Functional Safety Meets Cybersecurity

Nigel Stanley
Chief Technology Officer
Operational Technology and Industrial Cybersecurity
TÜV Rheinland

TÜVRheinland®
Precisely Right.

Agenda

- Modern industrial cybersecurity risk
- Functional safety and cybersecurity
- Assessing your cybersecurity risk

TÜVRheinland®
Precisely Right.

Agenda

- Modern industrial cybersecurity risk
- Functional safety and cybersecurity
- Assessing your cybersecurity risk

TÜVRheinland®
Precisely Right.

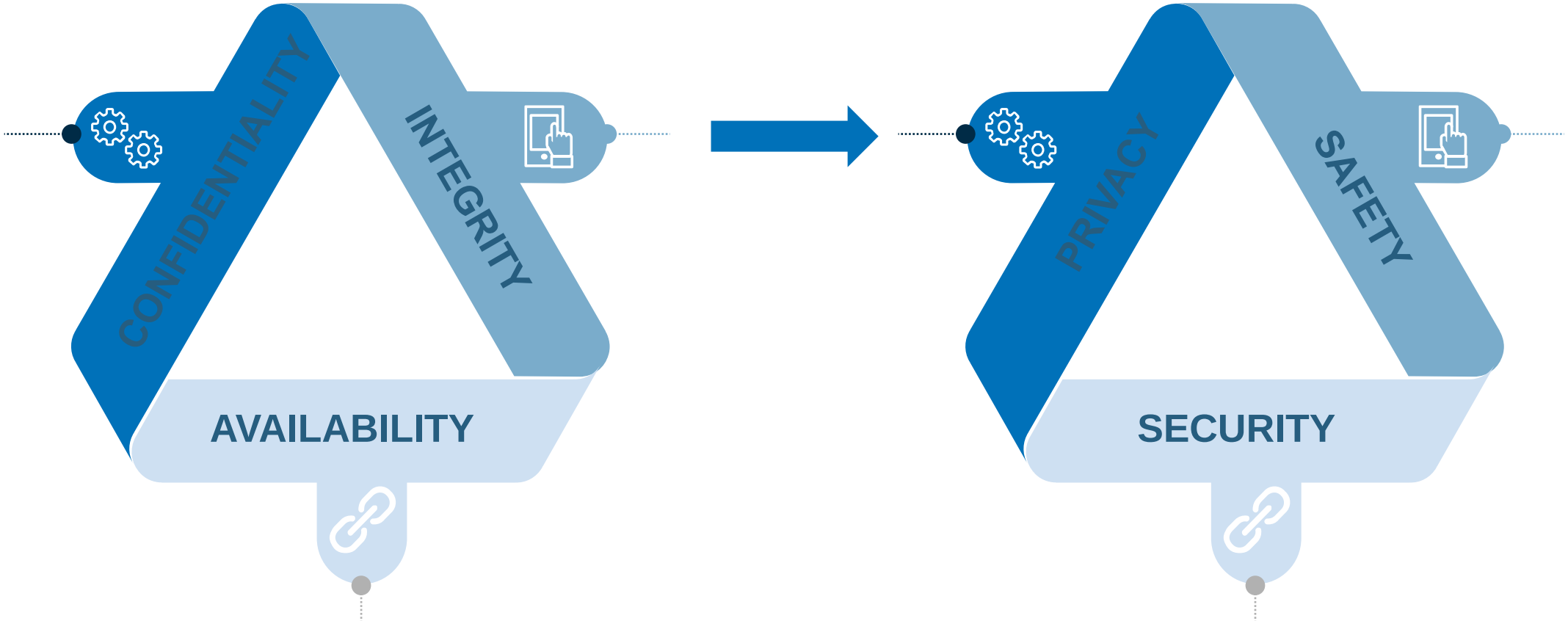
Society is hyper connected, cybersecurity risk permeates modern life

Internet of Things (IoT) = small things!

