MEGGITT

Enabling the Extraordinary
To Fly To Power To Live

CYBERSECURITY IN OT:

A PRACTICAL APPROACH TO MARKET DEMANDS

Technical Center of Excellence
Webinar

Webinar agenda

Subjects we will discuss

Cybersecurity in 2021

- Introduction
- Market trends overview
- Standards and certifications

Practical examples

- Cyber attack explained
- Cyber Assessment: what is it and how to make it?
- PenTest: all you need to know

Open discussion

- Answering questions
- Opinion exchange

CYBERSECURITY IN OT:
A PRACTICAL APPROACH
TO MARKET DEMANDS

INTRODUCTION

Cybersecurity in OT. Introduction

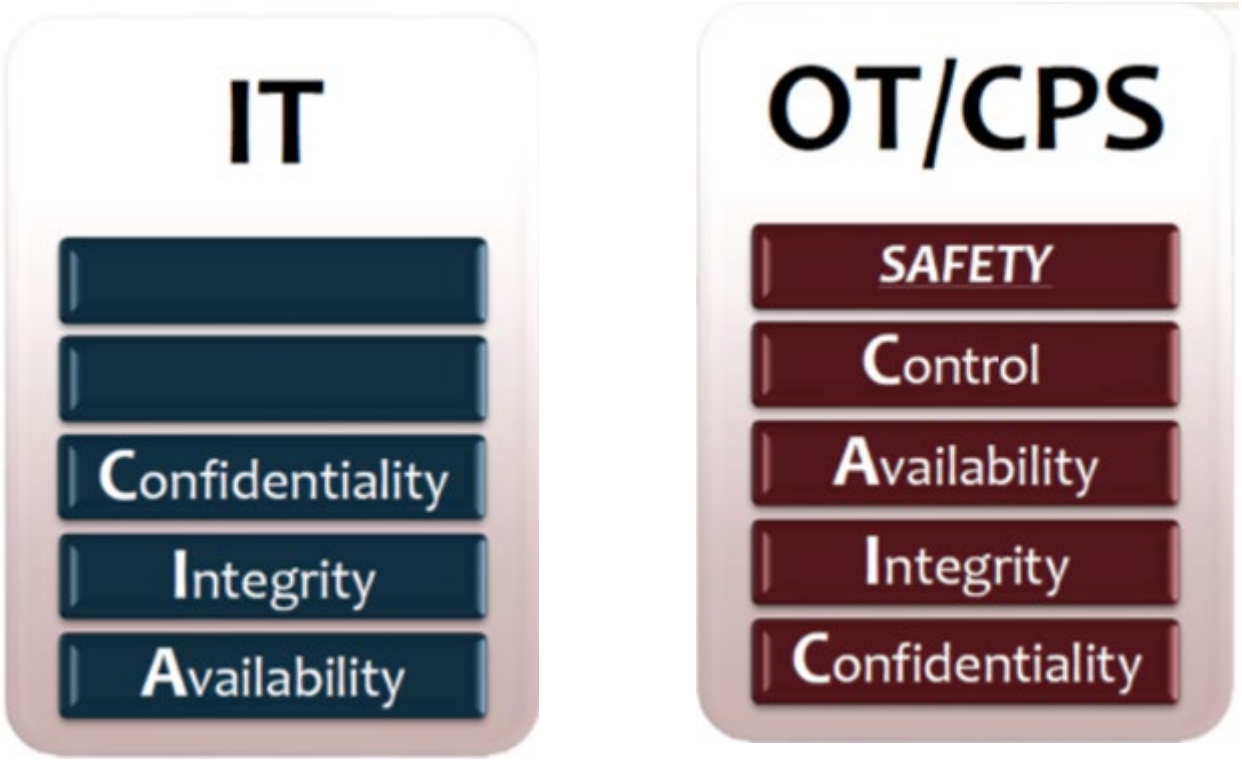
Definitions

- **IT = Information Technology**
- **OT = Operational Technology**
- **CPS =** A cyber-physical system is a computer system in which a mechanism is controlled or monitored by computer-based algorithms.
- **Cybersecurity:**
  - **In IT:** Cybersecurity is the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this.
  - **In OT:** Cybersecurity refers to the body of technologies, processes, and practices designed to protect networks, devices, processes, and data from attack, damage, or unauthorized access.

Cybersecurity in OT. Introduction

Importance

Why cybersecurity became so important?



MEGGiTT

Cybersecurity in OT

How do we mitigate the risk?

What's at stake?

People

Environment

Assets

Reputation

Liability

Applicable standards

- API670
- IEC-61508
- IEC-61511
- **IEC-62443 (formerly ISA99)**
- ISO/IEC-27001
- ISO-13849-1
- EN62061
- ISA84

MEGGiTT

CYBERSECURITY IN OT:
A PRACTICAL APPROACH
TO MARKET DEMANDS

2021 MARKET OVERVIEW

2021 Market situation

Summary

- We observe the exponential growth in requests related to cybersecurity.
- All major players in Energy market are requiring the cybersecurity compliance from suppliers.
- Market standardization: 90% of projects are using their own cybersecurity standards
  - To remove irrelevant parts
  - To be able to harden/soften some requirements according to their vision
  - No suitable products/solutions are compliant with global standards
- Customer-specific cybersecurity standards:
  - 100% of relevant requirements can be translated to IEC-62443
- The next target for the market:

"Our goal is to align with the IEC62443 standard"

