MITSUBISHI ELECTRIC
Changes for the Better

# Safeguarding your operational technology

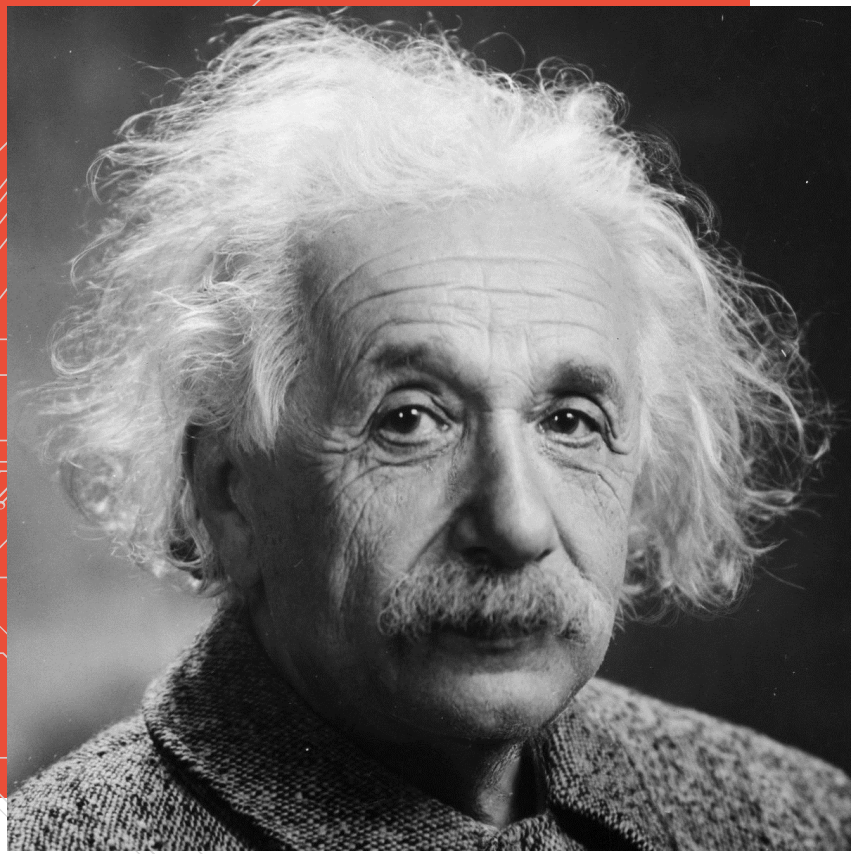
Frederik Kok
Senior Cyber Security Contributor

COPYRIGHT © 2021 MITSUBISHI ELECTRIC EUROPE B.V. ALL RIGHTS RESERVED

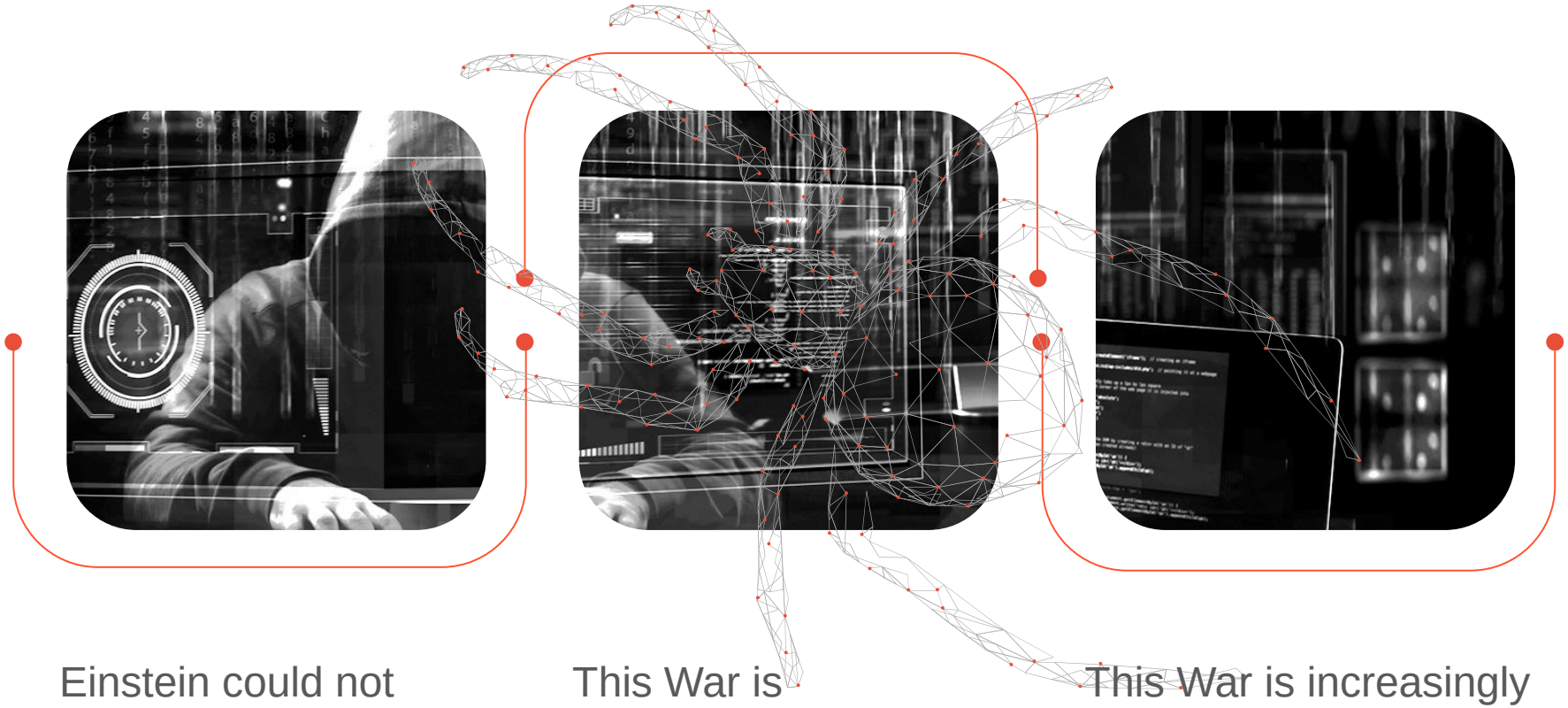
MITSUBISHI ELECTRIC
Changes for the Better

*“I know not with what weapons World War III will be fought, but World War IV will be fought with sticks and stones.”*

*Albert Einstein*



COPYRIGHT © 2021 MITSUBISHI ELECTRIC EUROPE B.V. ALL RIGHTS RESERVED. All product names, trademarks and registered trademarks are property of their respective owners



Einstein could not have foreseen a Cyber War

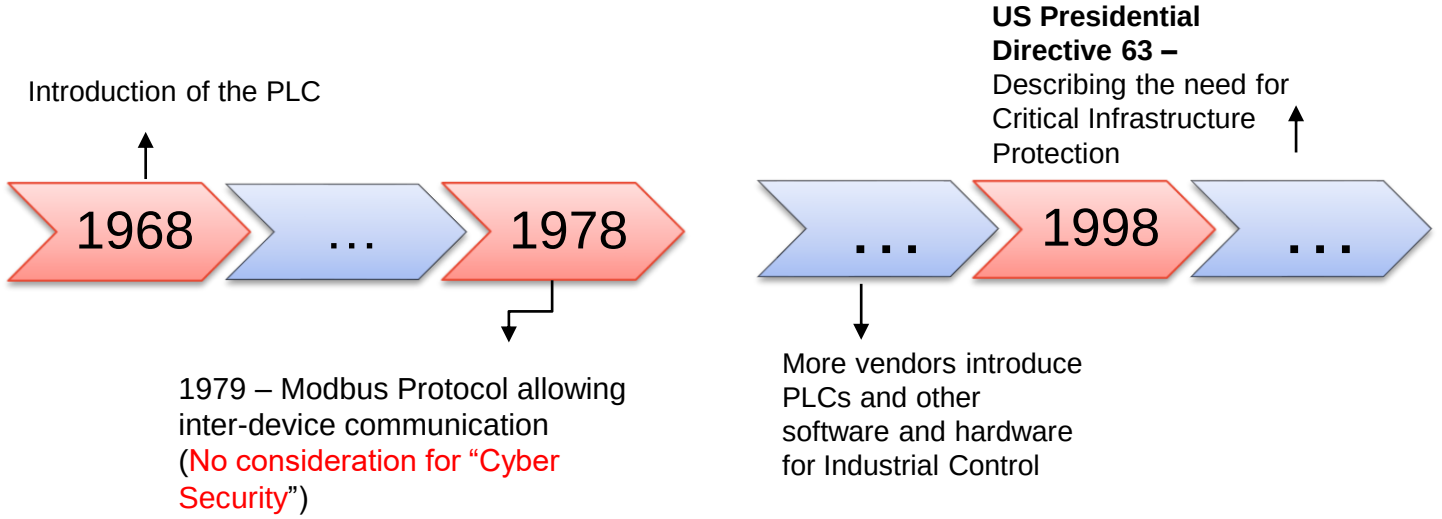
This War is occurring daily

This War is increasingly targeting critical infrastructure and industrial installations

COPYRIGHT © 2021 MITSUBISHI ELECTRIC EUROPE B.V. ALL RIGHTS RESERVED. All product names, trademarks and registered trademarks are property of their respective owners

# A brief walk through history

*"Industrial Control Cyber Security have gained greater importance since the invention of the first PLC"*




*"What lessons have we learned and how can we better safeguard our OT environments?"*

COPYRIGHT © 2021 MITSUBISHI ELECTRIC EUROPE B.V. ALL RIGHTS RESERVED. All product names, trademarks and registered trademarks are property of their respective owners

# Agenda

- Cybersecurity framework
- Defense-in-depth details
- Cybersecurity in focus
- Summary

Safeguard your automation infrastructure through the Mitsubishi Electric FA “Defense In Depth” approach

I ELECTRIC EUROPE B.V. ALL RIGHTS RESERVED. All product names, trademarks and registered trademarks are property of their respective owners