Industrial Internet of Things (IIoT)= big things!

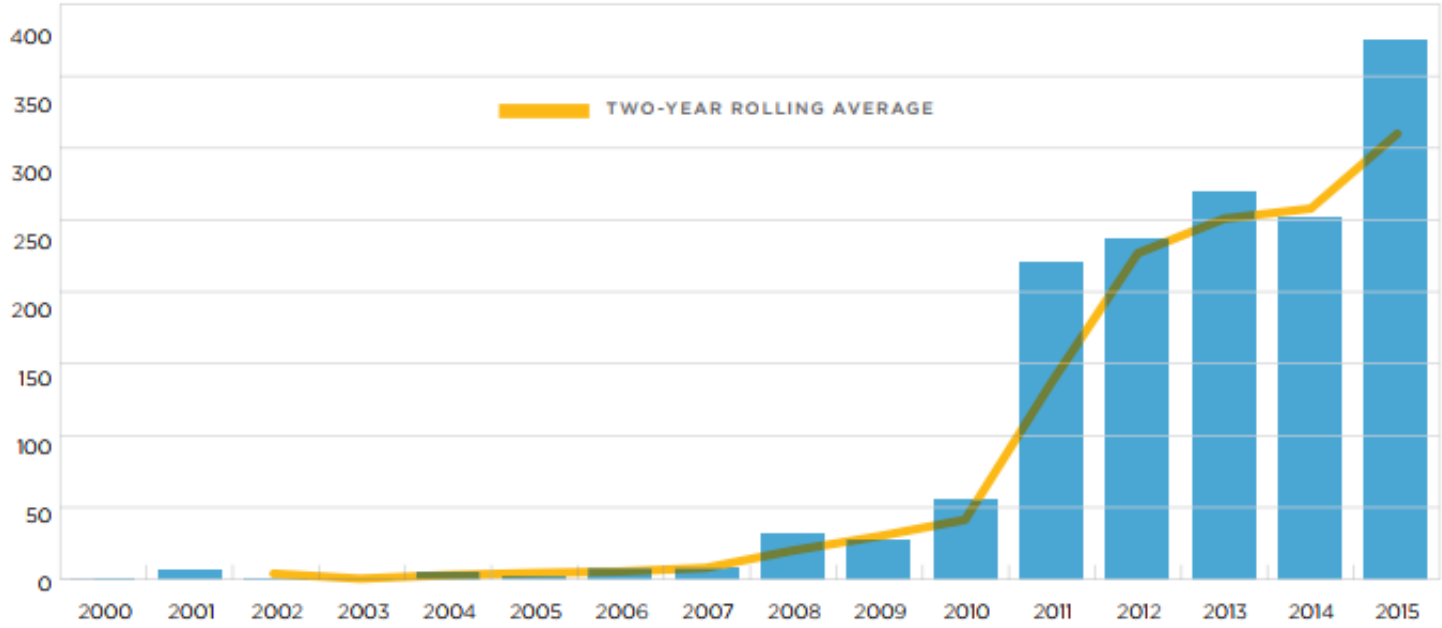
TÜVRheinland®
Precisely Right.

Information security vs operational technology cybersecurity



TÜVRheinland®
Precisely Right.

Dramatic increase in industrial control system cybersecurity vulnerability disclosures



- Nearly every ICS vendor is affected by vulnerabilities, patches are not available for all discovered issues and even if patches are available they can be difficult to apply to control systems
- Common vulnerabilities in Industrial Control Systems include buffer overflows, unauthenticated protocols, weak user authentication, poor password policies or management

Source: Fireeye

TÜVRheinland®
Precisely Right.

Potential impacts of industrial cybersecurity incidents

Injury or Fatal Accident

Financial Loss

Shareholder Confidence

Destruction of Property

Public Image

Intellectual Property Theft

TÜVRheinland®
Precisely Right.

