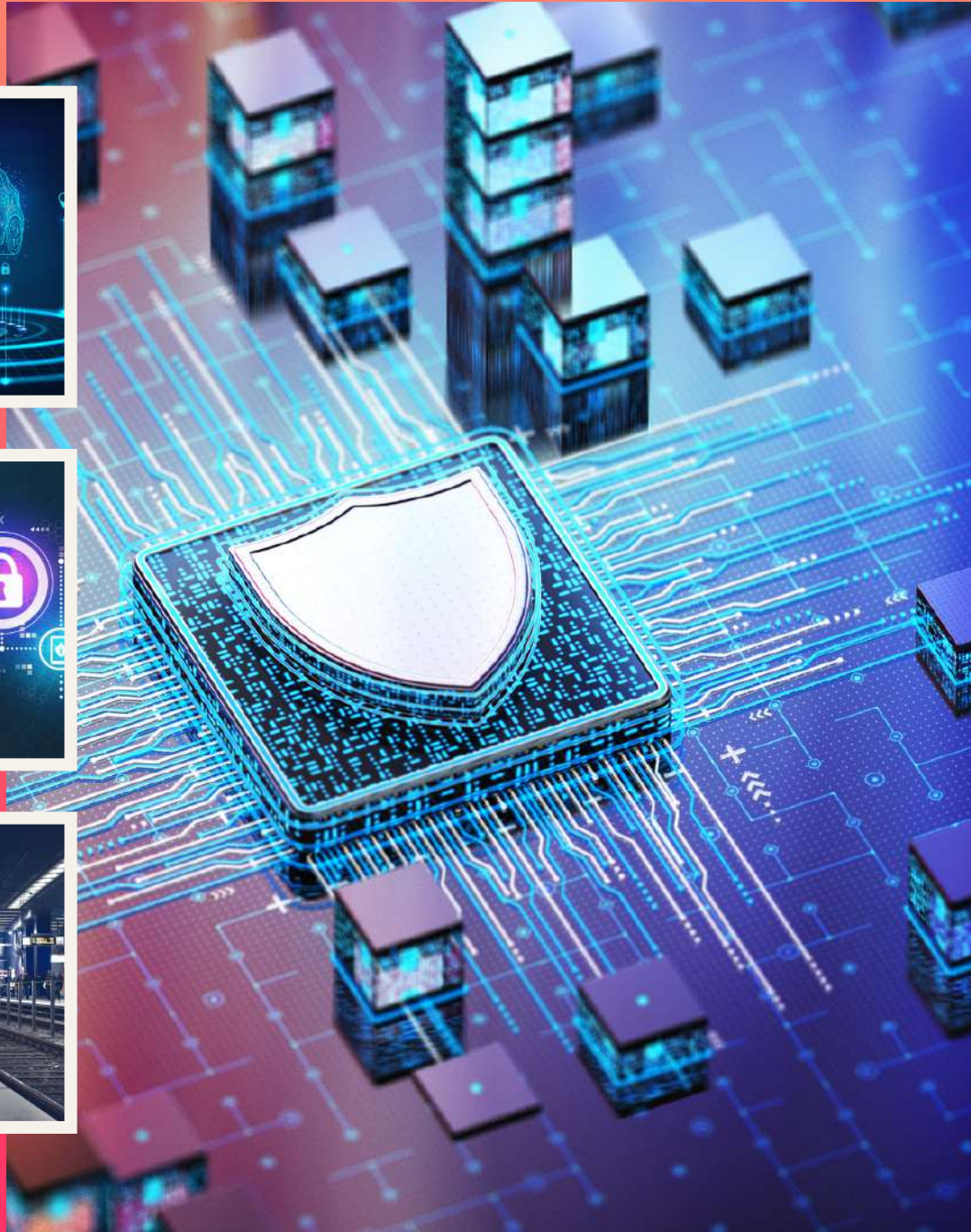


SECURE YOUR FUTURE



# SERMA ACADEMY

TRAINING COURSES 2024

# ABOUT SERMA GROUP

Founded in 1991, SERMA Group is an independent French expert, a unique contact for the reliability and security of products, systems and data.

Specialized in sectors with high environmental constraints, SERMA is characterized by its culture of technical excellence and its network of experts.

## Expert in Electronics, Energy, Cybersecurity and Telecoms technologies.

Through its various subsidiaries, the SERMA Group is involved throughout the product life cycle, from R&D and design to maintenance in operational conditions.

The Group has several laboratories for electronics, materials and cybersecurity expertise, engineering offices and various test platforms (components, boards, equipment, power electronics, electric motors, batteries, safety).