MITSUBISHI ELECTRIC
Changes for the Better

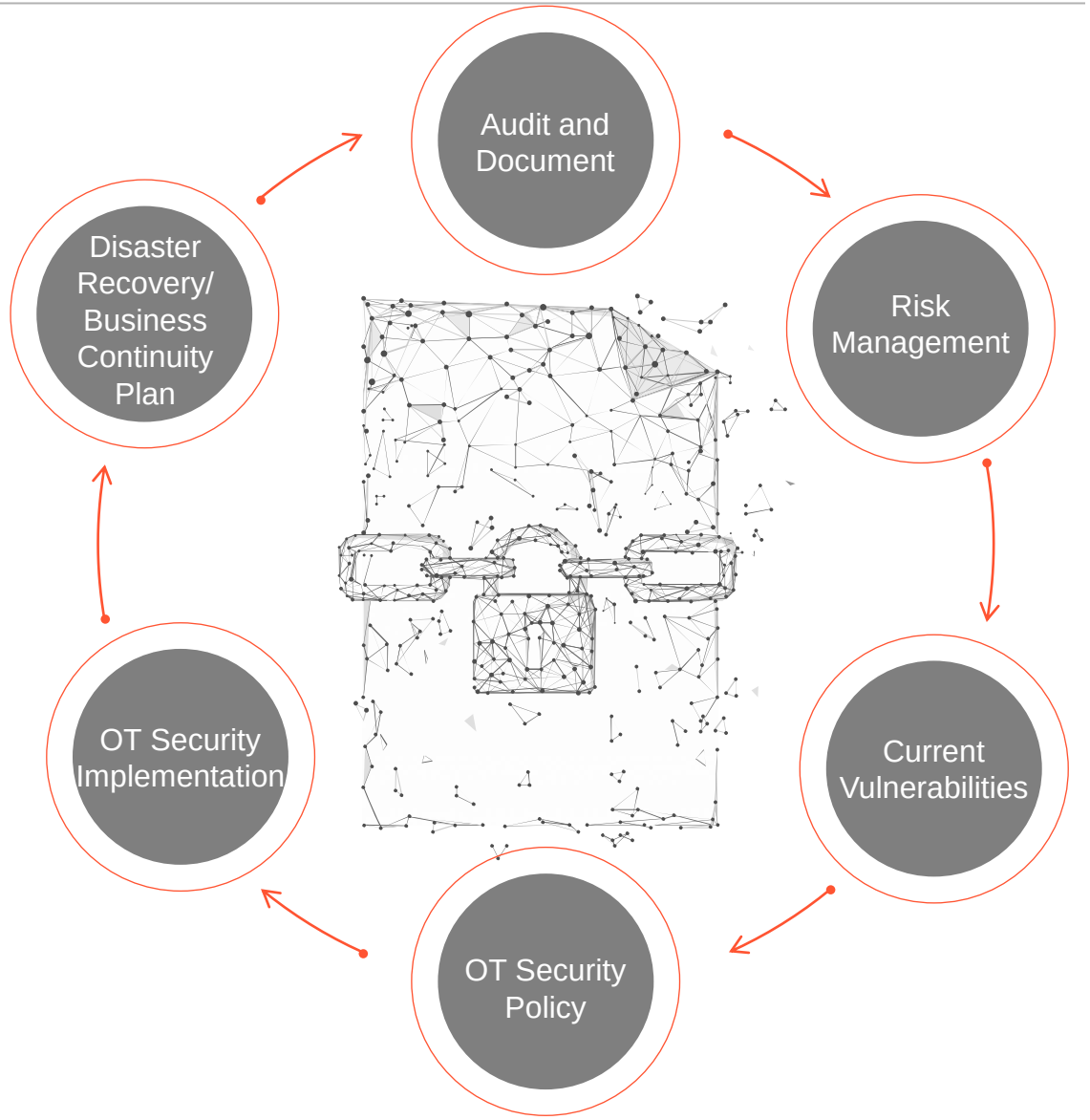
# Cybersecurity framework

COPYRIGHT © 2021 MITSUBISHI ELECTRIC EUROPE B.V. ALL RIGHTS RESERVED. All product names, trademarks and registered trademarks are property of their respective owners

# Begin with a risk assessment

## STEPS

- Define assets/inventory/equipment
- Define roles/responsibilities and chain of command
- Define connectivity, protocols and applications
- Identify potential threats, mitigation and preventative steps
- Rank threats according to quantifiable values (such as financial damage)
- Plan effective measures based on threat level and then implement accordingly
- Test the Recovery Strategy!
- Documentation is very important - ISO 27001 is the “Gold Standard”

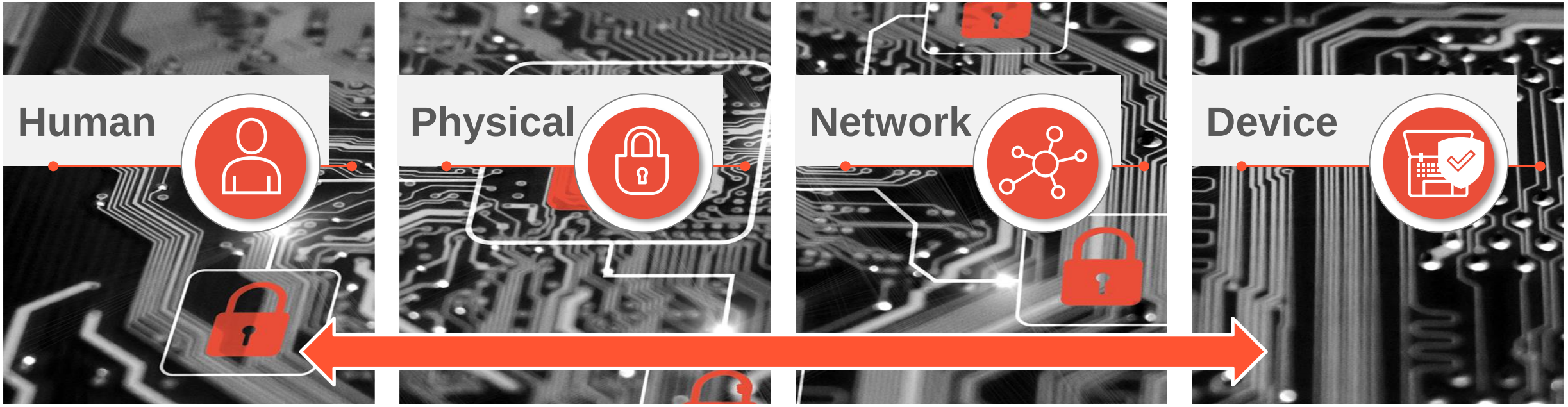



COPYRIGHT © 2021 MITSUBISHI ELECTRIC EUROPE B.V. ALL RIGHTS RESERVED. All product names, trademarks and registered trademarks are property of their respective owners

# Securing your process and infrastructure

## DEFENSE-IN-DEPTH

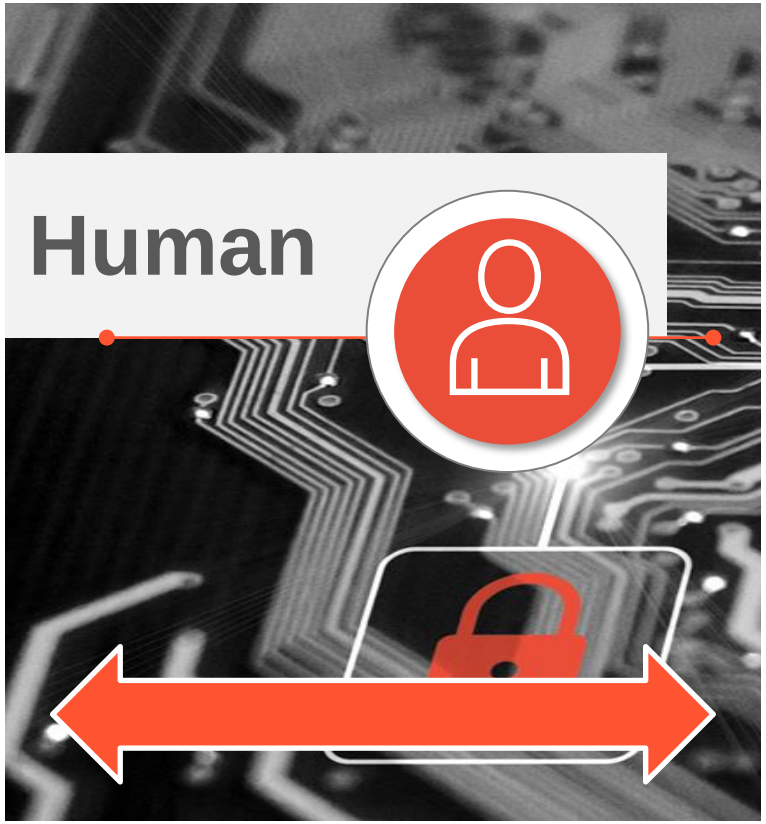
- Based on IEC 62443-3 / 4 – Securing the automation environment at a System Level as well as at a Device Level
- Harden every layer of the human, network and automation environment
- Improve the ability to prevent and detect attacks and system weaknesses




COPYRIGHT © 2021 MITSUBISHI ELECTRIC EUROPE B.V. ALL RIGHTS RESERVED. All product names, trademarks and registered trademarks are property of their respective owners

