The ISA/IEC 62443 cybersecurity standard and its application in manufacturing and automation

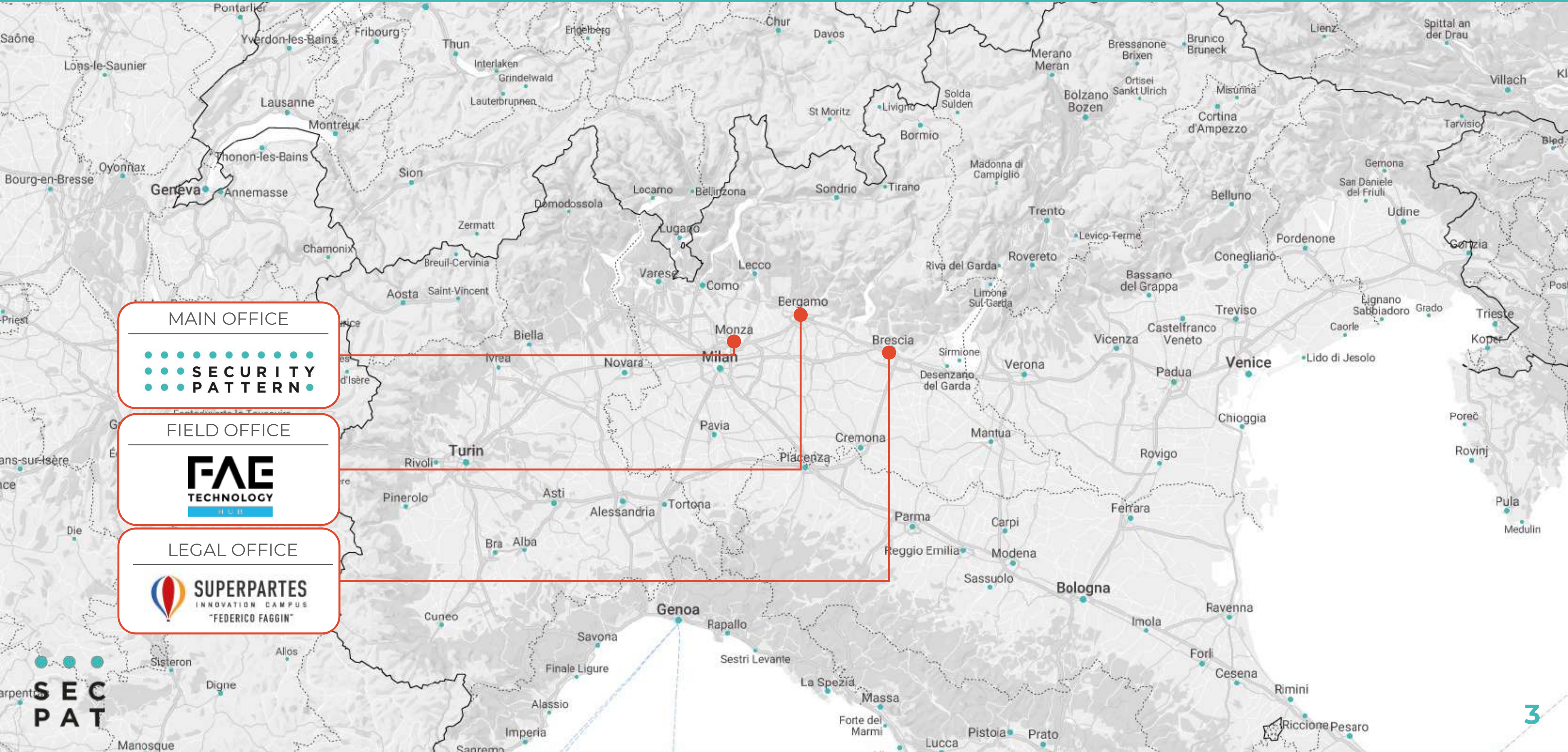
Manuel Crotti

Mission

We help creators of intelligent connected devices to **design**, **implement** and **operate** their systems with a **sustainable security level**