Meggitt response to market needs

What are we doing to keep up

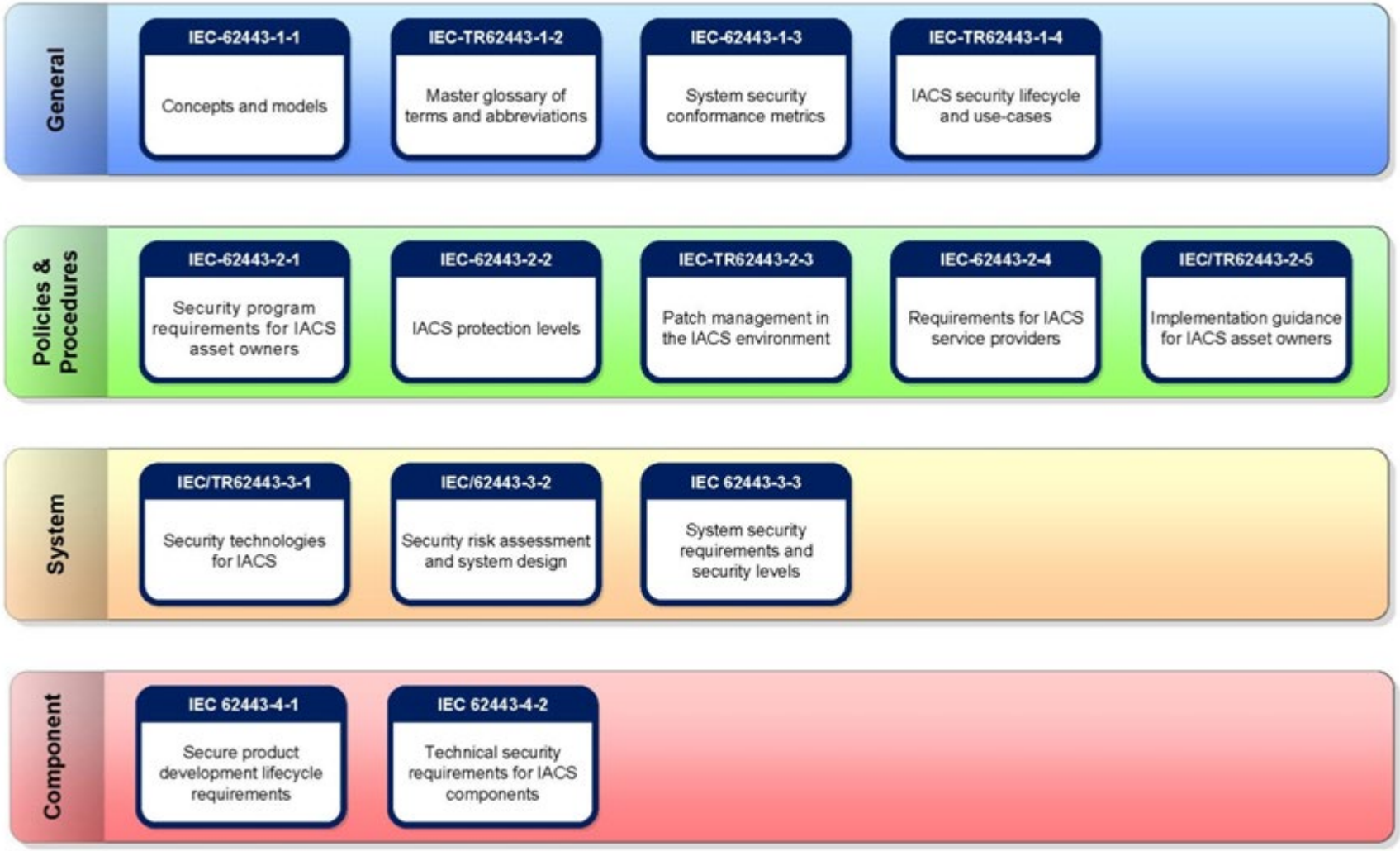
- Various audits and questionnaires (screening Meggitt as a supplier)
- Assistance in quotations - include cyber defence items and commissioning work
- Security assessments and system solutions for end-users.
- Penetration testing (Pentests) of vibro-meter® products
- Cyber security patch management
- Awareness: Online trainings and webinars
- Certification IEC-62443
  - Process certification
  - Product certification