# Defense-in-depth

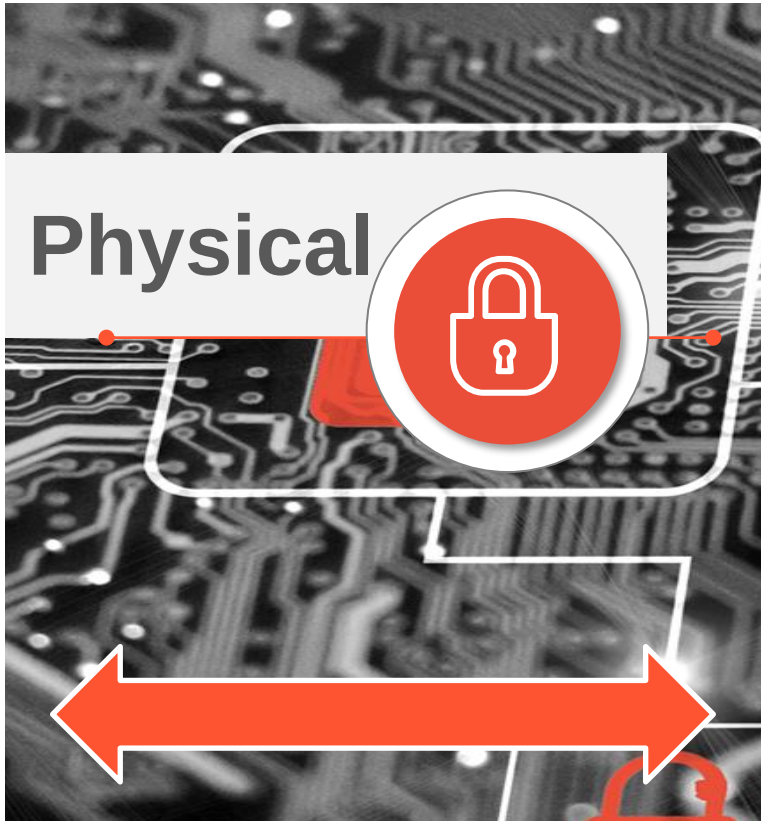
## Measures to control user behavior




- Create a well defined automation security framework
- Clearly define roles and responsibilities and chain of command
- Educate employees, contractors and partners on correct use of security measures
- Make use of multi-factor authentication to secure access

COPYRIGHT © 2021 MITSUBISHI ELECTRIC EUROPE B.V. ALL RIGHTS RESERVED. All product names, trademarks and registered trademarks are property of their respective owners

# Measures to restrict and control physical access

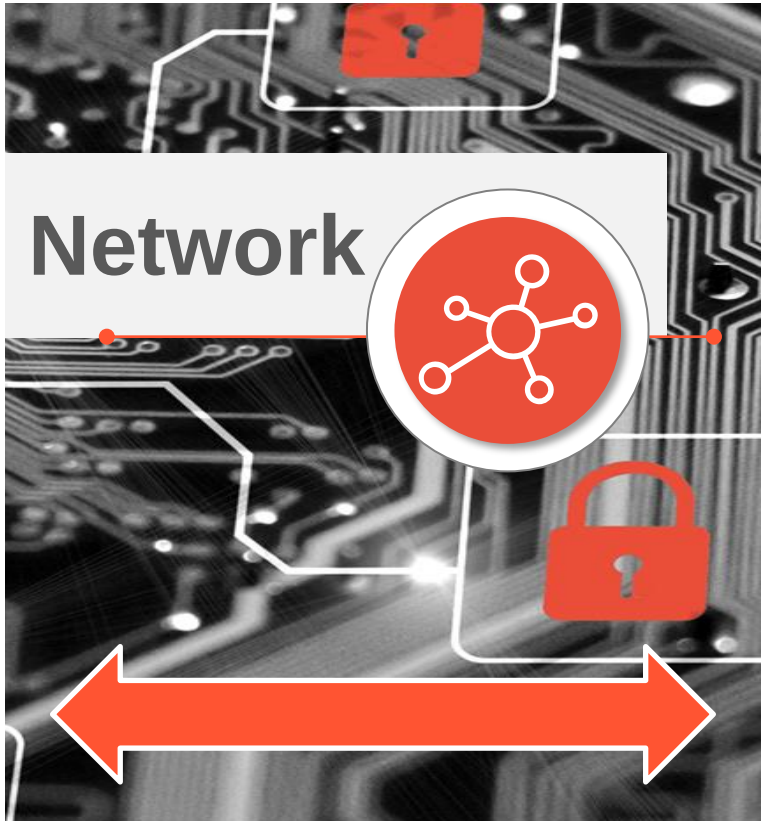



- Create a structured physical access control environment
- Disable and prevent unauthorized access to network switches, cabling, USB ports and computer terminals.
- Prohibit the connection of personal devices to the automation / information system

COPYRIGHT © 2021 MITSUBISHI ELECTRIC EUROPE B.V. ALL RIGHTS RESERVED. All product names, trademarks and registered trademarks are property of their respective owners

# Defense-in-depth

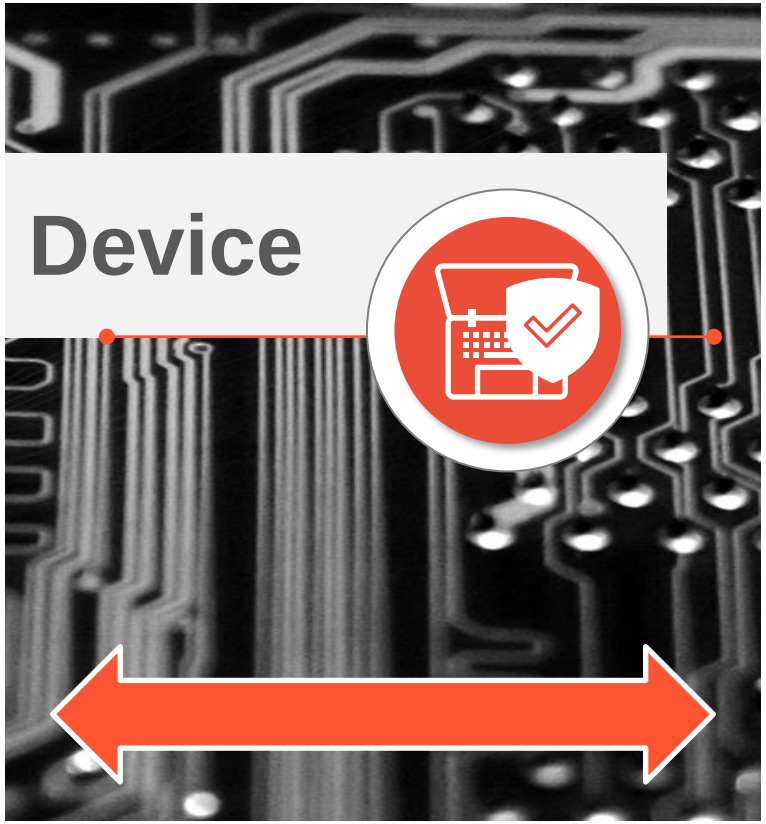
## Measures to secure inter-connectivity




- **Separate the OT network from the IT network**
  - → Use network segmentation through a firewall or VLAN
  - → Make use of a DMZ (Demilitarized zone) for fine-grained network / application control and to manage risk
- **Use encrypted communication layers**
  - → Digital certificates and OPC UA
  - → MACSec
  - → VPN
- **Restrict / Control Internet connectivity from within the OT network**

COPYRIGHT © 2021 MITSUBISHI ELECTRIC EUROPE B.V. ALL RIGHTS RESERVED. All product names, trademarks and registered trademarks are property of their respective owners

# Product / device security functions




- Restrict network access with the IP Filter function
- Make use of password and multi-factor authentication to limit access
- Encrypt data storage
- Install Anti-virus / Anti-malware software on computers connected to the OT network
- Allow communication from verified sources only
  → E.g. by making use of mutual authentication through the use of digital certificates or verified credentials
- Only allow specified software to be installed on computers connected to the OT network
- Ensure proper product disposal for decommissioned items so that valuable information cannot be exploited by a third party

COPYRIGHT © 2021 MITSUBISHI ELECTRIC EUROPE B.V. ALL RIGHTS RESERVED. All product names, trademarks and registered trademarks are property of their respective owners

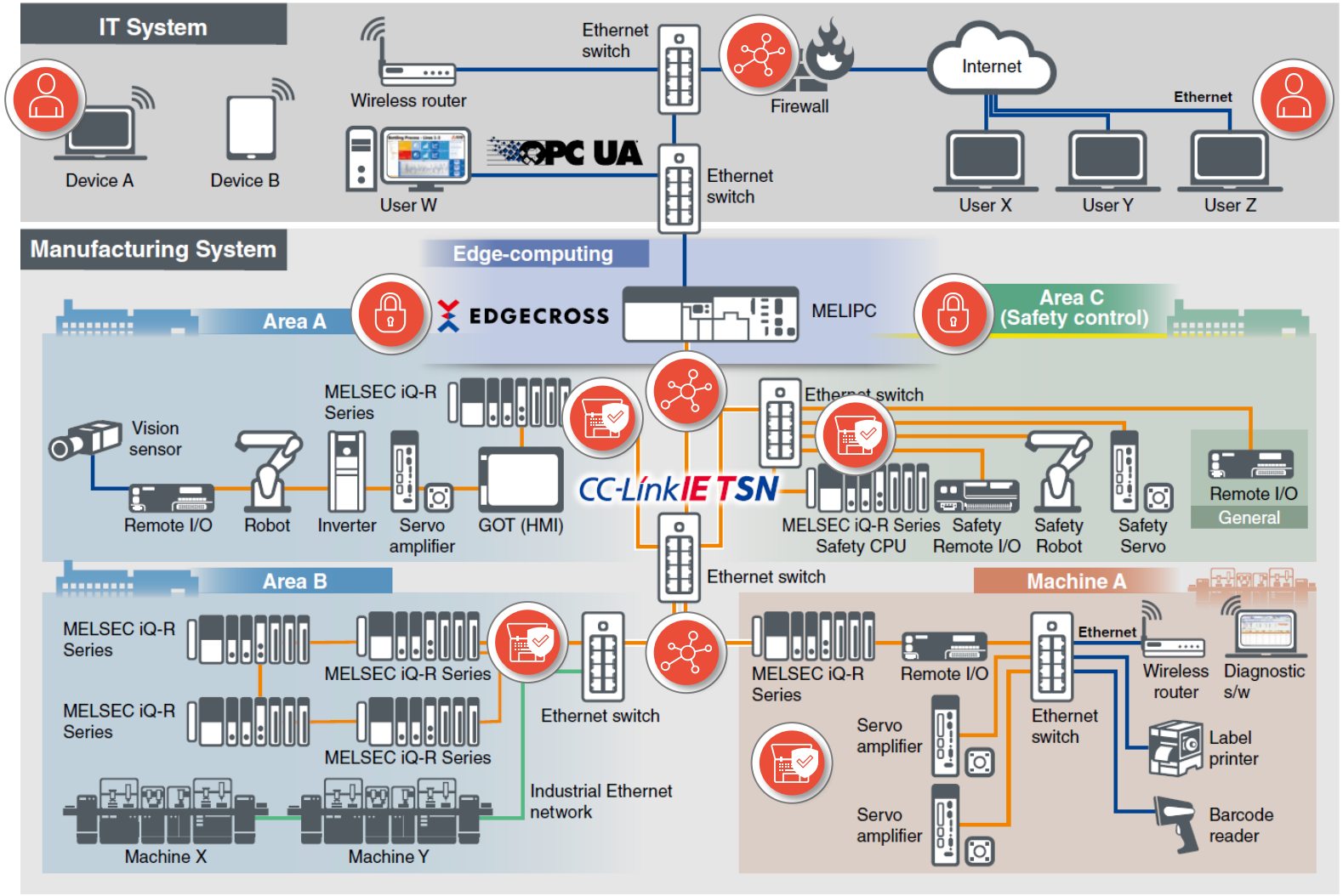
# Defense-in-depth: Network layout

Human

Physical

Network

Device




Example of Network Layout

COPYRIGHT © 2021 MITSUBISHI ELECTRIC EUROPE B.V. ALL RIGHTS RESERVED. All product names, trademarks and registered trademarks are property of their respective owners