SEC PAT

Location



MAIN OFFICE

SECURITY PATTERN

FIELD OFFICE

FAE TECHNOLOGY HUB

LEGAL OFFICE

SUPERPARTES INNOVATION CAMPUS "FEDERICO FAGGIN"

SEC PAT

Who we are: the team

Alberto Battistello
Senior Security Engineer

Lorenzo Nava
Security Engineer

Stefano Cristalli
Senior Security Engineer

Gabriele Quagliarella
Security Expert

Maria Chiara Molteni
Security Engineer

Marta Fornasier
Security Engineer

Isabella Donders
Operations Lead

Fabiana Gaffurini
Administrative Manager

- Engineer - M.Sc.
- Ph.D.
- Author of SHA-3
- Patents / Certs
- Master

SEC PAT

Who we are: the partners

25+

Guido Bertoni
CEO

4

Filippo Melzani
CTO

4

Massimo Ratti
DevOps Manager

1

Manuel Crotti
Business developer

- Engineer - M.Sc.
- Ph.D.
- Author of SHA-3
- Patents / Certs
- Master

SEC PAT

Security Pattern's reference markets

- IIoT
  - Industrial automation
  - Utilities
  - Automotive
  - Medical
  - …

- IoT
  - Smart building
  - Home automation

- Misc.
  - Consulting
  - FW development
  - Government/Defense

SEC PAT

Cybersecurity in IACS

Is it needed?

Cybersecurity in IACS: it's needed!

- **IACS** = Industrial Automation and Control Systems
- There is a need to address security triggered by:
  - IACS are **increasingly connected, becoming IIoT**
  - **COTS** (commercial off-the-shelf) systems are **increasingly being used** in IACS
- These two trends imply **increased exposure to cyberattacks**
- And an ever growing number of cases of attacks to IACS reported

SEC PAT

Some attack example

March 2021. Suspected Chinese hackers targeted electricity grid operators in India in an apparent attempt to lay the groundwork for possible future attacks.

April 2020. Government and energy sector entities in Azerbaijan were targeted by an unknown group focused on the SCADA systems of wind turbines

August 2019. Russian hackers were observed using vulnerable IoT devices like a printer, VOIP phone, and video decoder to break into high-value corporate networks

December 2017. French company Schneider Electric was forced to shut down operations of a power plant in the Middle East after malware compromised its industrial control systems. Analysis by security researchers indicated that the attack was sponsored by a nation-state.

Source: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

SEC PAT

Security By Design: the approach

Architecture Lifecycle as seen from the IIoT perspective:

- Development cycle ranging from a few months up to some years
- Service life of the product of some years up to 10+ years

Architecture Security as seen from the IIoT perspective

- Security needs to be ensured over the entire life of the device
- We firmly believe that this is possible only by means of a **Security-by-design** approach

SEC PAT

Let’s talk about pastry

What is the best standard to choose?

Shortcomings of Existing Standards

- Securing an operational technology (OT) system is not the same as securing an information technology (IT) system:
  - Functional safety contextualization

- There is need for a framework covering IACS development, integration and operation
  - At both a product and a process level
  - Through a risk-based approach (typical of the industrial context)
  - Addressing the security in the supply chain

- Aspects above are not holistically addressed by any one of the existing standards (ISO27001, Common Criteria, IEC62531, IEC 61850, FIPS140…)