In the news…

BBC | Your account | News | Sport | Weather | iPlayer | TV | Rad

NEWS

Home | UK | World | Business | Politics | Tech | Science | Health | Family & Education

Technology

Hack attack causes 'massive damage' at steel works

22 December 2014 | Technology

Share

The hack attack led to failures in plant equipment and forced the fast shut down of a furnace

c|net

REVIEWS | NEWS | VIDEO | HOW TO | SMART HOME | CARS | DEALS | DOWNLOAD

SECURITY

Researchers find factory robots can be easily hacked

As the world's factories shift to automation, a series of tests finds some troubling flaws.

BY ALFRED NG / MAY 3, 2017 12:10 PM PDT

M News ▸ World news ▸ NHS cyber attack

Renault stops production at several plants after ransomware cyber attack as Nissan also hacked

Scores of countries have been affected by the so-called ransomware hack, which has infected computers around the world in a number of industries

c|net

REVIEWS | NEWS | VIDEO | HOW TO | SMART HOME | CARS | DEALS | DOWNLOAD

SECURITY

Cadbury chocolate factory shut down by Petya cyberattack

The massive ransomware attack reaches Australia, sending things really wonky at the chocolate factory. Ahhhhh, fudge.

BY CLAIRE REILLY / JUNE 27, 2017 10:31 PM PDT

TÜVRheinland®
Precisely Right.

…and there‘s more

TECH | CYBERSECURITY

Hackers are holding San Francisco's light-ra system for ransom

'You Hacked, ALL Data Encrypted'

By Andrew Liptak | @AndrewLiptak | Nov 27, 2016, 4:16pm EST

PRIVACY | SECURITY

Ontario transit agency ‘extremely confident’ cyber attack came from North Korea

Howard Solomon @howarditwc

Published: January 24th, 2018

News

Cyber attack hits German train stations as hackers target Deutsche Bahn

share

An information monitor at a German train station displays the ransomware message CREDIT: @ZEICHENTATEN/TWITTER

BBC | Sign in | News | Sport | Weather | iPlayer | TV

NEWS

Home | UK | World | Business | Politics | Tech | Science | Health | Family & Education

Technology

Train-switching technology 'poses hacking threat'

8 March 2012 | Share

MIND THE HACK

Hackers ‘could hijack new digital train signalling system’ and cause MAYHEM, expert warns

Digital train signalling could be a 'risk' according to a cybersecurity expert. But Network Rail says Britain's train lines are 'safest in Europe'

By Margi Murphy

25th September 2017, 11:26 am | Updated: 25th September 2017, 11:26 am

OPINION

U.S. gov't security site hacked & TSA claimed railway suffered cyberattack

Sources: http://www.telegraph.co.uk/news/2017/05/13/cyber-attack-hits-german-train-stations-hackers-target-deutsche/
https://www.thesun.co.uk/tech/4525438/hackers-could-hijack-new-digital-train-signalling-system-and-cause-mayhem-expert-warns/
http://www.bbc.co.uk/news/technology-16347248
https://www.computerworld.com/article/2472165/endpoint-security/u-s--gov-t-security-site-hacked---tsa-claimed-railway-suffered-cyberattack.html
https://www.itworldcanada.com/article/ontario-transit-agency-extremely-confident-cyber-attack-came-from-north-korea/401047

TÜVRheinland®
Precisely Right.

Information in the open!

SHODAN

SCADAhacker.com

Home | Training | Library | Resources | Tools | Dashboard | Newsletter | Blog

Library of Resources for Industrial Control System Cyber Security

Industrial Control Systems

Spotlight

XZERES Wind Turbine

XZERES Wind designs & manufactures wind energy systems for small wind turbine market designed for powering homes farms or businesses with clean energy.

Explore

PIPS Automated License Plate Reader

The PIPS AutoPlate Secure ALPR Access Control System catalogs all vehicles entering or exiting an access point to a site or facility.