# Defense-in-depth: Summary

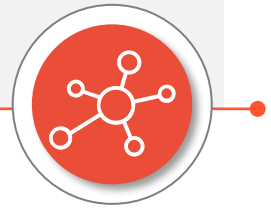
## Human

- Clearly define roles and responsibilities and chain of command
- Prohibit the connection of personal devices to the automation / information system
- Separate guest network from IT / OT networks
- Make use of a centralized and secure account management solution (such as LDAP / Active Directory)
- Make use of multi-factor authentication

## Physical

- Define physical assets
- Create a well structured physical access control environment
- Implement physical asset monitoring
- Create multi-factor authentication requirements for safety critical assets

## Network



- Separate the OT network from the IT network
- Use network segmentation through a firewall or VLAN
- Make use of a DMZ (Demilitarized zone) for fine-grained network / application control and to manage risk
- Use encrypted communication layers (such as a VPN or Layer 2 Encryption)

## Device

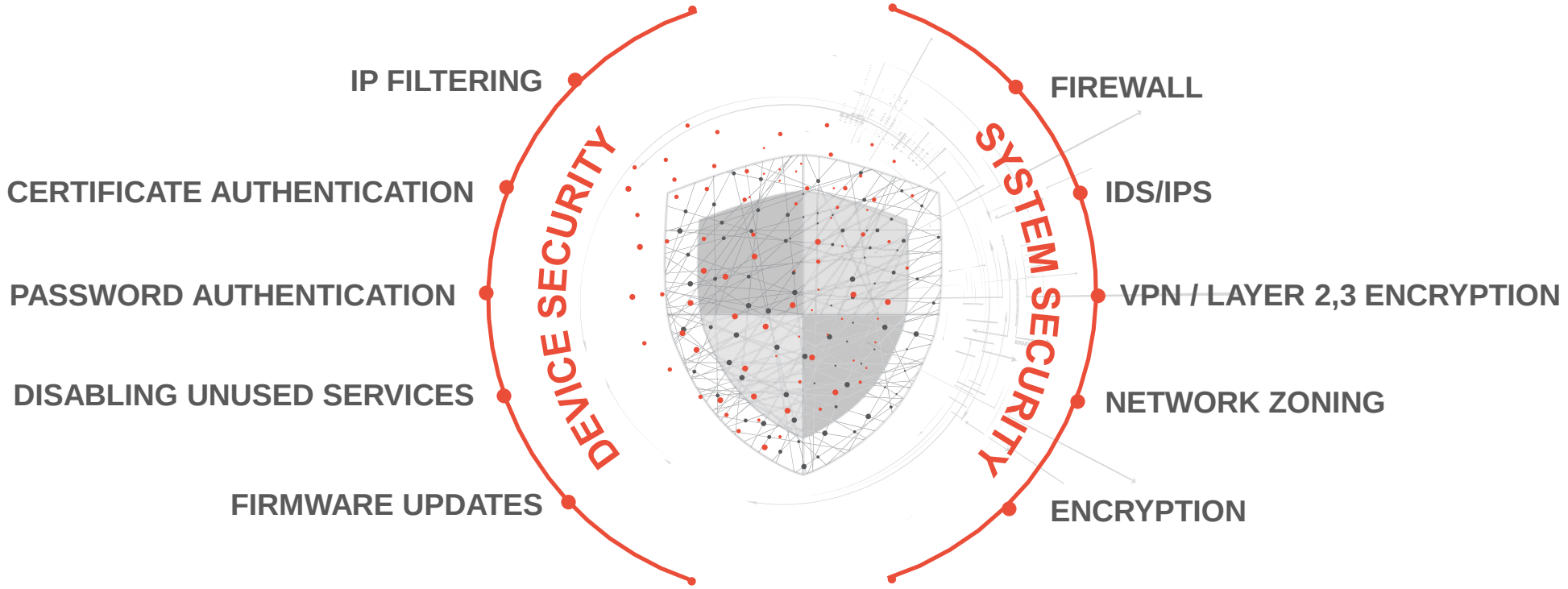
- Allow only authenticated device access (e.g. by utilizing digital certificates)
- Make use of the IP filtering function
- Install Anti Virus / Anti Malware on computers connected to the OT Network
- Disable unused services on Devices and Equipment

Set of Safeguarding Mechanisms

COPYRIGHT © 2021 MITSUBISHI ELECTRIC EUROPE B.V. ALL RIGHTS RESERVED. All product names, trademarks and registered trademarks are property of their respective owners

# Defense-in-depth: Summary

- Mitsubishi recommends using a “Defense in Depth” approach by applying security measures to the Human, Physical, Network and Device layers
- The Open Systems Interconnect (OSI) model can also assist by securing the different layers in a connected/networked environment
- Each of these “layers” require specific security measures in order to “harden” the layer’s defenses
- By providing security measures at the Human, Physical, Network and Device levels, a secure IACS solution can be provided to critical infrastructure using Mitsubishi FA products

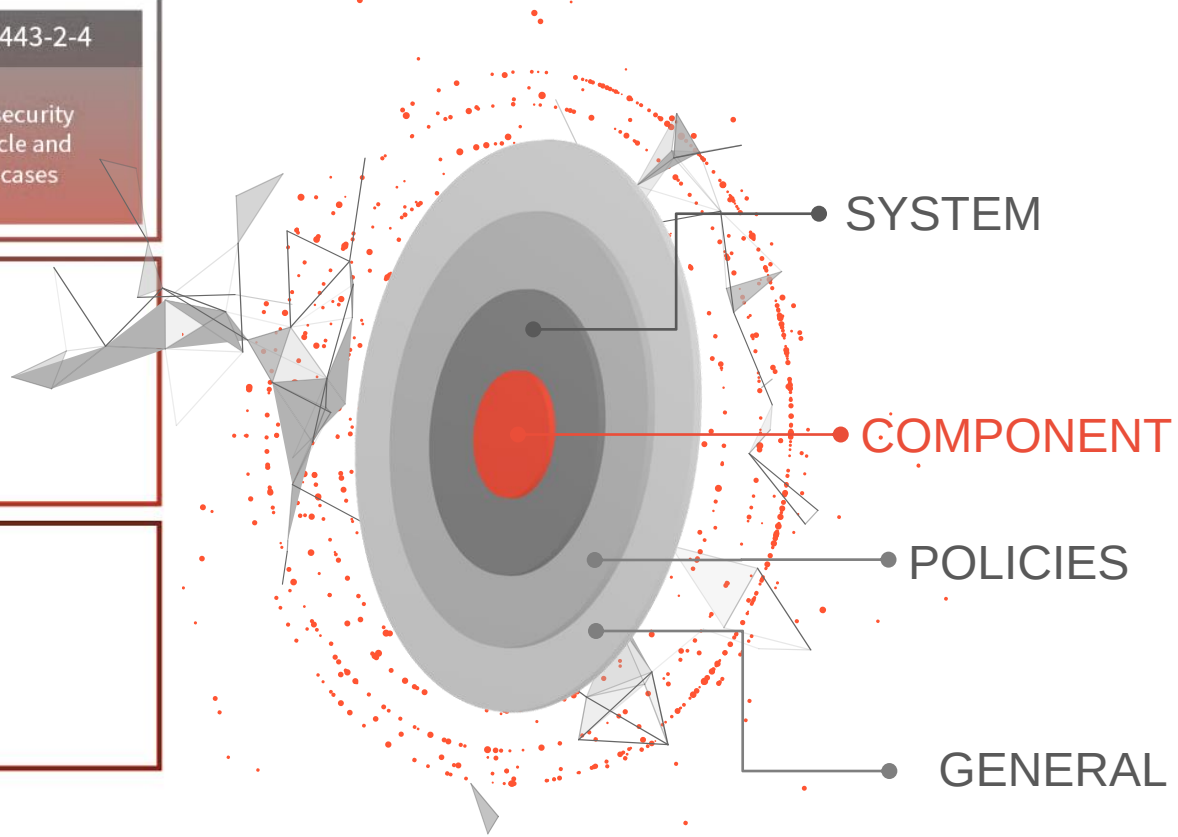



COPYRIGHT © 2021 MITSUBISHI ELECTRIC EUROPE B.V. ALL RIGHTS RESERVED. All product names, trademarks and registered trademarks are property of their respective owners

# Security standards: IEC 62443

| | | | | |
|---|---|---|---|---|
| General | IEC 62443-1-1<br>Terminology, concepts and models | IEC TR-62443-1-2<br>Master glossary of terms and abbreviations | IEC 62443-1-3<br>System security conformance metrics | IEC TR-62443-1-4<br>IACS security lifecycle and use-cases |
| Policies & Procedures | IEC 62443-2-1<br>Establishing an industrial automation and control system security program | IEC TR-62443-2-2<br>Master glossary of terms and abbreviations | IEC TR-62443-2-3<br>System security conformance metrics | IEC 62443-2-4<br>IACS security lifecycle and use-cases |
| System | IEC TR-62443-3-1<br>Terminology, concepts and models | IEC 62443-3-2<br>Master glossary of terms and abbreviations | IEC 62443-3-3<br>System security conformance metrics | |
| Component | IEC 62443-4-1<br>Product development requirements | IEC 62443-4-2<br>Technical security requirements for IACS components | | |

- Focus on the **SYSTEM** and the **COMPONENT** levels
- IT is important to ensure that the **SYSTEM protects the COMPONENT!**




COPYRIGHT © 2021 MITSUBISHI ELECTRIC EUROPE B.V. ALL RIGHTS RESERVED. All product names, trademarks and registered trademarks are property of their respective owners

# Mitsubishi Electric's certification: IEC 62443

- Mitsubishi Electric FA have received certification for the Electrotechnical Commission's IEC 62443-4-1 standard regarding the Security Development Lifecycle (SDL) of industrial automation and control systems.
- Programmable controllers, industrial PCs, FA sensors, human-machine interfaces, servo amplifiers, inverters, robots, CNCs, electrical discharge machines, laser processing machines and related software and services are in the scope.
- Going forward Mitsubishi Electric FA will continue to strengthen its Cyber Security certification initiatives.