SEC PAT

ISA/IEC 62443

A recipe for Cybersecurity in IACS

SECPAT

ISA/IEC 62443 – Roles and Scope

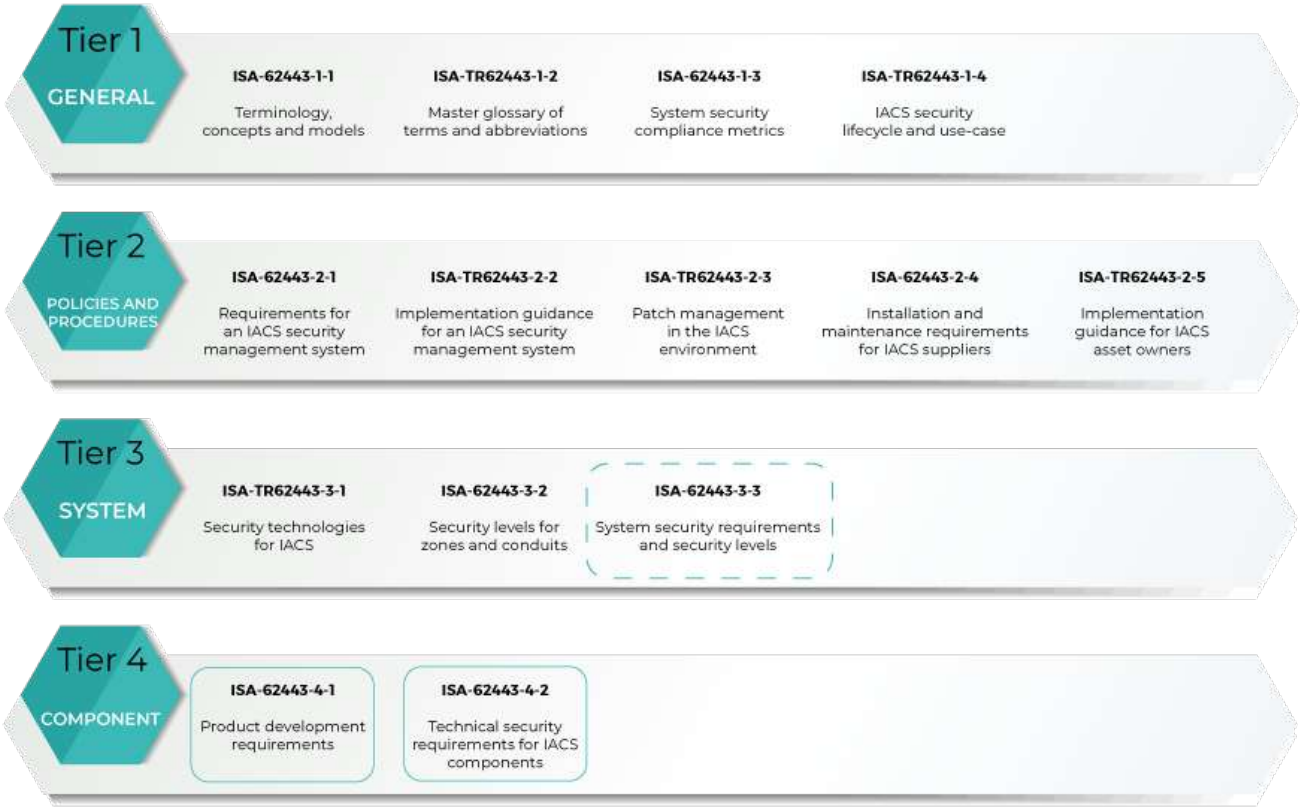
- ISA/IEC 62443 defines three main roles:
  - **Asset Owner (AO)** who operates the IACS
  - **System Integrator (SI)** who integrates subsystems and components to build and configure the IACS in the intended environment
  - **Product Supplier (PS)** who develops and maintains a component (or subsystem) that can be a software application, an embedded device, a network component, a host device

- We are addressing ISA/IEC 62443 from a **Product Supplier** perspective

SEC PAT

ISA/IEC 62443 - Structure

- General
  - Contains standards and reports that are general in nature
- Policies and Procedures
  - Addresses the people and process aspects of an effective security program (OPERATION)
- System
  - address the technology related aspects of security (INTEGRATION)
- Component
  - Focuses on the security-related procedural and technical requirements related to products/components (DEVELOPMENT)



SEC PAT

ISA/IEC 62443 - Tier 4

SECPAT

Concepts – Security Levels (4-2)

- 62443 defines **Security Levels** (**SLs**), based on the protection provided against threats that are characterized as per the table below.
- For a component, the SL defines its ***capability to provide a certain level of protection*** *when it is properly integrated and configured, without additional or compensating countermeasures.*