CYBERSECURITY IN OT:
A PRACTICAL APPROACH
TO MARKET DEMANDS

IEC-62443: INTERNATIONAL INDUSTRIAL SECURITY STANDARD OVERVIEW

Cyber Security Standards Evolution

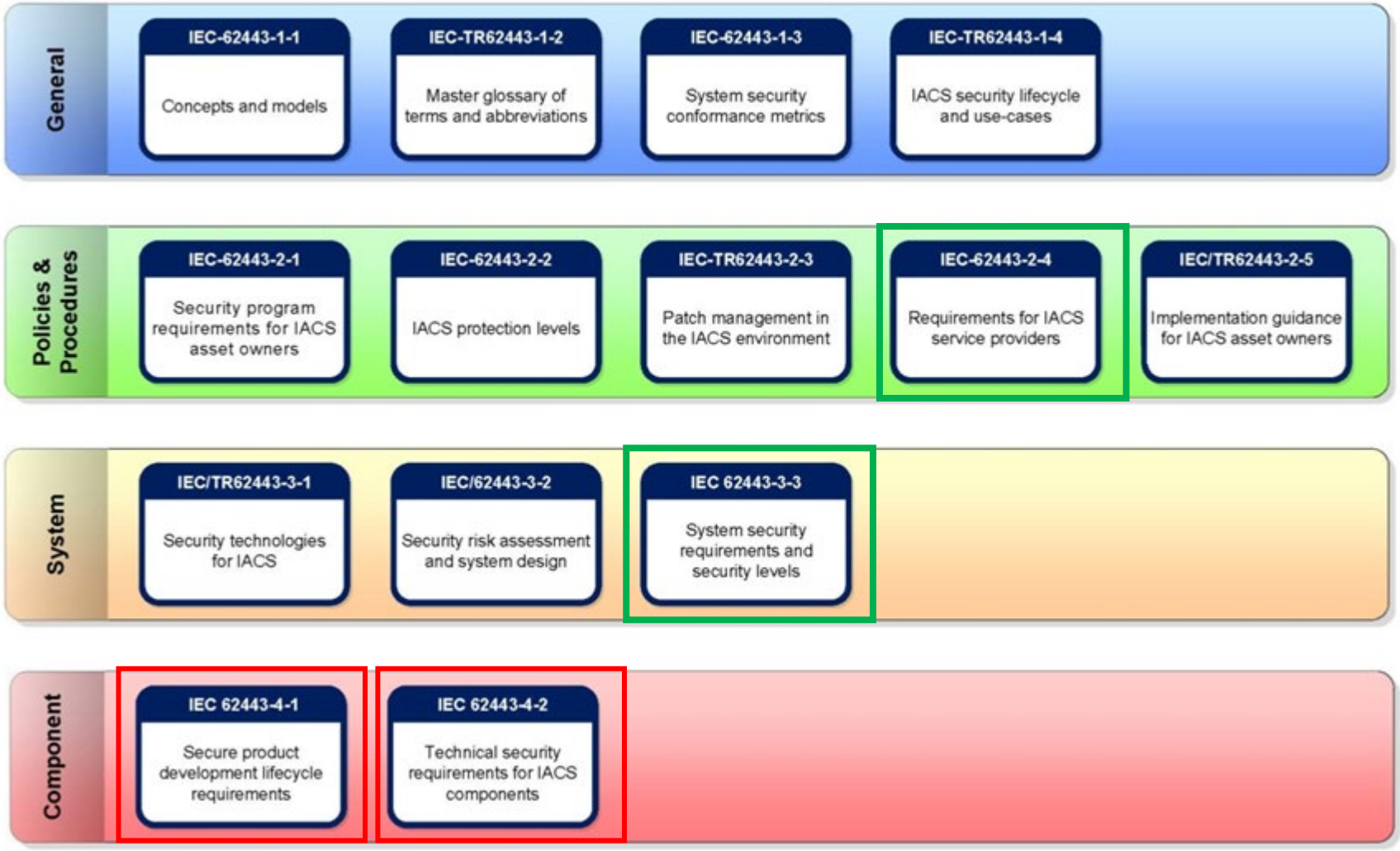
IEC 62443 leading the way



MEGGiTT

Cyber Security Standards Evolution

IEC 62443 applicable parts



MEGGiTT

IEC62443-4-2

Security Levels

Protect against…

- casual or coincidental misuse (**SL 1**)
- circumvention by entities using simple means with low resources, generic skills and low motivation (**SL 2**)
- circumvention by entities using sophisticated means with moderate resources, IACS specific skills and moderate motivation (**SL 3**)
- circumvention by entities using sophisticated means with extended resources, IACS specific skills and high motivation (**SL 4**)

Level	Methods	Resources	Skills	Motivation
1	Casual	None	None	None
2	Simple	Low	Generic	Low
3	Sophisticated	Moderate	IACS Specific	Moderate
4	Sophisticated	Extended	IACS Specific	High

IEC62443-4-2 requirement categories (across all levels)

Each level complements to the previous one

- **Identification and authentication control**
- **Use control**
- **System integrity**
- **Data confidentiality**
- **Restricted data flow**
- **Timely response to events**
- **Resource availability**

MEGGiTT

Benefits and value of complying to IEC62443?

Why go through all the hassle?

For Meggitt (Component supplier)

- Avoiding re-inventing the wheel – necessary features and techniques are well defined and explained.
- It differentiates our solutions on the market
  - Soon will become a "must have"
- Well-defined robust process ensures that our products are secure over their lifetime
- Reduce the likelihood of cyber-incidents leading to company liabilities

For End User (System owner)

- Simplifies procurement specification process
- End users better understand product cyber security capabilities
- Capabilities independently validated by external entity
- Confidence that security features will evolve over time

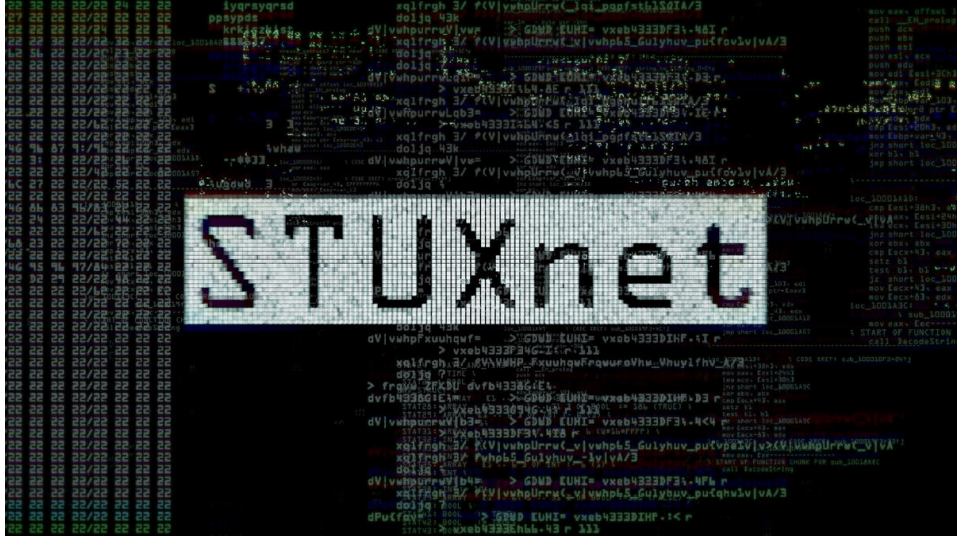
CYBERSECURITY IN OT:
A PRACTICAL APPROACH
TO MARKET DEMANDS

CYBER ATTACK LANDSCAPE

Cyber Attack Landscape

How did we get here?

- [1971] **"Creeper"**: 1st computer virus
- [1982] **"Elk Cloner"**: 1st malware to use an attack vector
- [2010] **"Stuxnet"**: 1st Cyber Physical System substantial damage
- [2016-2017] **"Petya"** - Targeted infrastructure attacks in Ukraine spreading to Europe
- [2017] **"WannaCry"**: Ransomware attack -> Global impact, including PetroChina, Iberdrola, Gas Natural, Petrobras, West Bengal State Electricity Distribution Company
- [2018] Prolific group **"Dragonfly"** conducts hundreds of small attacks on US power plants