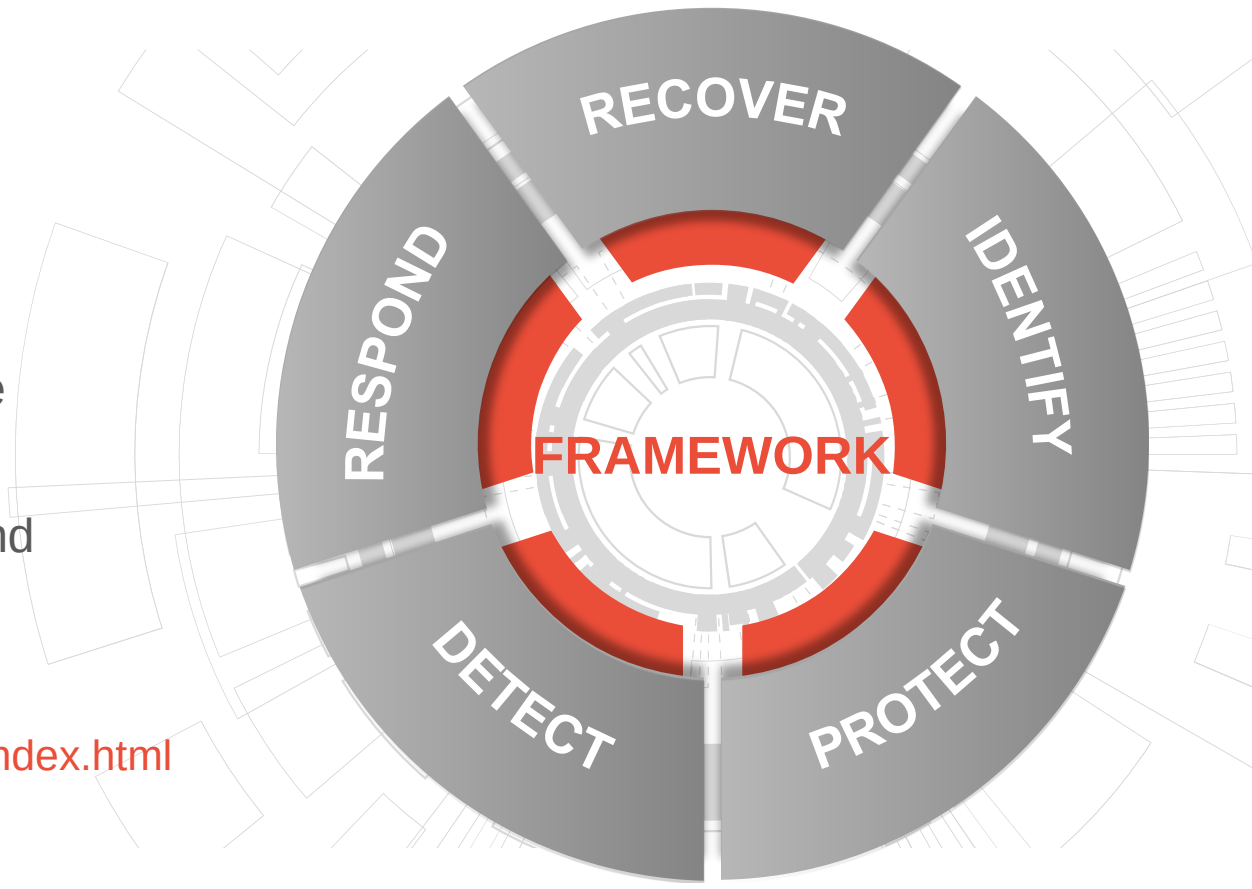
Nagoya Works and Industrial Systems Mechatronics Works

COPYRIGHT © 2021 MITSUBISHI ELECTRIC EUROPE B.V. ALL RIGHTS RESERVED. All product names, trademarks and registered trademarks are property of their respective owners

# Mitsubishi ELECTRIC FA Cyber Security Response Team

## Mitsubishi PSIRT - Product Security Incident analysis and reporting

- Product Security Incident Response Teams (PSIRT) at head office and every factory
- These teams are also involved in the Secure Product Development
- ICS incidents, vulnerabilities and remedial action are provided on the Mitsubishi PSIRT vulnerabilities website
- Each incident is described in detail, along with the product(s) affected and the impact, countermeasures and mitigation.




https://www.mitsubishielectric.com/en/psirt/vulnerability/index.html

COPYRIGHT © 2021 MITSUBISHI ELECTRIC EUROPE B.V. ALL RIGHTS RESERVED. All product names, trademarks and registered trademarks are property of their respective owners

MITSUBISHI ELECTRIC
Changes for the Better

# Cybersecurity in focus

COPYRIGHT © 2021 MITSUBISHI ELECTRIC EUROPE B.V. ALL RIGHTS RESERVED. All product names, trademarks are property of their respective owners

# European critical infrastructure initiatives

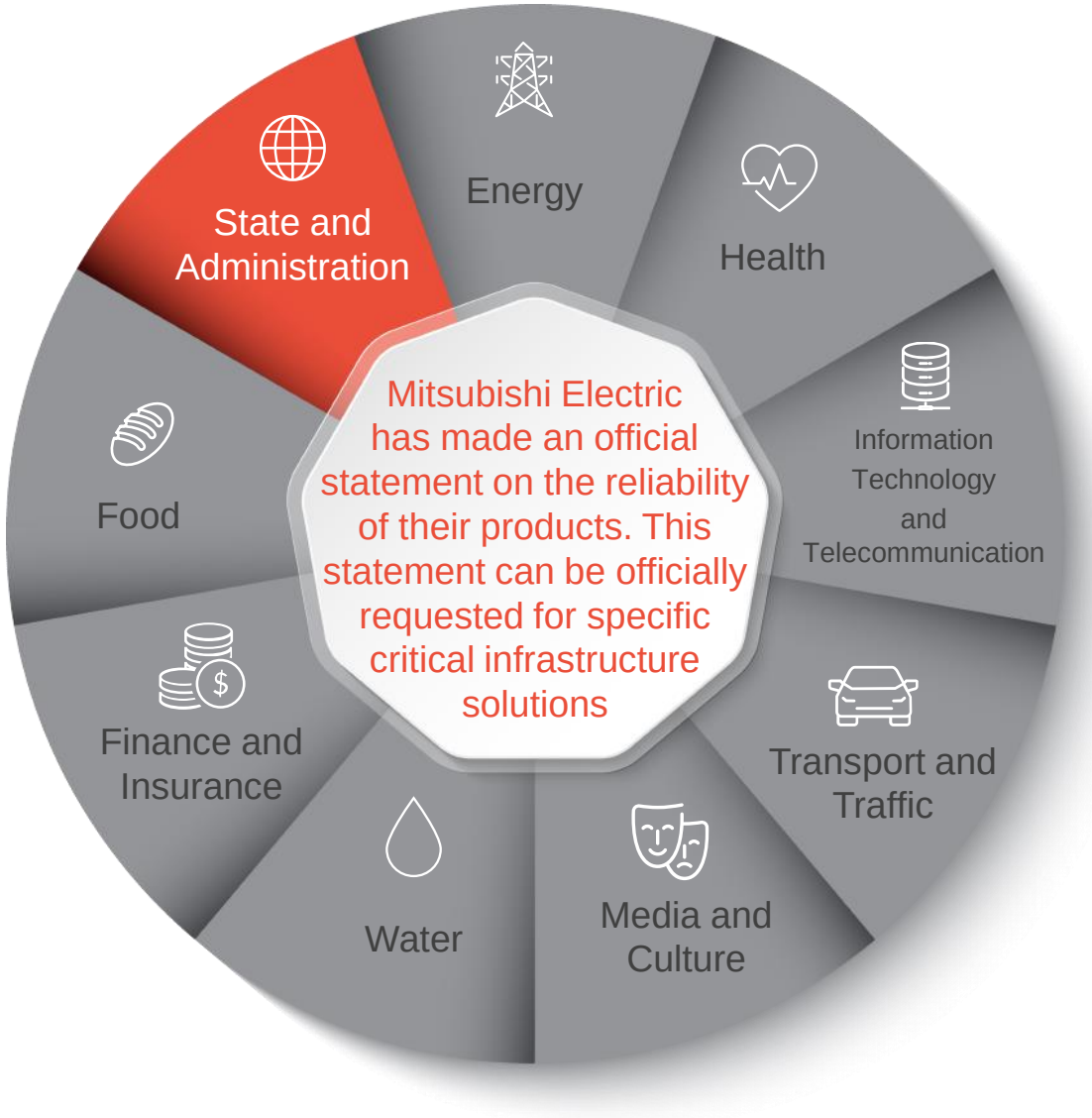
## Overview

- Several EU initiatives exist for the protection of critical infrastructure
  - → These include:
    - ENISA (NIST)
    - KRITIS
    - CIIP