LEVEL	TYPE OF VIOLATION	MEANS USED	RESOURCES USED	SKILLS	MOTIVATION
SL1	CASUAL OR COINCIDENTAL	-	-	-	-
SL2	INTENTIONAL	SIMPLE	LOW	GENERIC	LOW
SL3	INTENTIONAL	SOPHISTICATED	MODERATE	IACS-SPECIFIC	MODERATE
SL4	INTENTIONAL	SOPHISTICATED	EXTENDED	IACS-SPECIFIC	HIGH

SEC PAT

62443-4-2 – Foundational Requirements

- Identification and Access Control (IAC)
  - Control access to selected devices, information or both to protect against unauthorized interrogation of the device or information.
- Use Control (UC)
  - Control use of selected devices, information or both to protect against unauthorized operation of the device or use of information.
- System Integrity (SI)
  - Ensure the integrity of data on selected communication channels to protect against unauthorized changes.
- Data Confidentiality (DC)
  - Ensure the confidentiality of data on selected communication channels to protect against eavesdropping.
- Restrict Data Flow (RDF)
  - Restrict the flow of data on communication channels to protect against the publication of information to unauthorized sources.
- Timely Response to Event (TRE)
  - Respond to security violations by notifying the proper authority, reporting needed forensic evidence of the violation, and automatically taking timely corrective action in mission critical or safety critical situations.
- Resource Availability (RA)
  - Ensure the availability of all network resources to protect against denial of service attacks.

SEC PAT

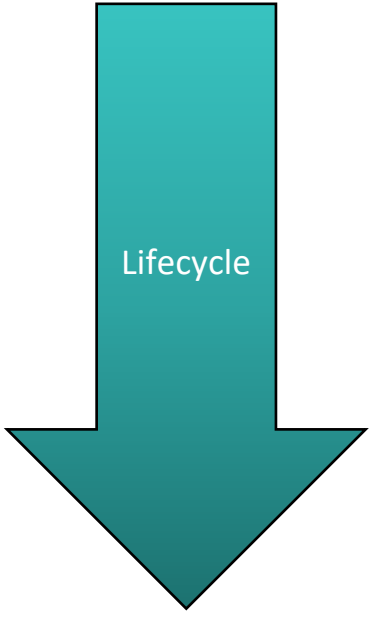
Concepts – Maturity Levels (4-1)

LEVEL		DESCRIPTION
ML1	Initial	The supplier performs product development in an **ad-hoc** and **not fully documented** manner. As a result, **consistency across projects and repeatability** of processes may not be possible.
ML2	Managed	The supplier has the capability to manage the development according to **written policies**. The supplier also has evidence that **the personnel** who performs the process **has the expertise, are trained and/or follows written procedures**. However, the supplier does **not yet have experience** developing products according to these policies and procedure.
ML3	Defined	**The performance of the supplier can be shown to be repeatable** across the supplier's organization. The processes have been practiced and **evidence exists** to demonstrate that this has occurred.
ML4/ ML5	Quantitatively Managed/Improving/ Optimizing	Using suitable **process metrics**, the product supplier controls the effectiveness and performance of the product and demonstrates **continuous improvement** in these areas.

SEC PAT

62443-4-1 – Practices

1. Security management
2. Specification of security requirements
3. Secure by design
4. Secure implementation
5. Security verification and validation testing
6. Management of security-related issues
7. Security update management
8. Security guidelines



Headache?!?

SECPAT

What Security Pattern can do for you

- Support for gap analysis between product and certification
- Aids in **technical discussions with the selected certification body**
- Provide tools for covering security gaps:
  - Secure firmware upgrade procedures
  - Continuous vulnerability monitoring
  - ....
- Bring strong and certified security to your IIoT System

...we are the **first** Italian Cybersecurity Company certified for

IEC 62443-4-1:2018

SEC PAT

Thank you!

hello@securitypattern.com

Bonus slides!