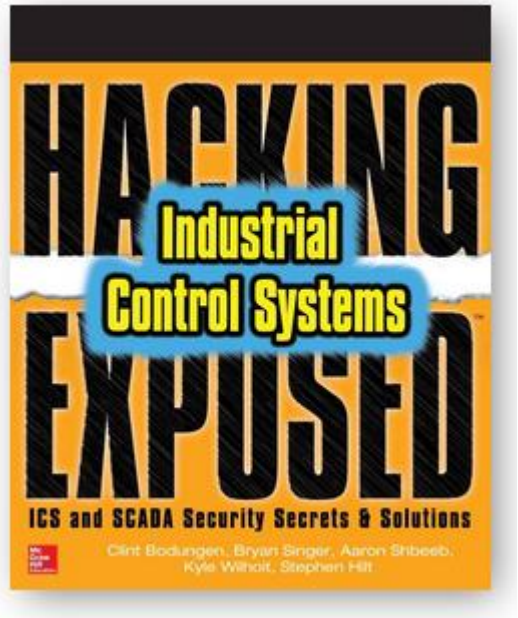
Explore

What Are They?

In a nutshell, Industrial control systems (ICS) are computers that control the world around you. They're responsible for managing the air conditioning in your office, the turbines at a power plant, the lighting at the theatre or the robots at a factory.

Common Terms

ICS	Industrial Control System
SCADA	Supervisory Control and Data Acquisition
PLC	Programmable Logic Controller
DCS	Distributed Control System
RTU	Remote Terminal Unit



Sources: https://www.shodan.io/explore/category/industrial-control-systems
https://scadahacker.com/library/
https://cyberx-labs.com/en/iiot-ics-scada-security-knowledge-base/

TÜVRheinland®
Precisely Right.

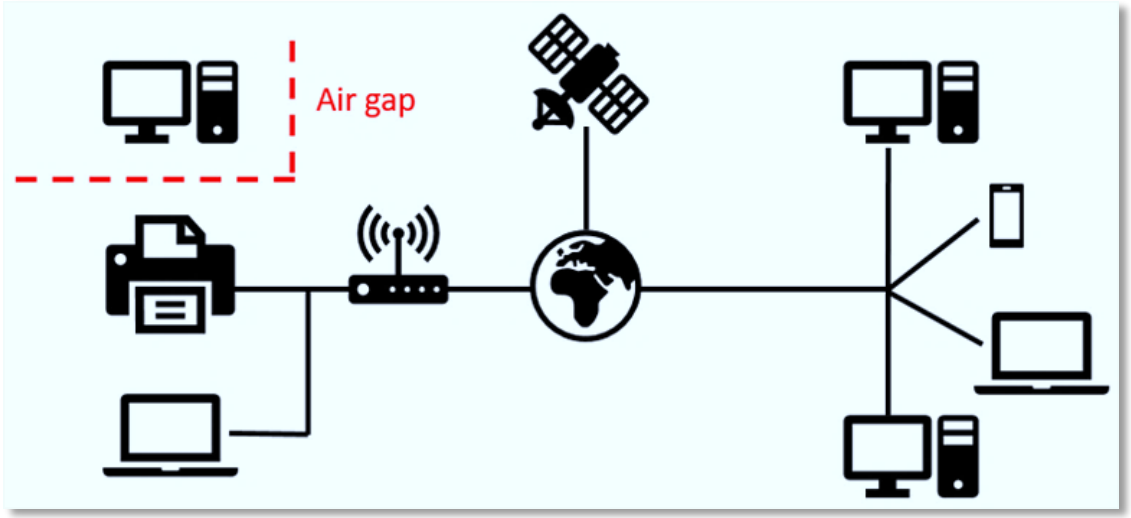
OT cybersecurity for manufacturers

Smart Factory	Attack Vector
Mobile workers and smartphone controllers	User attitudes inside/outside of the plant
Cloud systems	No perimeter security for the data
24/7 smart maintenance	Key data residing where???
Legacy systems, complex transition to new working	Reduced investment in older systems opens up a door
New capital equipment	Will want to access the internet (see above!)

