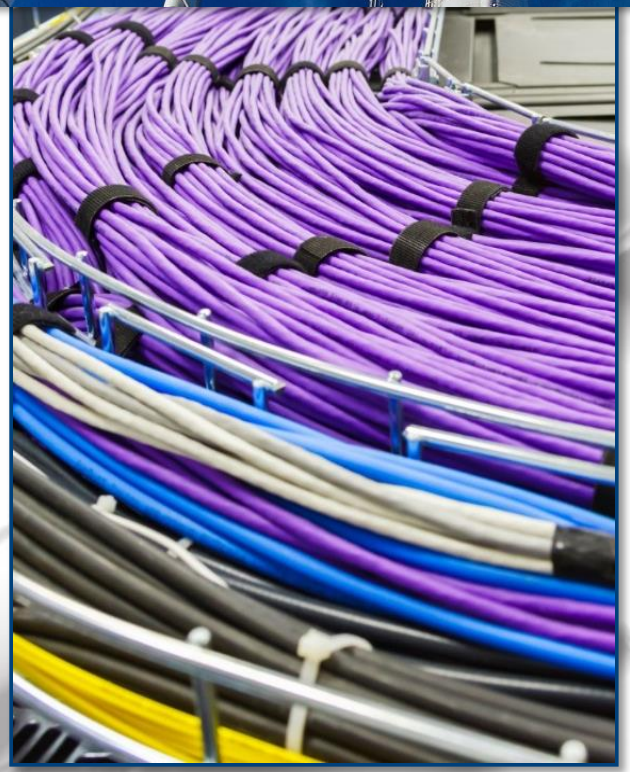
KU LEUVEN

Kwetsbare

Bijkomende Risicofactoren

es & beleid





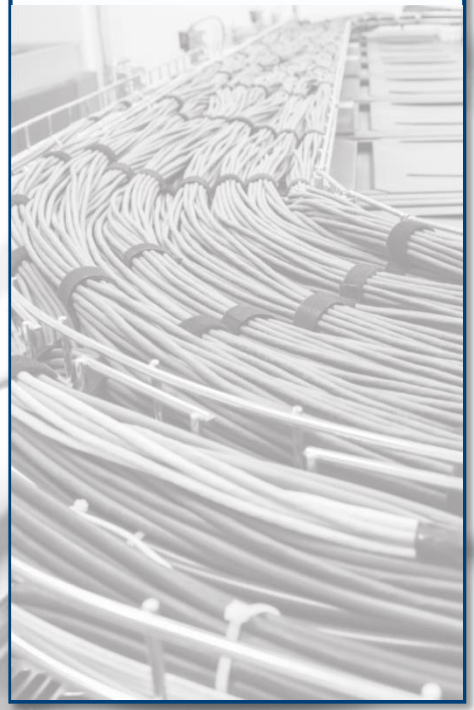
Kwetsbaarheden industriële infrastructuur