With 1,300 employees and almost 10,000 expert expertises per year carried out in our laboratories, SERMA is a recognized expert for many key accounts in all sectors of activity.

The Group has grown through numerous investments, both in terms of resources and external growth, in the fields of auditing, consulting, design, testing, expertise and, more broadly, understanding technologies.



Discover SERMA in video !

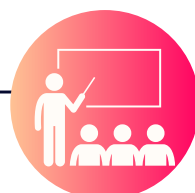


# OUR TRAININGS

SERMA supports you in strengthening and developing your know-how and thoses of your teams.



**500**  
trainees  
trained  
each year



Nearly  
**100**  
training  
courses  
every year



More than  
**40**  
catalog  
training



**25**  
expert  
trainers

**Qualiopi**  
processus certifié  
RÉPUBLIQUE FRANÇAISE

Our training courses  
are Qualiopi certified.

Our professional training courses are available both **face-to-face** and **remotely**: **practical** or **theoretical**, **predefined** or **customized**, **inter** or **intra-company**, in **French** or **English**, our training courses are driven by our teams whose daily experience in the field in all business sectors makes them benchmarks in their respective fields.



### ON SERMA PREMISES

We are at your disposal to set up **training courses adapted to your needs** in terms of date, place, programme or content.



### IN-COMPANY

Sessions are planned in our catalogue and delivered **throughout France**.



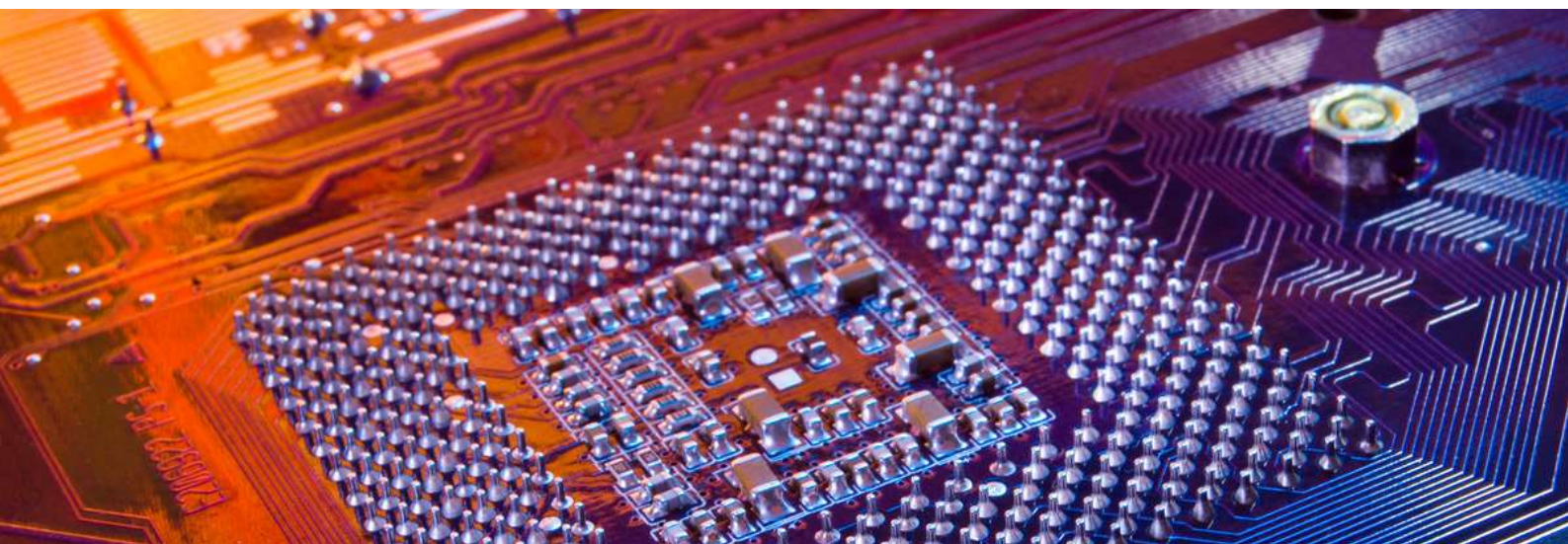
### REMOTE LEARNING

**Streaming** or **live**, online training is available for training courses that take place over 1 to 2 days maximum.



### CUSTOMISED

We accompany you in the transformation of your company by creating solutions with you that are **as close as possible to your needs**.



# Our training sites.

Our inter-company training courses take place at our various sites throughout France.

In-house or customized training can take place on your premises anywhere in France and around the world.