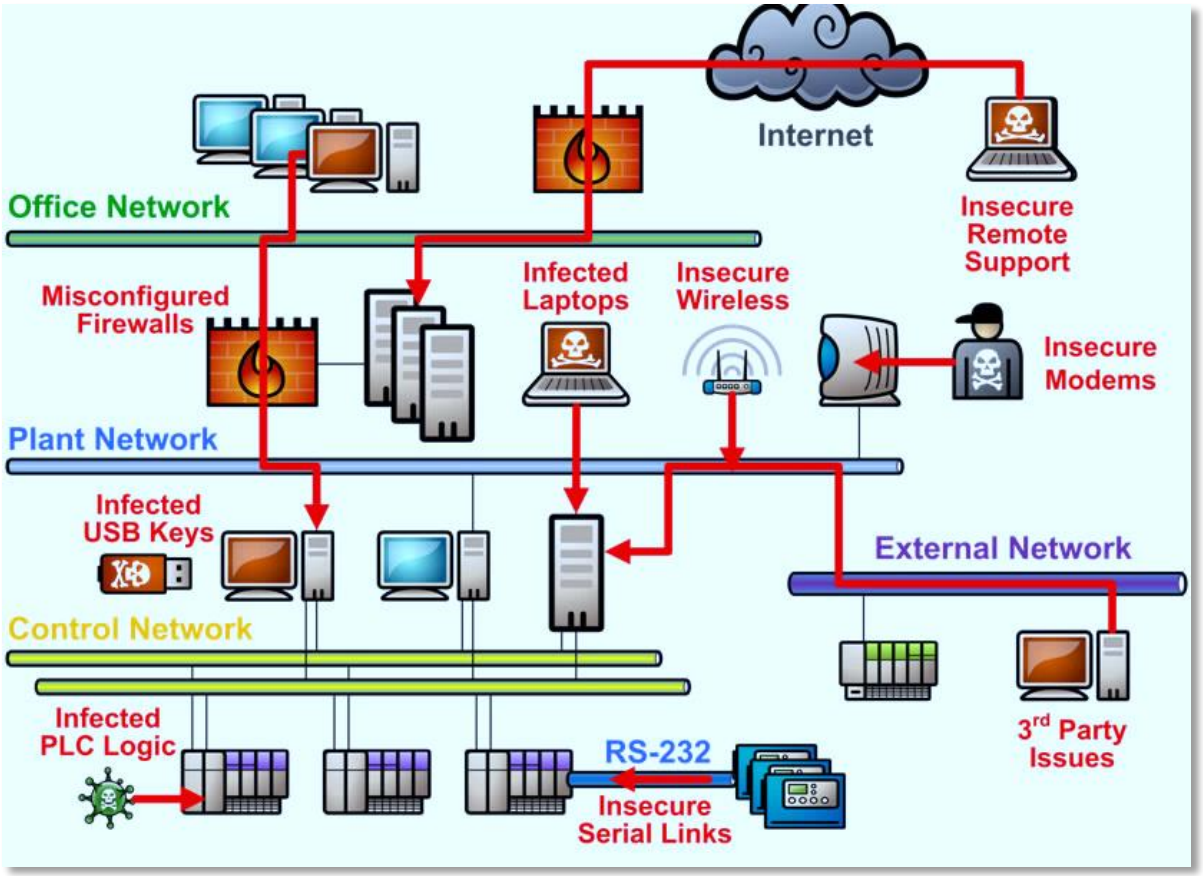
TÜVRheinland®
Precisely Right.

The myth about air gaps

IN THEORY



IN PRACTICE



TÜVRheinland®
Precisely Right.