IoT – SUM:
Security Update and Monitoring

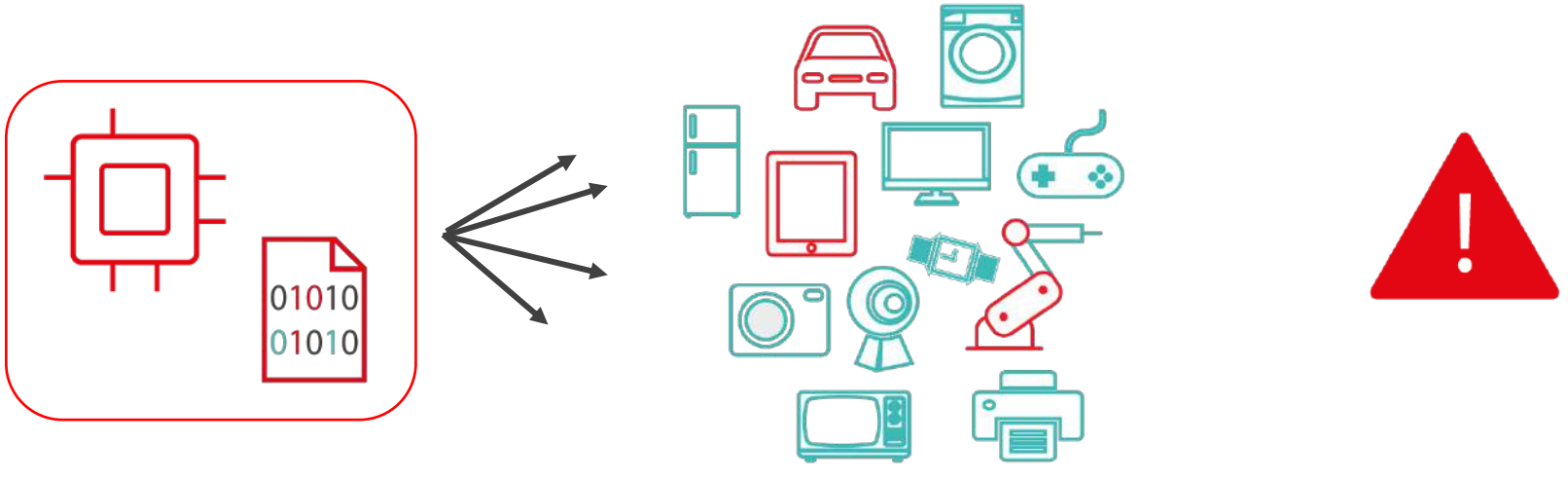
A new feature of IoT Secure Suite®

SECPAT

IoT® SECURE SUITE

Component updates and vulnerabilities

- Monitoring component updates and vulnerability notifications can be somehow complex



IoT Secure Suite® - SUM

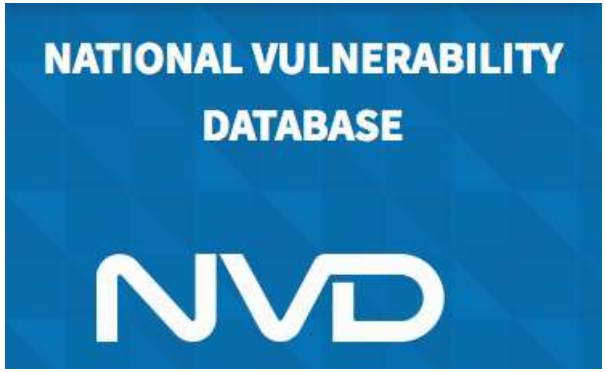
- That's why we released **IoT - SUM**:
  IoT - SUM (**S**ecurity **U**pdate and **M**onitoring) is a sum of tools for the monitoring of component's security update and for the management of vulnerability notifications

Easy monitoring with IoT - SUM

- IoT-SUM allows an easy monitoring of all the emerging vulnerabilities of every component of your IoT device

What we care about

- What we care about:
  - 1. Continuous monitoring on NVD, CVE and release notes on SW stack and system components
  - 2. Customer care oriented vulnerability notification service



Need more?

- We can also provide support for vulnerability mitigation strategies

Thank you!

hello@securitypattern.com