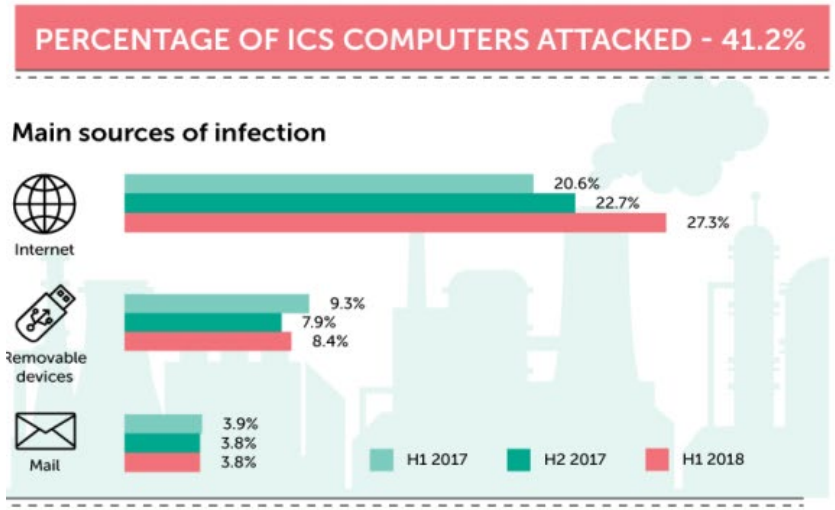


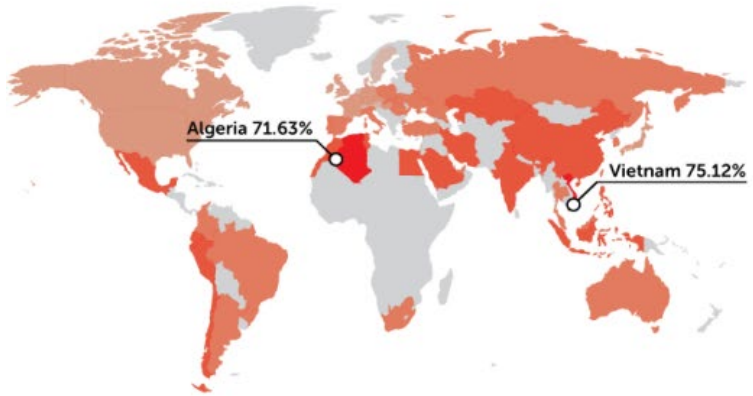
MEGGITT

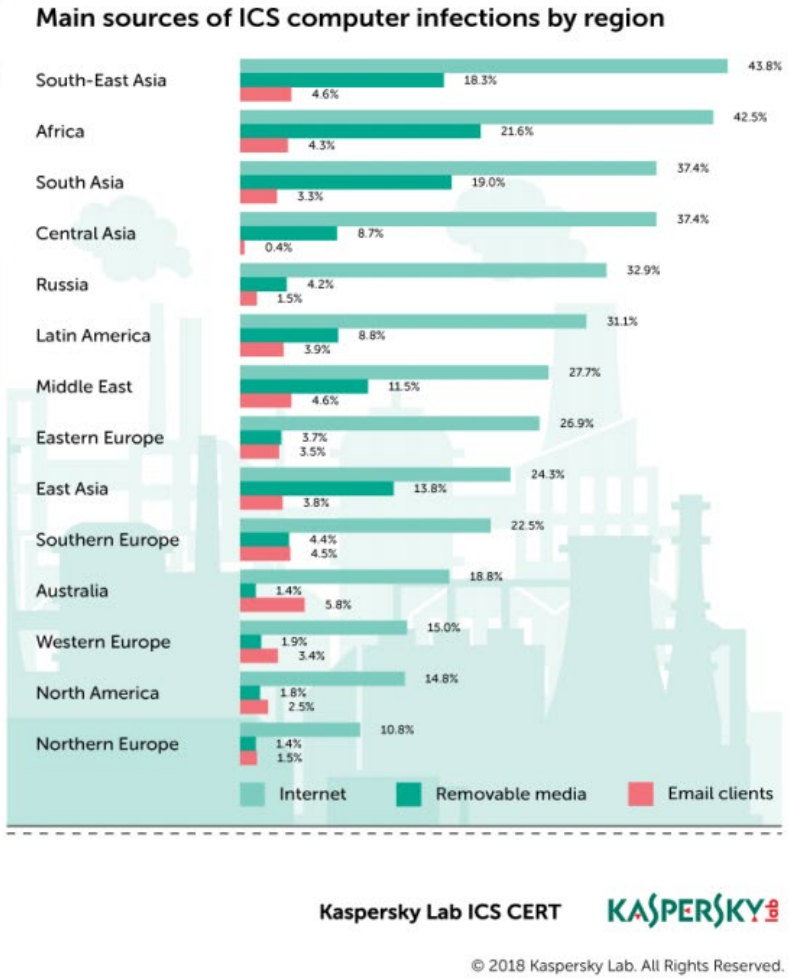
Cyber Attack Landscape

How did we get here?

2018 in numbers







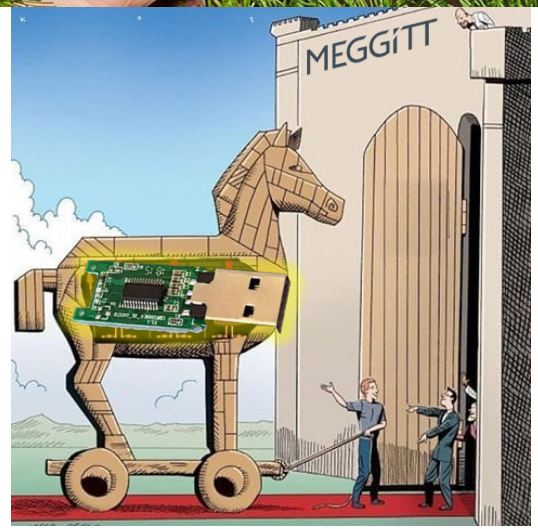
Kaspersky Lab ICS CERT KASPERSKY lab

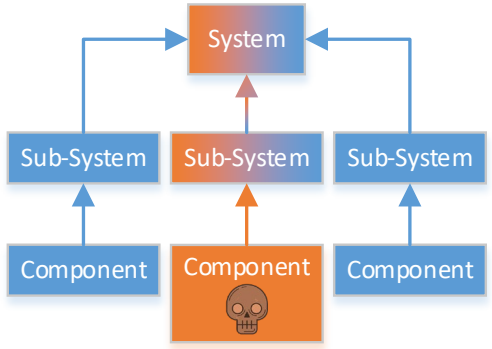
MEGGITT

Cyber Attack Landscape

Typical attack steps

- Investigation/reconnaissance/scanning
  - Determining what can be attacked
- Intrusion
  - Finding their way in
- Pivot
  - From their infected system, interfere with other systems