# Enrolment conditions and process

SERMA Technologies is registered under the no. 75 33 11 38 933.  
This registration is not equivalent to government certification.

**Registration and information requests** can be made to Gwenola BOIREAU :

- **By phone:** +33 (0)5 57 26 29 92
- **By email :** formation@serma.com
- **On our website** [www.serma.com/formation](http://www.serma.com/formation)

Enrolment is official once the enrolment agreement is received, after a 10 day legal withdrawal window and at least 15 days before the scheduled start of the course.

**Enrolment fees include** 1 person's access to the course, documentary materials, lunch and coffee breaks.

**Enrolment fees do not include** transportation costs and accommodation costs for course participants.

Enrolment in one of our training courses implies acceptance of all our conditions and terms of payment. No verbal agreements that are not confirmed by email can be taken into account.

## Terms of payment

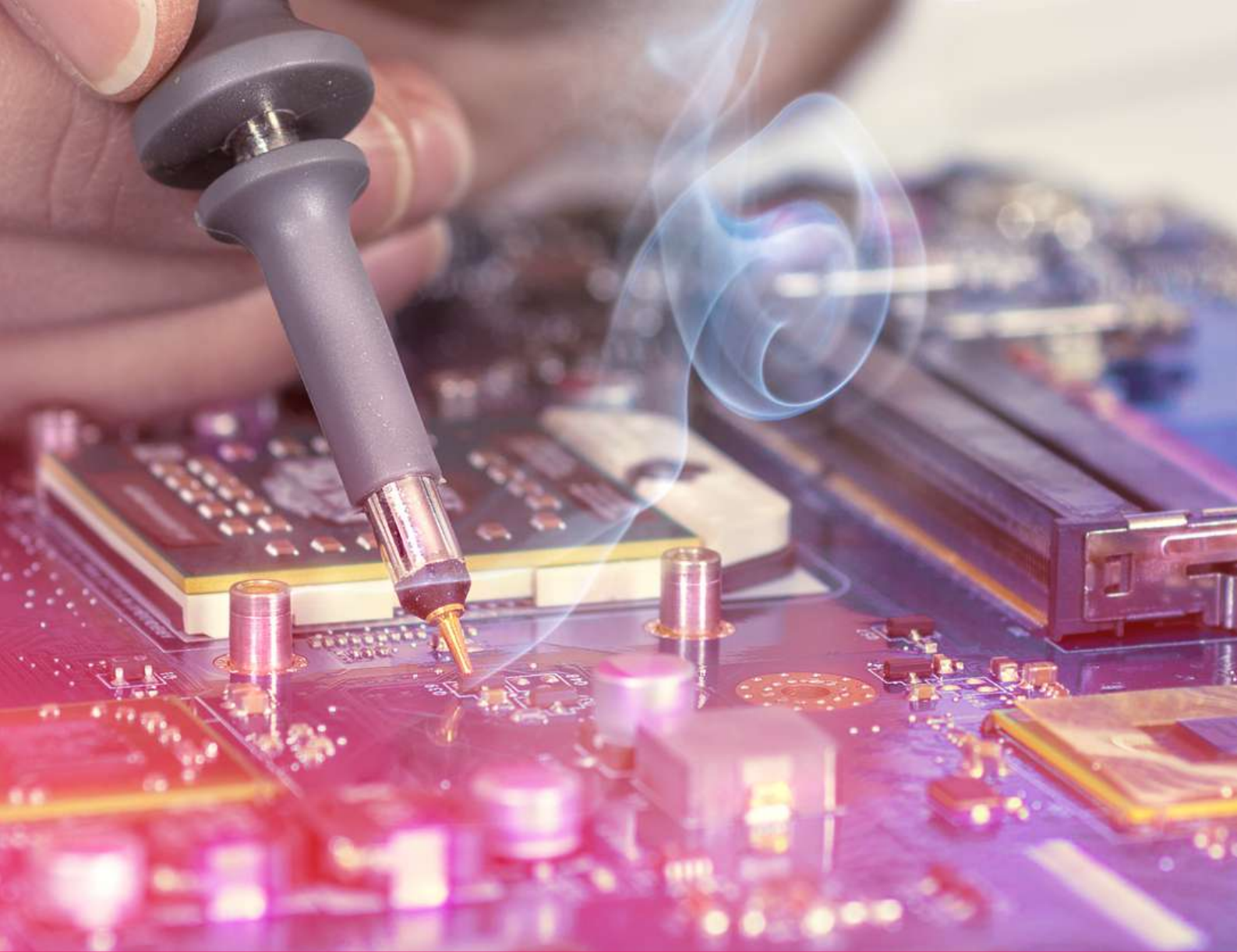
- **By cheque:** Made out to SERMA Technologies for the total cost including tax indicated on the invoice.