*"Critical infrastructures are organizational and physical structures and facilities of such vital importance to a nation's society and economy that their failure or degradation would result in sustained supply shortages, significant disruption of public safety and security, or other dramatic consequences."*

*KRITIS*

- Proof of sufficient IT Security for operators of critical infrastructure which extends to suppliers
- Similar initiatives are underway for various European countries

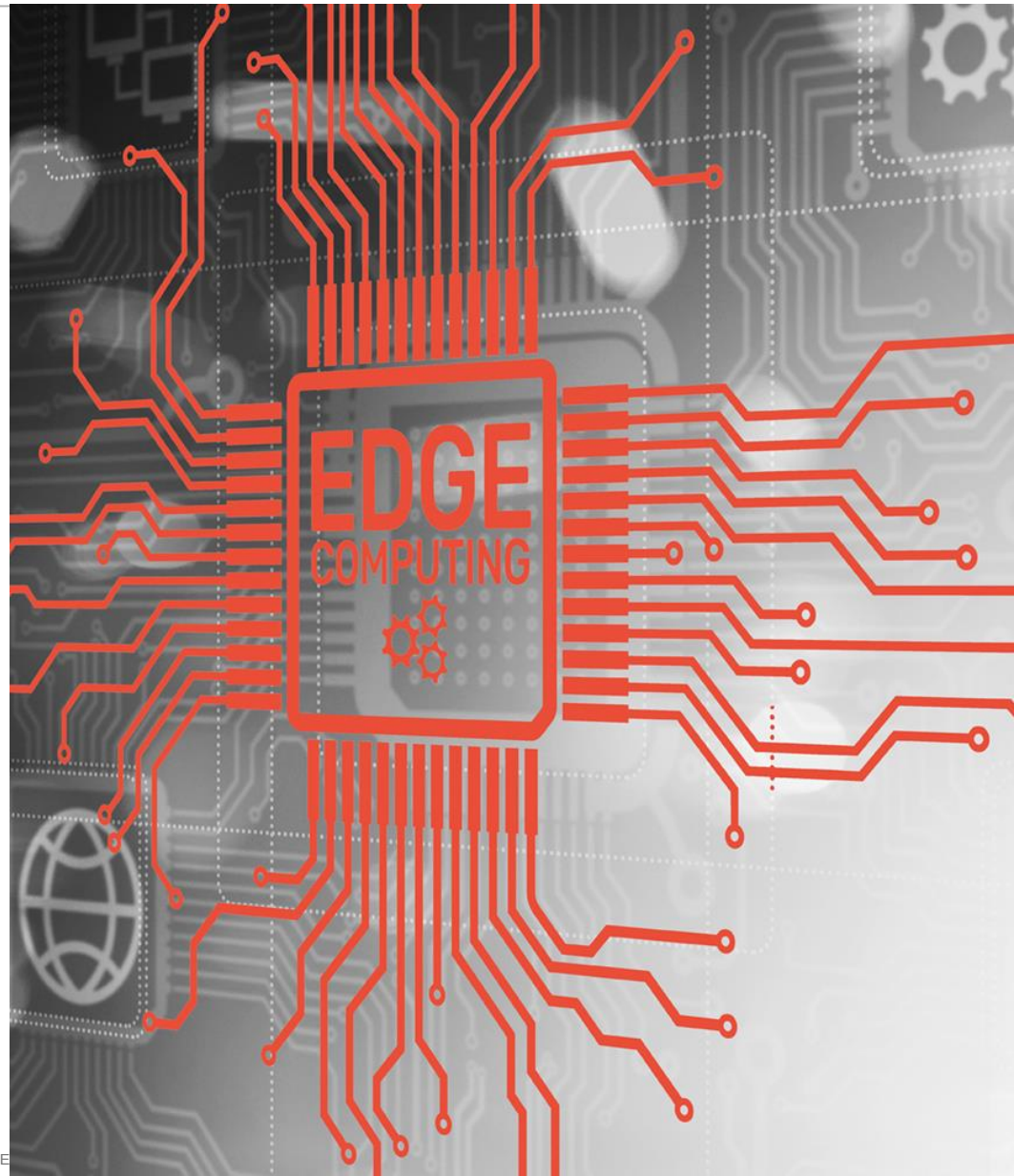



COPYRIGHT © 2021 MITSUBISHI ELECTRIC EUROPE B.V. ALL RIGHTS RESERVED. All product names, trademarks and registered trademarks are property of their respective owners

# Considerations for Edge computing

## FA: EDGE COMPUTING

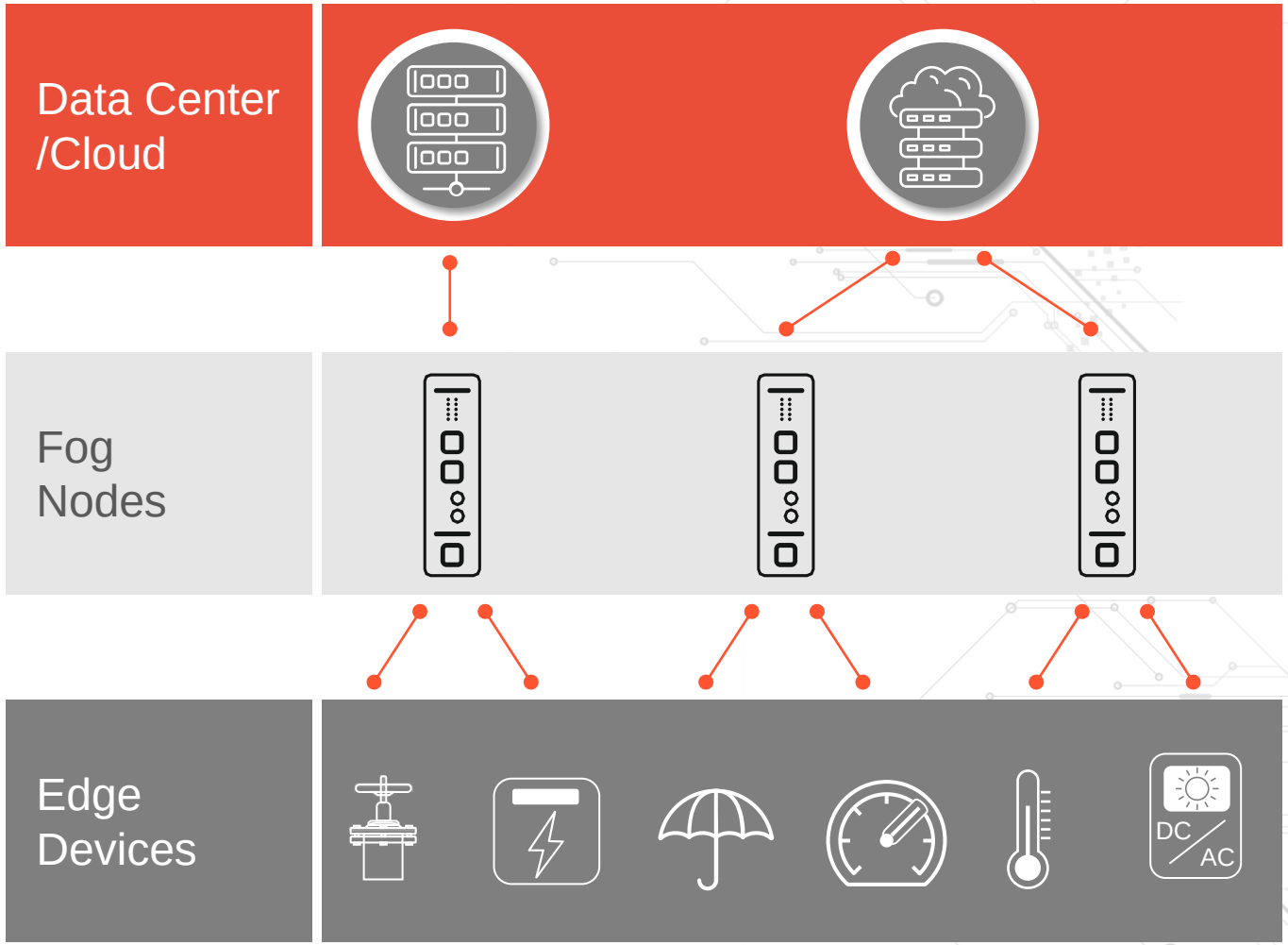
- EDGE computing requires additional security measures, including separation of monitoring and control functionality and network zoning
- In most cases information provided by the FA solution should be in the direction of the Cloud Environment, with no direct link back into the FA network i.e. single uplink direction only (read-only).
- The creation of a DMZ (Demilitarized Zone) is recommended in most scenarios
- Separate OT and IT Networks to maintain the “AIR GAP” as far as possible
- Limit access to well-defined services
- A single point of access is easier to shutdown in the case of emerging attacks than multiple access points




COPYRIGHT © 2021 MITSUBISHI ELECTRIC EUROPE

# Considerations for IIOT

- IIOT offers powerful, flexible and cost effective new mechanisms for production and automation
- Careful cyber security considerations are required:
  - → Make use of FOG nodes to protect and encrypt data before connecting to the cloud
  - → Ensure that FOG nodes are secured within the DMZ -De-Militarized Zone
  - → Ensure that the default configuration for all connected devices are read-only
  - → Write-access should only be allowed via multi-factor authentication




COPYRIGHT © 2021 MITSUBISHI ELECTRIC EUROPE B.V. ALL RIGHTS RESERVED. All product names, trademarks and registered trademarks are property of their respective owners