KU LEUVEN

Bijkomende Risicofactoren

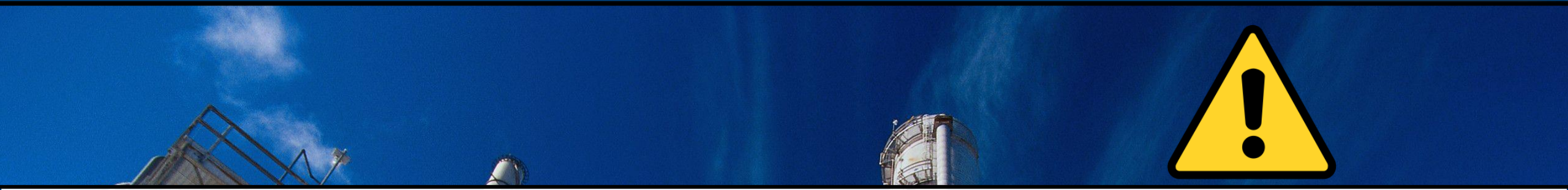
Kwetsbare platformen

Kwetsbare Netwerken



Zwakke procedures & beleid

Bijkomende risicofactoren

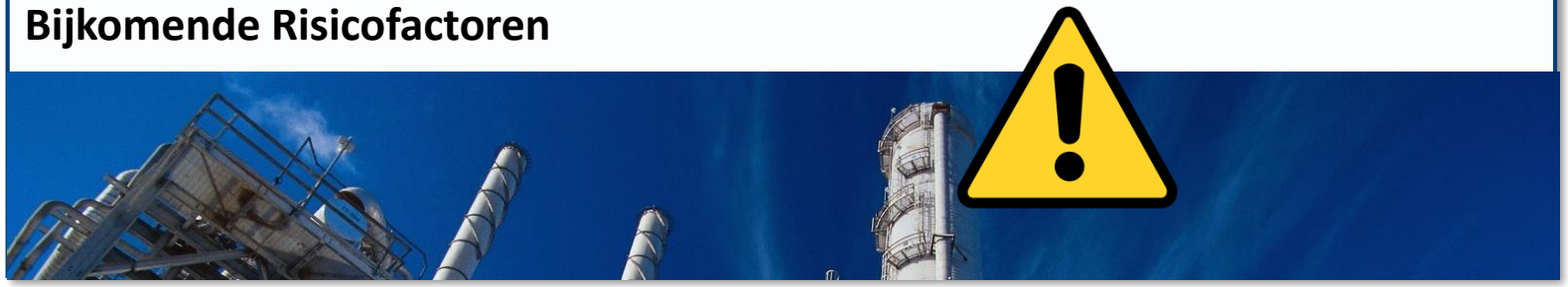


- Gestandaardiseerde protocollen en technologieën
  - Vaak met gekende Kwetsbaarheden
- Publieke informatie
- Koppeling van controlesystemen met andere netwerken
- Onveilige connecties

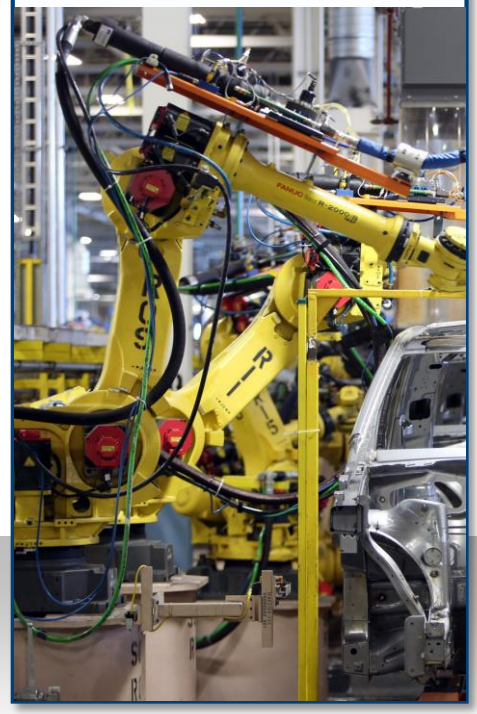
Kwetsbaarheden industriële infrastructuur

KU LEUVEN

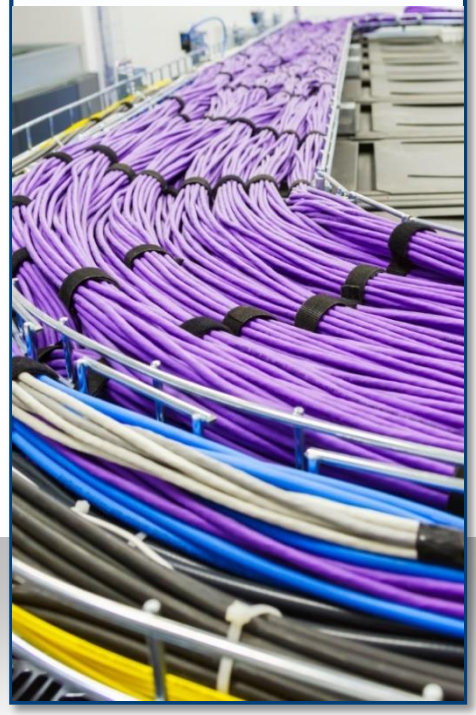
Bijkomende Risicofactoren



Kwetsbare platformen



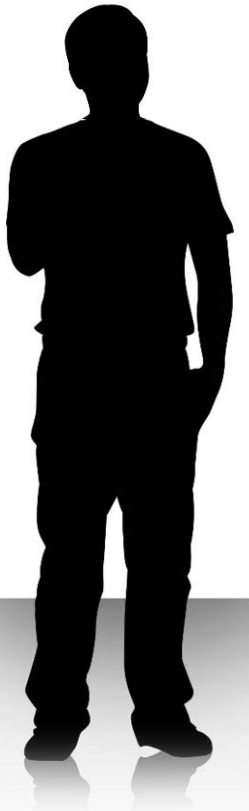
Kwetsbare Netwerken



Zwakke procedures & beleid

KU LEUVEN


HOE
KWETSBAAR
IS MIJN
INDUSTRIËLE
INFRASTRUCTUUR
VOOR
CYBERAANVALLERS?
Sleutelconcepten voor de
beveiliging van industriële
controlesystemen



Brochure

- Brochure -

Hoe kwetsbaar is mijn industriële infrastructuur voor cyberaanvallers?

Kwam tot stand door de expertise van:

- *E&A – Energie & Automatisering*
- *MSEC – DistriNet – Mobile & Secure*
- *Xiak – eXpertisecentrum industriele Automatisering Kortrijk*

In het kader van twee technologie transfer (TETRA) projecten:

- *Industriële Security (140354)*
- *Verboten - Veilig beheer en ontwerp van industriële netwerken (140318)*

KU LEUVEN

Bedankt!

Vragen?