Agenda

- Modern industrial cybersecurity risk
- Functional safety and cybersecurity
- Assessing your cybersecurity risk

TÜVRheinland®
Precisely Right.

Functional safety and cybersecurity

Cybersecurity

Defence against negligent and wilful actions to protect devices and facilities

Functional Safety

Defence against random and systematic technical failure to protect life and environment

TÜVRheinland®
Precisely Right.

Relationship between functional safety & cybersecurity

Generic Standard for Functional Safety: IEC 61508:2010.

7.4.2.3

If the hazard analysis identifies that malevolent or unauthorised action, constituting a security threat, as being reasonably foreseeable, **then a security threats analysis** should be carried out.

NOTE 3 For guidance on security risks analysis, **see IEC 62443** series.

7.5.2.2

If security threats have been identified, then a vulnerability analysis should be undertaken in order to specify **security requirements**.

NOTE Guidance is given in **IEC 62443** series.

TÜVRheinland®
Precisely Right.

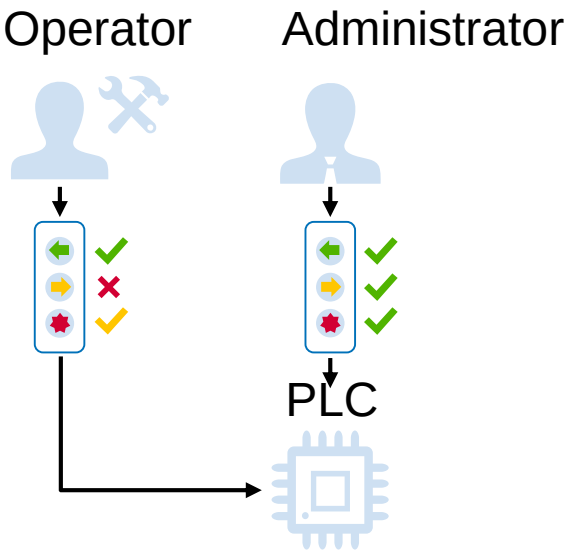
Requirements for Cybersecurity.

Foundational Requirements for Product Development according to IEC 62443.

FR 7 – Resource availability

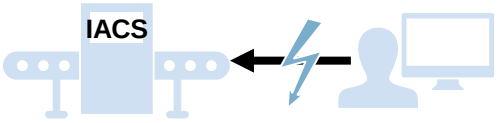
FR 1 – Identification and authentication control

FR 2 – User control



FR 6 – Timely response to events

FR 5 – Restricted data flow



FR 4 – Data Confidentiality

FR 3 – System integrity

TÜVRheinland®
Precisely Right.

Lifecycle for Functional Safety and Cybersecurity.

Functional Safety IEC 61508

Cyber Security IEC 62443

1	Concept	
2	Overall scope definition	
Hazard and risk analysis	3	Risk and Threat analysis
4	Overall safety & security requirements	
5	Overall safety & security requirements allocation	
9	Specification of E/E/PE System	
10	Realization of E/E/PES Systems	
12	Overall installation and commissioning	
13	Overall validation	
14	Overall operation, maintenance and repair	
16	Decommissioning	

→ **Safety Integrity Level (SIL) 1 – 4**

Probability of a dangerous failure in:

SIL 1	≈ 10 years
SIL 2	≈ 100 years
SIL 3	≈ 1,000 years
SIL 4	≈ 10,000 years

→ **Security Level (SL) 1 – 4**

SL 1	Protection against casual or coincidental violation
SL 2	Protection against intentional violation using simple means
SL 3	Protection against intentional violation using sophisticated means
SL 4	Protection against intentional violation using sophisticated means with extended resources

TÜVRheinland®
Precisely Right.