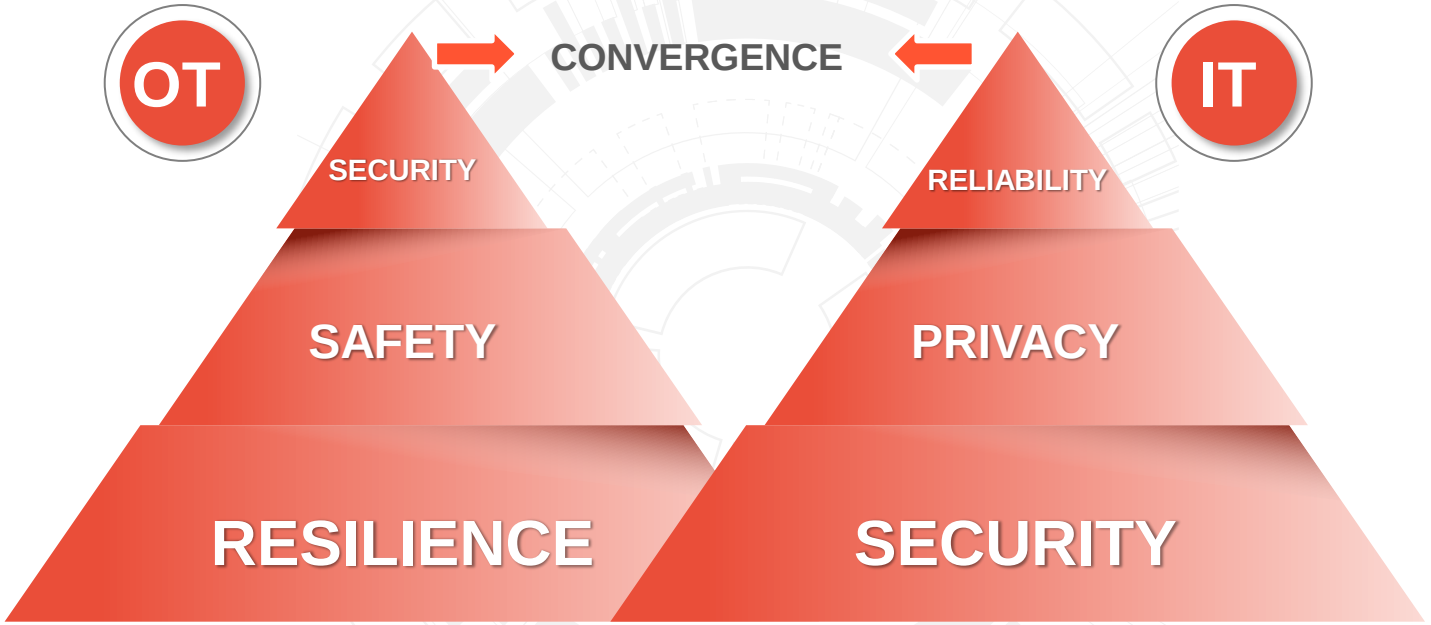
# Inherent network Security provided through CC-Link IE TSN

- Support for standard Ethernet devices and switching infrastructure allows for support of high-speed, low-level Layer 2 encryption technologies such as MACSec to encrypt traffic on the network or to secure critical CC Link IE TSN network endpoints
- Support for TCP/IP ensures that a comprehensive range of existing IT / OT based security products can be used on CC-Link IE TSN Networks
- CC-Link IE Devices can implement additional measures such as user authentication to prevent unauthorized access on the network
- One network for all communication means:
  - → Easier management of devices
  - → Easier maintenance of network nodes
  - → Increased visibility and transparency

COPYRIGHT © 2021 MITSUBISHI ELECTRIC EUROPE B.V. ALL RIGHTS RESERVED. All product names, trademarks and registered trademarks are property of their respective owners

# OT and IT priorities

- IT policies are increasingly being applied to OT environments
- IT policies are focused on updates, security patches and Operating System components on a regular basis.
- These policies often negatively affect the efficiency and effectiveness of the OT components.
- IT and OT policies should coexist at a system level.
- For the production floor - OT policies should be applied at the component level
- This also follows recommendations at a system and component level according to the IEC 62443 security standard




COPYRIGHT © 2021 MITSUBISHI ELECTRIC EUROPE B.V. ALL RIGHTS RESERVED. All product names, trademarks and registered trademarks are property of their respective owners

MITSUBISHI ELECTRIC
Changes for the Better

# In focus:
# *Password Security*

COPYRIGHT © 2021 MITSUBISHI ELECTRIC EUROPE B.V. ALL RIGHTS RESERVED. All product names, trademarks and registered trademarks are property of their respective owners

# Password Security

## Is Your Windows password already cracked?

| length: | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|
| LM-enabled | completely cracked | completely cracked | completely cracked | completely cracked | completely cracked | completely cracked | completely cracked | safe |
| simple passwords | completely cracked | lower, upper, numeric cracked | numeric cracked | numeric cracked | numeric cracked | safe | safe | safe |
| complex passwords | completely cracked | CLN cracked | CLN cracked | CLN cracked | safe | safe | safe | safe |

All data is based on rainbow tables available at FreeRainbowTables.com. Rainbow tables can be used to "decrypt" a password.
"LM-enabled" means the computer has LM password storage turned on. This is the default for Windows 2003/Vista and earlier.
"Complex" means it contains characters from at least three of the four categories (uppercase, lowercase, numbers, symbols).
"CLN" means it is in capital-lowercase-number format (ex. Password123).
Data compiled by Nick Brown ( http://nick-brown.com ). Last updated: February, 2012.

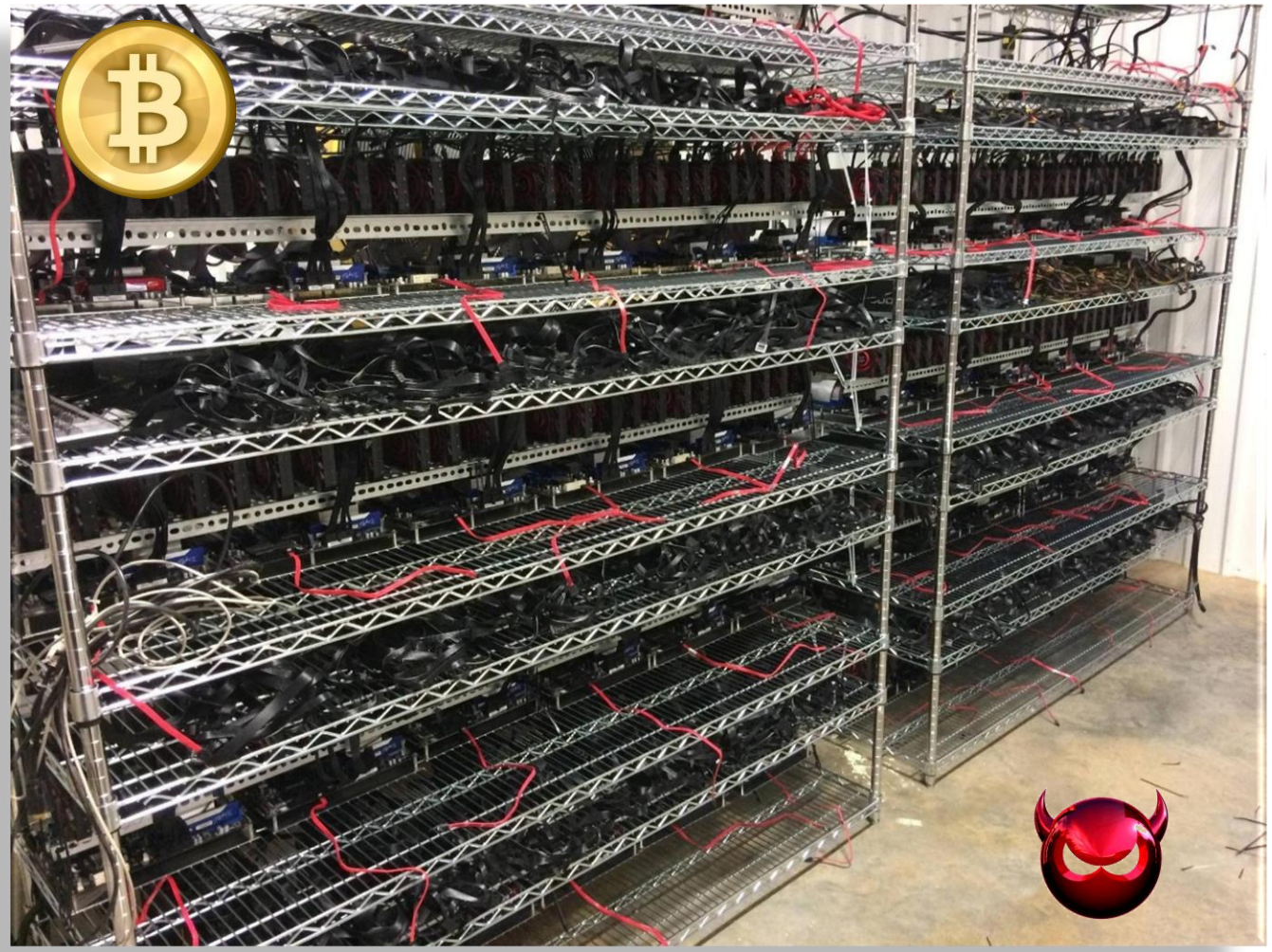
Example:

+-220 000 Dictionary Based Words

- Take the common word ‘PASSWORD’
- Using a dictionary and a combination of Uppercase, Lowercase and special characters – i.e. : “P@5SW0rd”
- There are 6561 combinations
- Breakable within less than a second
- Using combinations of words and numbers, still often breakable within < 30 minutes

COPYRIGHT © 2021 MITSUBISHI ELECTRIC EUROPE B.V. ALL RIGHTS RESERVED. All product names, trademarks and registered trademarks are property of their respective owners

# Brute Force Hash Attacks



- Bitcoin has fueled very high performance “mining rigs”
- These systems can be used for “dubious” purposes, such as being rented out for brute force hash attacks on the dark web.
- Computing power:
- > 1000 000 000 passwords per second brute force