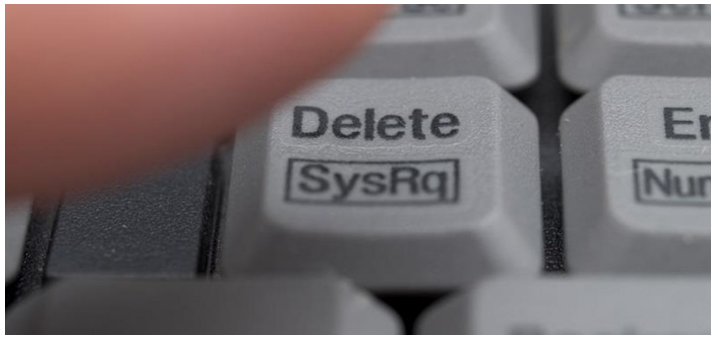


MEGGiTT

Cyber Attack Landscape

Typical attack steps

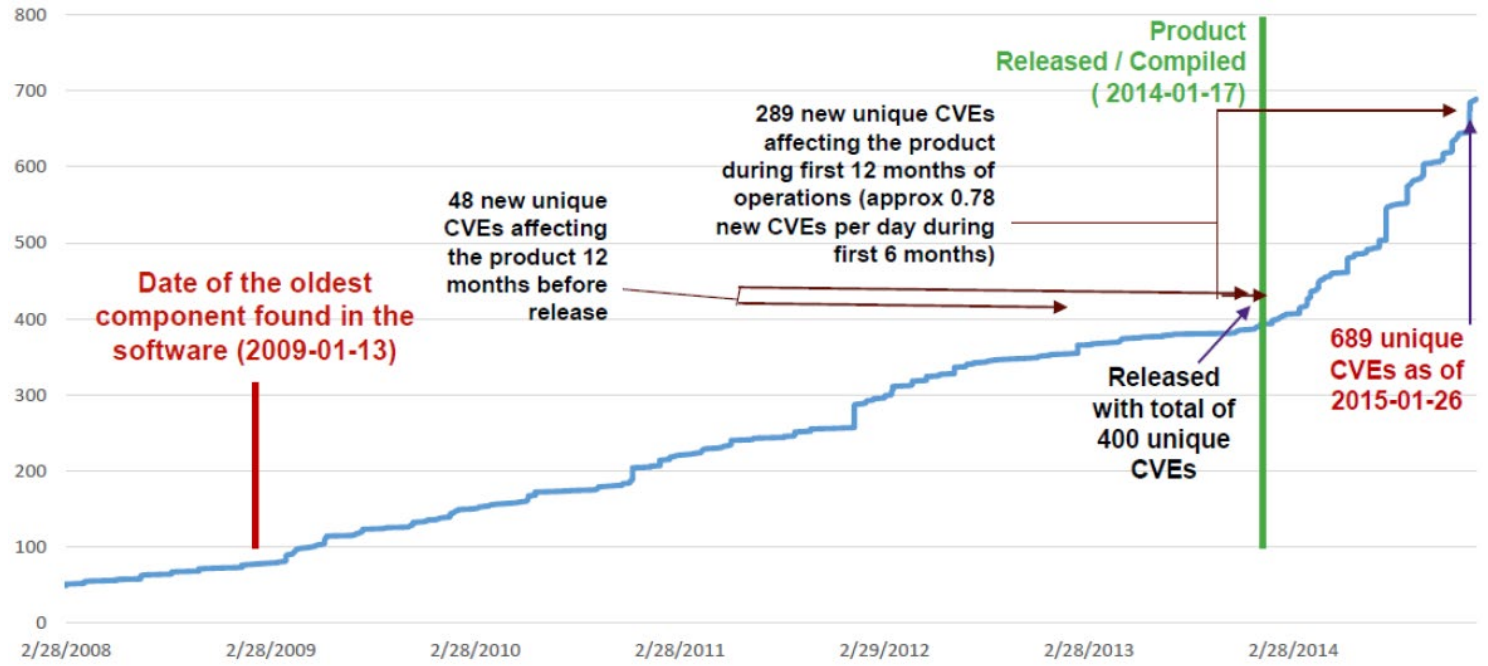
- Maintain Access
  - To continue investigation
  - To wait before sabotaging
- Exploitation – Steal/Destroy/Spy/Wait
  - The damage begins
- Covering tracks
  - Destroy logs
  - Hiding who the attacker might be
  - Making the attack completely silent



Cyber Attack Landscape - Vulnerabilities

"Time doesn't change us, it just unfolds us"

- Typical ICS product lifecycle in the decades
- It is inevitable that vulnerabilities will arise
- A Common Vulnerability and Exposure(CVE) is a term to describe a publicly disclosed vulnerability for a particular piece of software
- These are easy to discover, available in free to access databases
- CVEs can affect us via 3rd party embedded libraries, or in the main application software itself.
- Typically, once software is released, the rate of CVEs being discovered rapidly increases.