- **By bank tranfer:**

Bank	Counter code	Account number	Key	Currency
10 057	19012	003886501	80	EUR

## Accessibility

For all requests or for information concerning disabilities, please contact our disability reference person : Gwenola BOIREAU, formation@serma.com, +33 (0)5 57 26 29 92.



# Course postponement

In the event that the minimum number of participants is not reached and in order to better balance the organisation of groups, SERMA Technologies reserves the right to postpone a session no later than two weeks before its scheduled start date.

## **Cancellation of a session:**

- Cancellation by SERMA Technologies: In the event of a course postponement, SERMA Technologies promises to refund any fees already paid.
- Cancellation by the participant: Any enrolment cancellation not communicated to SERMA Technologies in writing at least 10 days before the start of the course will result in a penalty fee of 30% of the course fee (including current VAT).


A participant can be replaced at any time by another person from the same company for the same session, without extra fees, providing that SERMA is notified of the replacement before the start of the course.



## Stay informed

Find out more about our training courses on our website:

<http://www.serma.com/formations>

To keep up to date with our latest news and make sure you don't miss out any of our training courses, follow us on .



# SUMMARY

## **CYBERSECURITY**

Cybersecurity of embedded systems and connected objects.....	1
Cybersecurity of industrial systems IEC-62443.....	4

# CYBERSECURITY OF EMBEDDED SYSTEMS AND CONNECTED OBJECTS

Understanding hardware/software attacks and how to protect against them



## DATES & LOCATIONS

- May 14 to 16 – Paris
- Oct. 8 au 10 – Pessac

## DURATION

- 3 days

## PRICE

2 700€

## PREREQUISITES

No experience in IT security required. However, some knowledge of electronics or embedded software is desirable.

Equipment provided: The electronic and computer equipment required for the exercises will be provided to participants on site:

- Full HD screen with HDMI port
- Keyboard and mouse
- Pre-prepared Raspberry Pi
- Hardsplit with training board
- Radio analysis tools...

## TARGET AUDIENCE

This course is aimed at people interested in security aspects related to hardware or embedded systems. Electronics enthusiasts and professionals, as well as IT security professionals (developers, architects, integrators, hardware designers, project managers).

## OBJECTIVES

The aim of this training course is to understand the security weaknesses of embedded systems, master the attack techniques used by hackers so as to know how to limit the impact, learn how to secure embedded systems right from the design phase and understand the vulnerabilities so as to be able to limit the risks.

## INSTRUCTOR

Expert in embedded cybersecurity.

## TEACHING METHODS

- PowerPoint presentation
- Use of the Hardsplit IoT testing tool to carry out a hardware intrusion testing exercise
- Interactive Web platform (Klaxoon)
- Practical scenario for attacking/defending a mini-drone

## ASSESSMENT METHODS

Assessments at the beginning and end of the course, quizzes, etc.

## ENROLMENT DEADLINE

5 working days before the course start date (if financed by OPCO).

## SANCTION

A training certificate complying with the provisions of Article L. 6353-1 paragraph 2 is issued to the trainee.

**PROGRAM** ↓

## PROGRAMME

### UNDERSTAND THE BASICS OF HARDWARE HACKING

- Understand the historical context of attacks on connected objects
- Review vulnerabilities and their offensive and defensive aspects
- Know the fundamentals of electronics
- Take information from a target (component fingerprint)

### HOW DO HACKERS GAIN ACCESS TO HARDWARE?

- Present the tools and methods available for auditing a product
- Extract sensitive data with auditing tools (HardSploit)
- Acquire electronic signals, tools and demonstration

### HOW TO ACCESS THE SOFTWARE

- Present the different types of architecture (Microcontroller, FPGA), and the different direct accesses to the software via input and output interfaces (JTAG / SWD, I2C, SPI, UART, RF band ISM, etc.).
- Firmware access via various interfaces

### ATTACKS ON A SPECIFIC EMBEDDED SYSTEM, THE CONNECTED OBJECT (IOT)

- Carry out a complete audit applied to our vulnerable embedded system:
  - Identify electronic components
  - Acquire electronic signals
  - Intercept and analyze electronic signals with HardSploit
  - Modify and extract firmware via JTAG debug functions with HardSploit
  - Fuzz external interfaces to detect basic embedded vulnerabilities
  - Exploit vulnerabilities (buffer overflow) during a hardware security audit

## HOW TO SECURE YOUR HARDWARE?

- Discover cryptography and the different ways of securing your system and communications.
- Understand secure design and the notion of development cycles (SDLC)
- Understand hardware security best practices to limit risks
- Limiting JTAG access and software vulnerabilities at the embedded level

## HACKING WITH SDR TECHNOLOGY

- Learn SDR audit methodology (capture, analysis, exploitation with radio software)
- Use of tools (GQRX, GNU Radio, etc.)
- Reverse-engineer a wireless protocol from radio emissions captured in the air (wireless communication of an LED panel).