Triton – a seminal moment
Reported December 2017

- The attacker gained remote access to a safety instrumented system (SIS) engineering workstation and deployed the TRITON attack framework to reprogram Triconex SIS controllers
- SIS controllers entered a failed safe state
- Target – CNI but otherwise not publicly revealed (likely ME)
- Attribution – not publicly revealed (likely nation state)

Source: https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html

Agenda

- Modern industrial cybersecurity risk
- Functional safety and cybersecurity
- Assessing your cybersecurity risk

TÜVRheinland®
Precisely Right.

Risk assessments

- Manufacturers – risk assess your components (i.e. PLC) or systems
- Systems integrators – risk assess your solution to meet an operator's specifications
- Systems Operators – risk assess plant operations, factory operations, or your production facilities

TÜVRheinland®
Precisely Right.

Risk assessment approaches

NIST

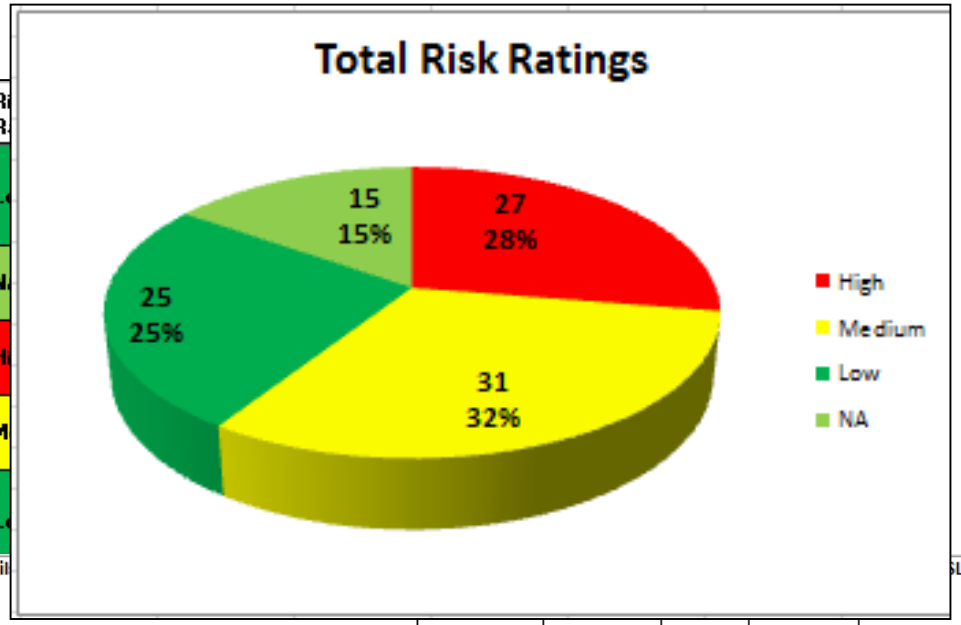
- Allows you to determine how identified risks are managed
- Will define how your organization stacks up at a high level against existing OT/cybersecurity standards, guidelines, and practices.
- Will help answer the question “How are we doing?”
- Will help you move in a more informed way to strengthen OT/cybersecurity practices