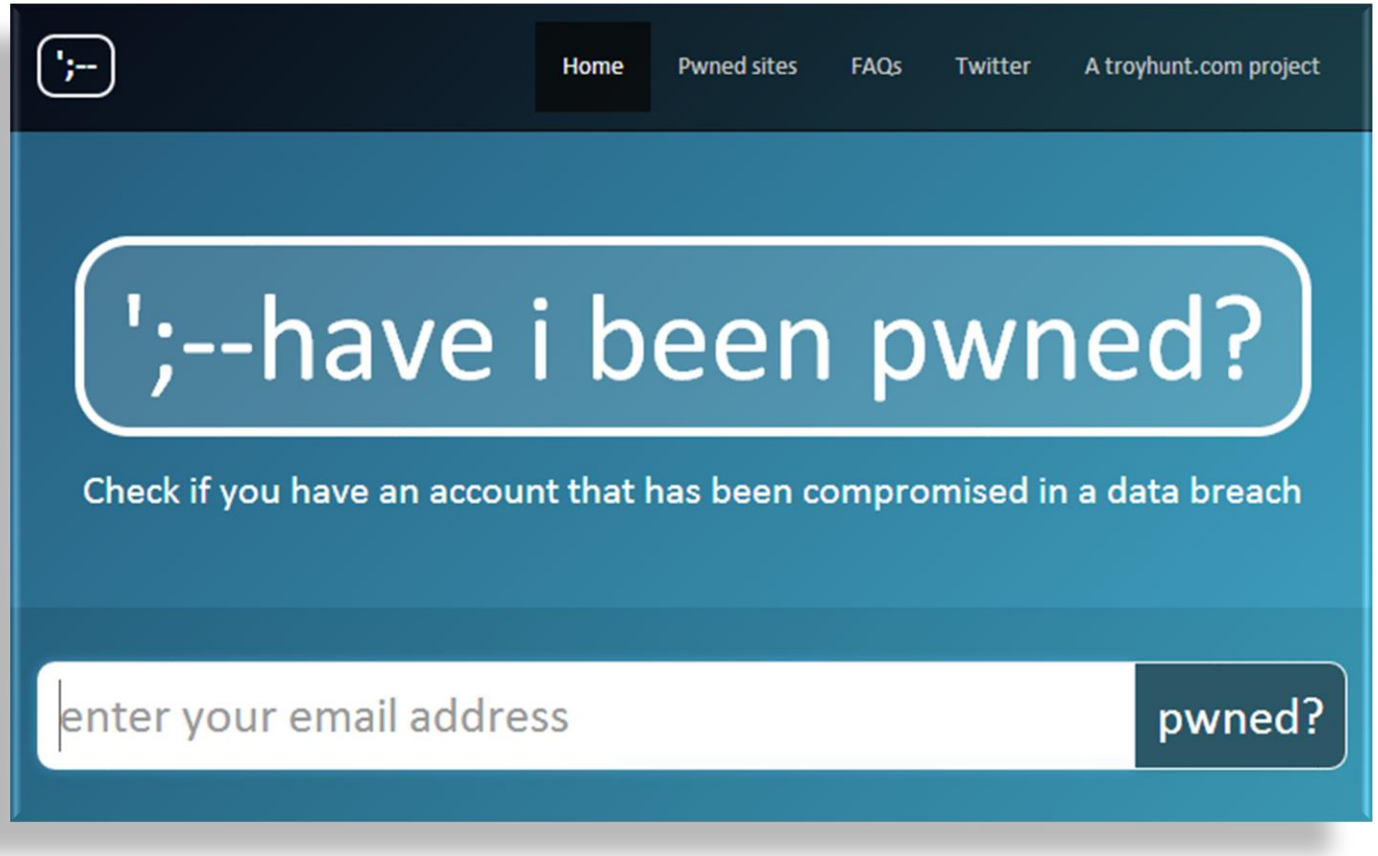
COPYRIGHT © 2021 MITSUBISHI ELECTRIC EUROPE B.V. ALL RIGHTS RESERVED. All product names, trademarks and registered trademarks are property of their respective owners

# Secure Authentication

- Passwords must be UNIQUE across all platforms and services
- Passwords should not contain recognizable words (even if these are obscured by numbers/symbols)
- Passwords should be at least 12 characters long
- A correctly hashed 12 character password will theoretically take several years to brute-force (bcrypt/sha512)
- Use a password manager, such as the Open Source KeePass, to assist in generating secure passwords
- Make use of Multi-factor authentication

COPYRIGHT © 2021 MITSUBISHI ELECTRIC EUROPE B.V. ALL RIGHTS RESERVED. All product names, trademarks and registered trademarks are property of their respective owners

# Already compromised…?



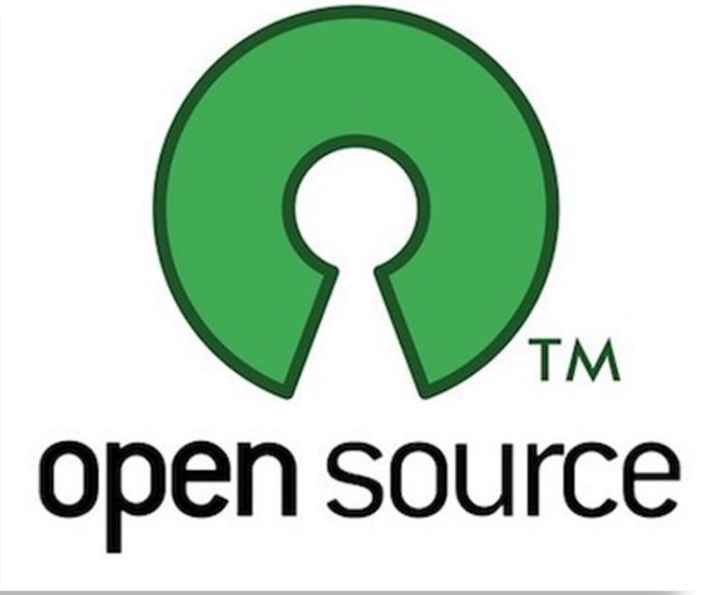

- Determine if some of your accounts have been breached
- Take immediate corrective action

* “PWNed” – Use of - (especially in video gaming) utterly defeat (an opponent or rival); completely get the better of

COPYRIGHT © 2021 MITSUBISHI ELECTRIC EUROPE B.V. ALL RIGHTS RESERVED. All product names, trademarks and registered trademarks are property of their respective owners

# Cyber Security and Open Source

- Open Source offers the ability to truly ensure transparency regarding security measures
- All current encryption and hashing algorithms have Open Source implementations that are widely used
- Open Source Security Solutions will form a bigger part of Cyber Security Solutions in the future



COPYRIGHT © 2021 MITSUBISHI ELECTRIC EUROPE B.V. ALL RIGHTS RESERVED. All product names, trademarks and registered trademarks are property of their respective owners

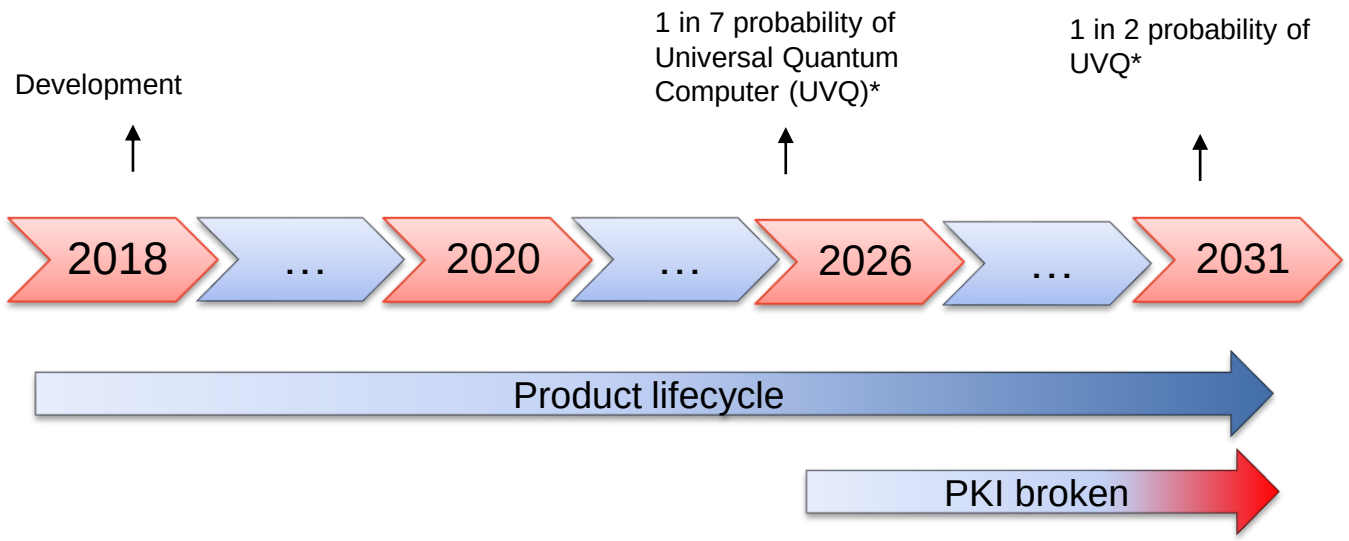
MITSUBISHI ELECTRIC
Changes for the Better

# Towards the future: Quantum Computing

COPYRIGHT © 2021 MITSUBISHI ELECTRIC EUROPE B.V. ALL RIGHTS RESERVED. All product names, trademarks and registered trademarks are property of their respective owners

# Quantum Realm

## Advancements in Quantum Computing poses a threat to current PKI solutions




***MOSCA, 2015**

- Information carries with it an associated “Time Value”
- For example to brute-force a 12 character password could take several years.
- This is because current brute-force algorithms still have to execute sequentially on the entire potential hash permutation database.
- In Quantum Computing, computations happen at the same time. The larger the number of available qubits, the larger the number of calculations that can happen simultaneously.

COPYRIGHT © 2021 MITSUBISHI ELECTRIC EUROPE B.V. ALL RIGHTS RESERVED. All product names, trademarks and registered trademarks are property of their respective owners

# Summary

## Providing a strong security framework with Mitsubishi Electric

Using the Defense-in-Depth approach **it is possible to provide a strong security framework for protecting your infrastructure and automation solutions today**

With *increased security comes increased inconvenience* – It is important to strike the right balance between security, performance and convenience based on the asset / protection value

Periodic revision and assessment is important to verify, validate and update security mechanisms to stay up to date with disclosed vulnerabilities and improved security mechanisms

By securing your solution at the **system level** it is possible to protect devices at the **component level** as well

COPYRIGHT © 2021 MITSUBISHI ELECTRIC EUROPE B.V. ALL RIGHTS RESERVED. All product names, trademarks and registered trademarks are property of their respective owners