MEGGiTT

CYBERSECURITY IN OT:
A PRACTICAL APPROACH
TO MARKET DEMANDS

RISK ASSESSMENT EXAMPLE

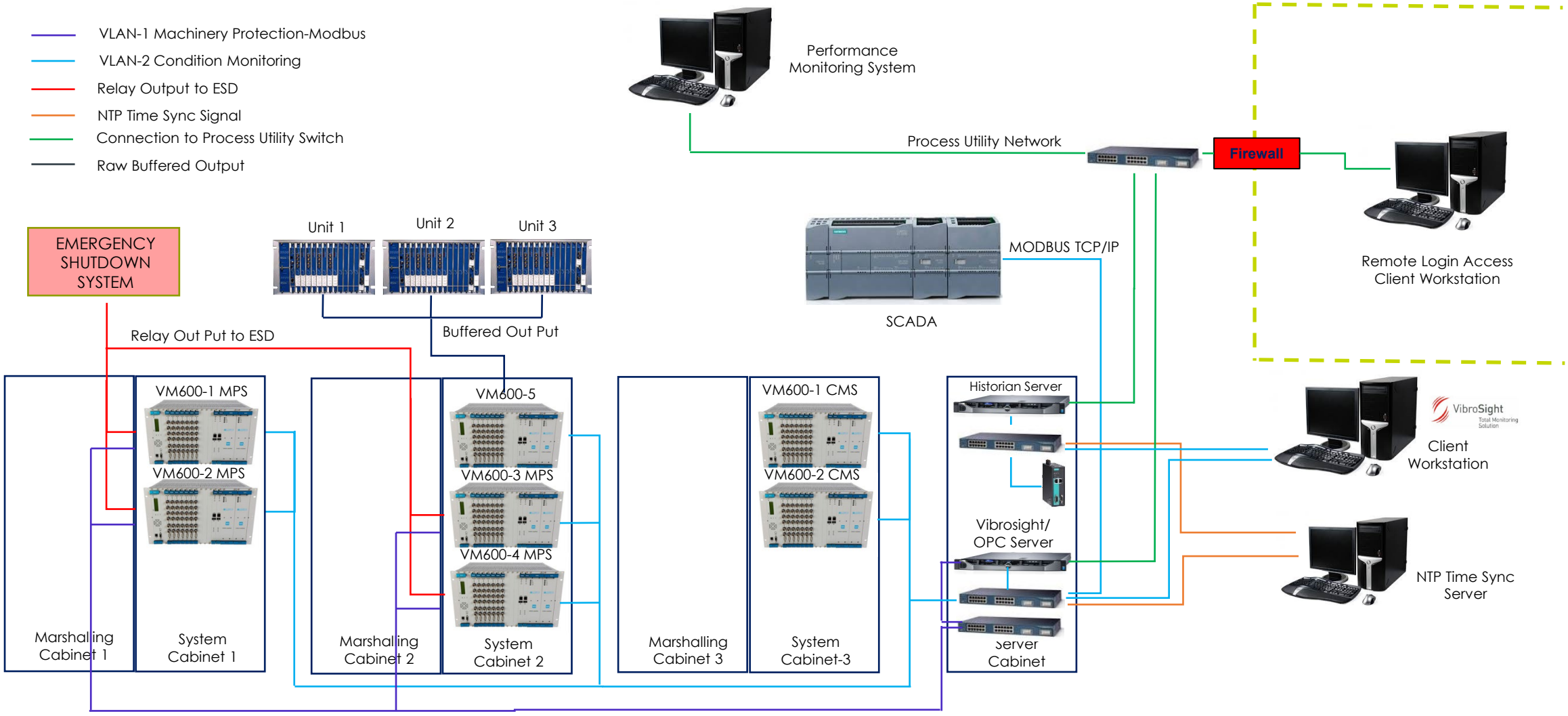
Risk assessment

Task definition

- Design and quote a Machinery Protection and Condition Monitoring system for the new project
  - 7x vm600 racks
  - Modbus, OPC, Relay outputs and signal sharing(raw buffered)
  - VibroSight: dedicated server with several clients - from local network and remotely connected
- Implement integration into customer infrastructure:
  - Split system by available cabinets
  - Implement data exchange with existing 3rd party systems
  - Implement remote access capabilities for Condition Monitoring
  - Design wiring schema for measurement signals and data transmission
- Assess overall vibro-meter subsystem security, identify risks and provide mitigations to satisfy customer requirements.

Risk assessment

Proposed System schema



Risk assessment

Asset Identification

Non-Critical Asset Role

- Used for monitoring
- Non-vital for plant operation

Requirements for this role

- Maintenance guide
- Backup/restore procedure
- Added to network documentation
- Disaster Recovery Plans developed and tested

Package Assets		
Asset Name	**Equipment Role**	**Description of Function/Purpose and Intended usage of the SYSTEM/Subsystem/Asset**
Switch	Non-Critical	Network communication/distribution devices
Modbus Gateway	Non-Critical	Gateway connected to 3rd party modules
Server	Non-Critical	Data collection & OPC Server
VM600	Both – Critical and Non-Critical	Controllers connected to 3rd party instrumentation, ESD and servers

Risk assessment

Asset Identification

Critical Assets Role

- Vital to safety or production.
- Continuous uptime

Requirements for this role

- Maintenance guide
- Backup/restore procedure
- Added to network documentation
- Disaster Recovery Plans developed and tested
- Verification/audit procedure
- Audit trail on successful and un-successful logons, config changes
- Personal user login (where applicable)
- Redundant

Package Assets		
Asset Name	**Equipment Role**	**Description of Function/Purpose and Intended usage of the SYSTEM/Subsystem/Asset**
Switch	Non-Critical	Network communication/distribution devices
Modbus Gateway	Non-Critical	Gateway connected to 3rd party modules
Server	Non-Critical	Data collection & OPC Server
VM600	Both – Critical and Non-Critical	Controllers connected to 3rd party instrumentation, ESD and servers

Risk assessment

Risk Scoring

			Production Shortfall (MAP)	<2K boe	>2K, <20K boe	>20K, <200K boe	>200K, <1M boe	>1M, <10M boe	>10M boe
	Risk Classifications & Definitions from DIR-GR-SEC-002 and DIR-GR-SEC-008		Media	Local rumour or no media consequence	Local rumour / regional press	Regional press + regional TV, national rumour	National press + national TV	International press + international TV	International press + international TV for prolonged period
			Material	<20K €	>20K, <200 €	>200K, <2M €	>2M, <10M €	>10M, <100M €	>100M €
			Environmental [1]	Minor spill with no environmental impact	Minor pollution with a very limited environmental impact	Moderate pollution with limited environmental consequences	Pollution having significant environmental consequences	Large-scale pollution of ecosystems having a recognized ecological value	Pollution having massive and durable consequences for vast ecosystems having a high ecological value
			Human	First aid or medical treatment or restricted work days	Single lost-time injury (LTI) with no disability	Single lost-time injury (LTI) with disability or multiple lost-time injuries	Internal: 1 Fatality and/or several disabilities Public: Disabilities	Internal: 2 to 5 Fatalities Public: 1 Fatality	Internal: >5 Fatalities Public: >1 Fatality
Production Shortfall (or Gain)	Human, Environmental, Material and Media			Severity of Consequence					
				Minor	Moderate	Serious	Very Serious	Catastrophic	Disastrous
				1	2	3	4	5	6
Incident almost inevitable under current conditions (or for gain) Certain fully successful modification outcome	Expected to occur several times during plant lifetime	Very Likely $> 10^{-1}$	Likelihood of Occurrence 6	6	12	18	24	30	36
Incident probable with additional factors (or for gain) High likelihood of fully successful modification outcome	Could occur several times during over plant lifetime	Likely 10^{-1} - 10^{-2}	5	5	10	15	20	25	30
Incident possible with additional factors (or for gain) Some uncertainty of successful modification outcome	Could occur once for every 10 to 20 similar plants over 20 to 30 years of plant lifetime	Unlikely 10^{-2} - 10^{-3}	4	4	8	12	16	20	24
Combination of rare factors required to cause an incident (or for gain) High uncertainty of successful modification outcome	One time per year for at least 1000 units. One time for every 100 to 200 similar plants in the world over 20 to 30 years of plant lifetime. Has already occurred in the company but corrective action has been taken	Very Unlikely 10^{-3} - 10^{-4}	3	3	6	9	12	15	18
Freak combination of factors required to cause an incident	Has already occurred in the industry but corrective action has been taken	Extremely Unlikely 10^{-4} - 10^{-5}	2	2	4	6	8	10	12
No similar incident in industry	Event physically possible but has never or seldom occurred over a period of 20 à 30 years for a large amount of sites (> few thousands, ex: wagons, process drums,...)	Remote $< 10^{-5}$	1	1	2	3	4	5	6