IEC 62443

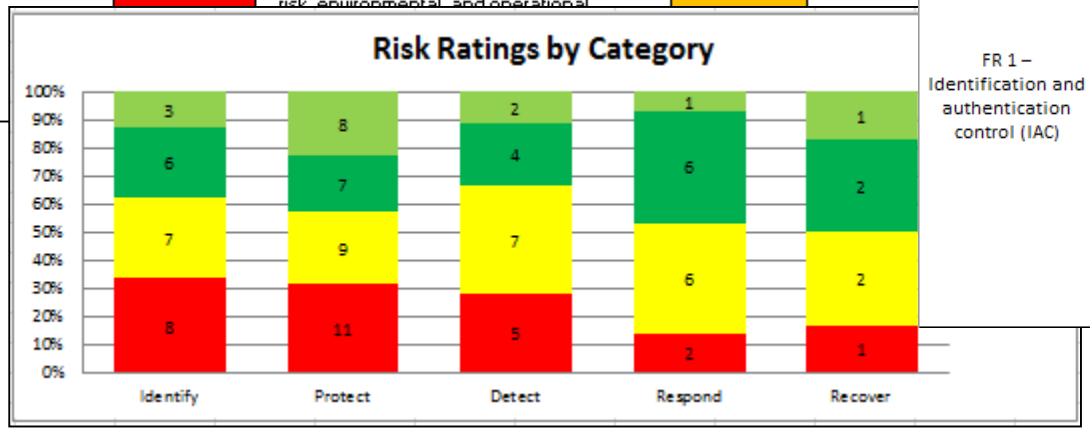
- Provides an assessment against industry standard for OT systems
- Based on 7 foundational requirements
- Can provide a security level (SL)
- Can be used by manufacturers, systems integrators or systems operators

Findings and recommendations

Function	Maturity Rating	Category	Maturity Rating	Subcategory	R
Identify	1	**Business Environment (ID.BE):** The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	3	**ID.BE-1:** The organization's role in the supply chain is identified and communicated	L
				ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	N
				ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	H
				ID.BE-4: Dependencies and critical functions for delivery of critical services are established	M
				ID.BE-5: Resilience requirements to support delivery of critical services are established	L
		Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational	2	**ID.GV-1:** policy is e	
				ID.GV-2 responsib internal ro	



Foundational Requirement	Individual Control System Requirements	Detail						Target SL Met?
FR 1 – Identification and authentication control (IAC)	SR 1.1	Human user identification and authentication	High	High	SL 2	SL 1	SL 0	No
	SR 1.1 RE 1	Unique identification and authentication	Medium	High	SL 2	SL 1	SL 1	No
	SR 1.2	Software process and device identification and authentication	High	Medium	SL 2	SL 3	SL 1	Yes
	SR 1.3	Account management	High	Low	SL 2	SL 1	SL 1	No
	SR 1.4	Identifier management	High	Medium	SL 2	SL 1	SL 1	No
	SR 1.5	Authenticator management	High	Medium	SL 2	SL 2	SL 1	Yes
	SR 1.6	Wireless access management	High	Medium	SL 2	SL 3	SL 1	Yes
	SR 1.6 RE 1	Unique identification and authentication	High	Medium	SL 2	SL 1	SL 1	No
	SR 1.7	Strength of password-based authentication	High	Medium	SL 2	SL 1	SL 2	No
	SR 1.8	Public key infrastructure certificates	High	Medium	SL 2	SL 1	SL 2	No
	SR 1.9	Strength of public key authentication	High	Medium	SL 2	SL 1	SL 2	No
	SR 1.10	Authenticator feedback	High	Medium	SL 2	SL 1	SL 2	No
	SR 1.11	Unsuccessful login attempts	High	Medium	SL 2	SL 1	SL 2	No
	SR 1.12	System use notification	High	Medium	SL 2	SL 1	SL 3	No
	SR 1.13	Access via untrusted networks	High	Medium	SL 2	SL 1	SL 1	No
	SR 1.13 RE 1	Explicit access request approval	High	Medium	SL 2	SL 1	SL 2	No



TÜVRheinland®
Precisely Right.

Next steps

- Understand your risk by conducting an assessment on your plants, factories, products or sites
- Regularly monitor new and emerging cyber risks on your OT network
- Understand how new connected systems can enhance productivity and safety if properly implemented
- Review and watch for new and emerging legislation and regulations that may impact cybersecurity in your industry – including data privacy

TÜVRheinland®
Precisely Right.

Thank you

Nigel Stanley

Chief Technology Officer

Operational Technology and Industrial Cybersecurity

TÜV Rheinland

E: nigel.stanley@us.tuv.com

TÜVRheinland®
Precisely Right.