Risk Level 1

Risk Level 2

Risk Level 3

Major Consequence

[1] For more details on environmental definitions, refer to the Guidance for Environmental Classification (CR EP HSE 102)

Definitions:

- Risk Level 3: Broadly acceptable risk level
- Risk Level 2: Tolerable risk level if demonstrated to be ALARP
- Risk Level 1: First Priority, risk level to be obligatorily reduced to Level 2 or 3

MEGGiTT

Risk assessment

Example threat – OPC Server

Asset	Equipment Role	Threat	Vulnerability
OPC Server	Non-critical	Virus software propagates through network to asset	Software exploit in asset operating system or installed software

Counter Measure	Risk	Likeli hood	Severity	Score	Risk Level
None	Corruption of integrity and/or availability	5	3	15	**2**
Antivirus software installed to server Security updates Validation of installation authenticity	Corruption of integrity and/or availability	3	3	9	**3**

MEGGiTT

Risk assessment

Example threat – OPC Server

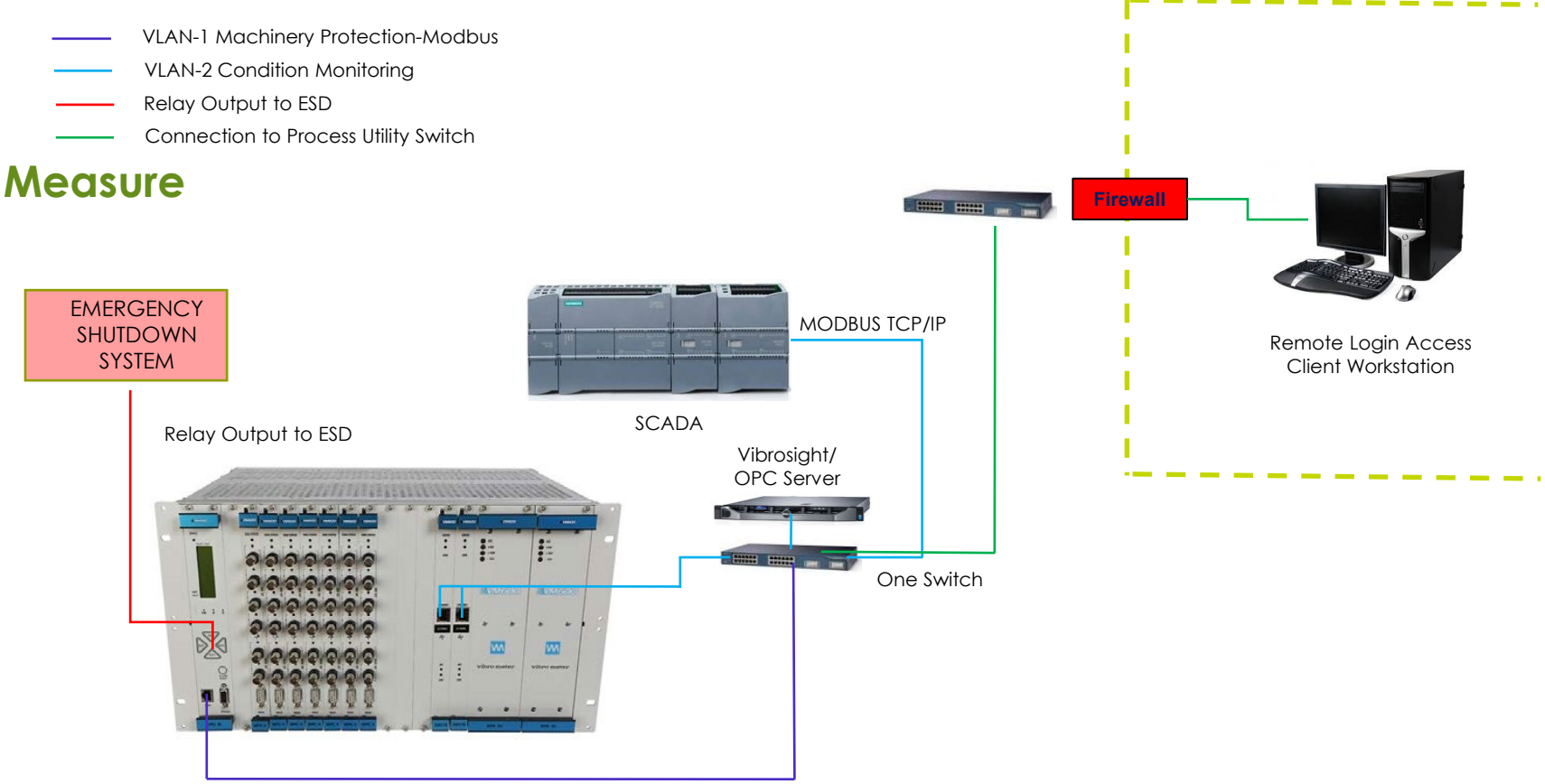
Asset	Equipment Role	Threat	Vulnerability
VM600	Critical and Non-critical	Exploitation of software installed on VM600	Latent vulnerabilities in software installed on VM600

Counter Measure	Risk	Likeli hood	Severity	Score	Risk Level
None	Corruption of integrity and/or availability	4	4	16	2

MEGGiTT

Risk assessment

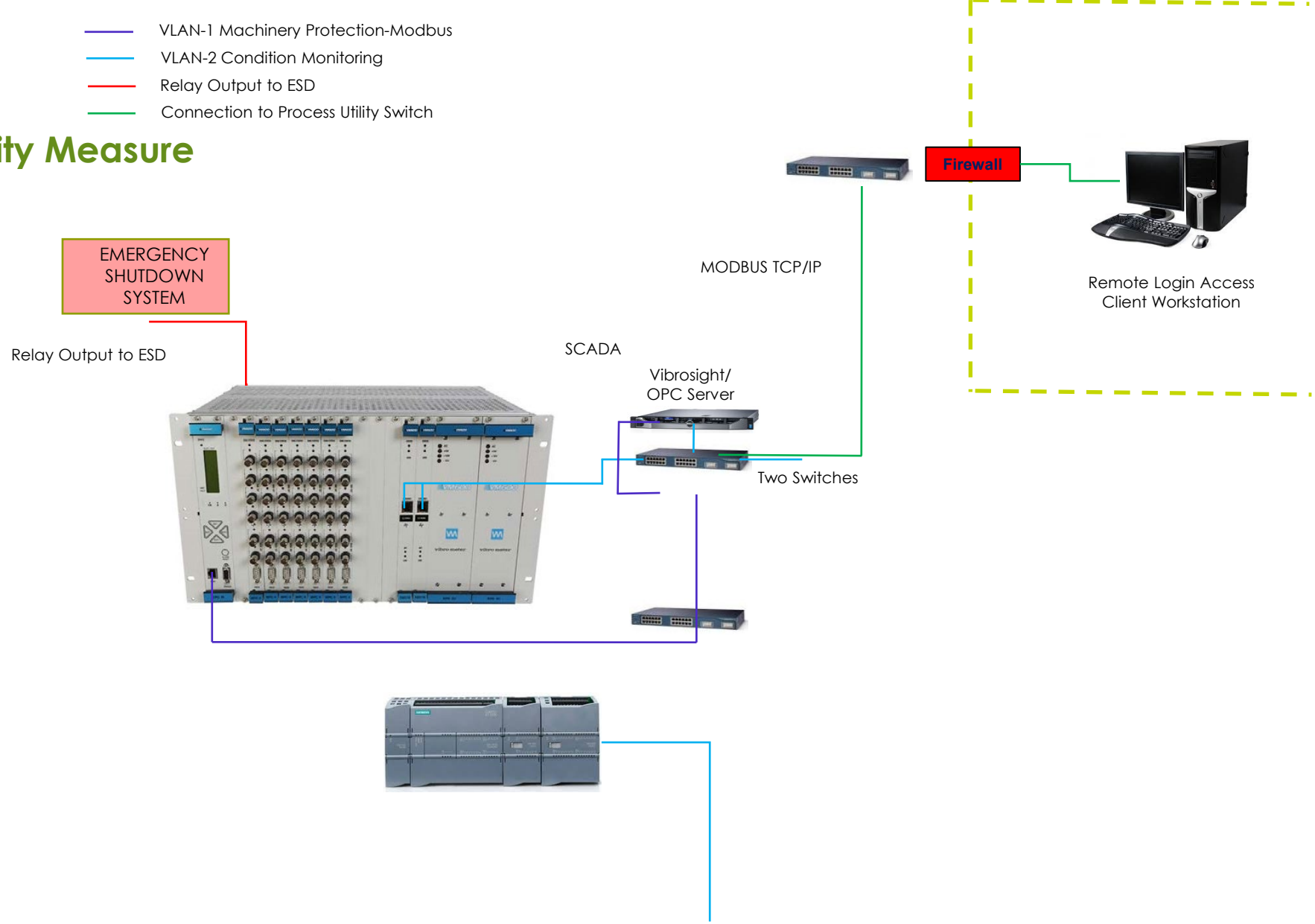
Network Segmentation Security Measure



MEGGiTT

Risk assessment

Network Segmentation Security Measure



MEGGiTT

Risk assessment

Example threat – OPC Server

Asset	Equipment Role	Threat	Vulnerability
VM600	Critical and Non-critical	Exploitation of software installed on VM600	Latent vulnerabilities in software installed on VM600

Counter Measure	Risk	Likeli hood	Severity	Score	Risk Level
None	Corruption of integrity and/or availability	4	4	16	2
Robust development process with verification testing Network segregation System hardening and commissioning checks	Corruption of integrity and/or availability	2	4	8	3

MEGGiTT

CYBERSECURITY IN OT:
A PRACTICAL APPROACH
TO MARKET DEMANDS

PEN TEST EXAMPLE

Pen Testing

What is it?

- **Port scanning**
  - Basic discovery of what systems are running
- **Vulnerability scanning**
  - Which of the systems are vulnerable? What are the weaknesses?
- **Penetration testing**
  - Lets try and exploit the vulnerabilities

MEGGiTT

Pen Testing

How does a test work? – Initial Work

- **Scope Definition**
  - What is the security goal?
  - What is the attacker trying to achieve?
  - Define what is deemed to be a successful attack

- **Reconnaissance**
  - Research phase
  - Scoping out the job
  - To save test costs, this can be directly shared with the testers

Pen Testing

How does a test work? – Discovery and Intrusion

- **Discovery**
  - Active scoping
  - Probing systems
  - Port scans
  - Reverse engineering

- **Intrusion**
  - Breaking into the system
  - Exploiting CVEs with prewritten software
  - Writing custom exploits
  - Brute forcing passwords
  - Social engineering

Pen Testing

How does a test work? – Finalising the test

- **Pivot**
  - Jump from the breached system to another system of interest

- **Safety Considerations**
  - Setting the ground rules
  - What types of attack can be used?
  - Is it OK to interfere with production systems?

- **Reporting**
  - Documenting what was performed, what was successful
  - Initiate remediation process

MEGGiTT

Enabling the Extraordinary
To Fly To Power To Live

Q&A

Technical Center of Excellence
Webinar

MEGGiTT

Enabling the Extraordinary
To Fly To Power To Live

THANK YOU

Cybersecurity in OT: A Practical Approach To Market demands

Presented by

Igor Karpekin,
SME IT/OT

Kevin Stanley-Adams
Security Engineer

Disclaimer

Business legal entity, Business address

Legal entity registration information as appropriate

Information contained in this document may be subject to export control regulations of the United Kingdom, European Union, United States or other national jurisdictions, including the US International Traffic in Arms Regulations and/or Export Administration Regulations.

Each recipient of this document is responsible for ensuring that transfer or use of any information contained herein complies with all relevant Export Control Regulations.

MEGGiTT