## "CAPTURE THE DRONE" EXERCISE

- Present a practical scenario for attacking/defending a mini drone
- Defend your drone and attack others using the tools and methods learned during training

# CYBERSECURITY OF INDUSTRIAL SYSTEMS IEC-62443

Understanding the standard to secure your architecture

4



## DATES & LOCATIONS

- May 28 to 30 – Paris
- Nov. 5 to 7 – Toulouse

## DURATION

- 3 days

## PRICE

2 700€

### PREREQUISITES

No industrial safety experience required. However, knowledge of industrial systems and some notions of IT, electronics and embedded software are desirable.

- A PC / MAC with Teams installed and unrestricted access to the Internet.

If remote :

- Stable Internet access via Ethernet or Wi-Fi with a decent bandwidth (1.2 Mb/s minimum downstream is recommended).

### TARGET AUDIENCE

This course is aimed at people interested in the design aspects of industrial architecture. Electronics enthusiasts and professionals, as well as IT security professionals (developers, architects, integrators, hardware designers, project managers).

### OBJECTIVES

This training course aims to raise awareness among system and product architects of the cybersecurity concerns, issues, constraints and challenges that can impact their current responsibilities, deliverables and day-to-day work.

### INSTRUCTOR

Expert in industrial cybersecurity.

### TEACHING METHODS

- Projected PowerPoint presentation
- Interactive web platform (Klaxoon)
- Practical attack/defense scenario on a connected mini-factory

### ASSESSMENT METHODS

Assessments at the beginning and end of the course, quizzes, etc.

### ENROLMENT DEADLINE

5 working days before the course start date (if financed by OPCO).

### SANCTION

A training certificate complying with the provisions of Article L. 6353-1 paragraph 2 is issued to the trainee.

**PROGRAM** 

## PROGRAMME

### INTRODUCTION AND SAFETY STANDARDS

- Introduction with key concepts and differences between IT and OT environments
- Threat overview and industrial cybersecurity risk analysis
- Introduction to IEC 62443 methodology and risk assessment
- Practical workshops on the definition of a SuC (System under consideration) and risk assessment according to IEC 62443
- Key concepts of IEC 62443 (zones, conduits and risk analysis methodologies)
- Defense-in-depth and the different layers of security (organizational, physical, perimeter)
- Demonstration: access system security, using Mifare technology as an example

### NETWORK SECURITY AND CRYPTOLOGY

- System security and basic network security principles
- Demonstration of a brute-force attack on a WPA2 network
- Introduction to cryptology: presentation of key concepts (symmetric and asymmetric encryption, hash, salt and pepper)
- Demonstration of how to exploit a vulnerability in precompiled Python files containing secrets

### PRODUCT SECURITY AND SECURE ARCHITECTURE

- Secure Software Lifecycle (SDLC) and best practices for secure software development
- Host and application security
- Demonstration of vulnerabilities affecting poorly protected USB ports with personnel unaware of attacks from seemingly innocuous devices.
- Demonstration of a replay attack using exploits on a bulletin board.
- Data security
- Practical workshops on detailed risk assessment, risk estimation and definition of security levels according to IEC 62443.
- Methods for identifying and dealing with vulnerabilities
- Presentation of best practices for designing a robust and secure architecture

## DAY 1

### INTRODUCTION

- Introducing SERMA

### CYBERSECURITY IN THE INDUSTRIAL WORLD

- Understanding cybersecurity in an industrial context
- Threats and attack methodologies
- IT / OT divergence and convergence

### ISA/IEC 62443 STANDARD

- Understanding the concepts of the standard
- Risk assessment process
- Initial assessment of detailed risks
- Risk acceptance and comparison

### WORKSHOPS

- WS1 - Define the system under consideration
- WS2 - Perform initial risk assessment
- WS3 - Partition Zones and Conduits

## DAY 2

### ISA/IEC 62443 STANDARD

- Detailed risk assessment process

### DEFENSE IN DEPTH

- Systems - Physical security
- Systems - Perimeter security
- Systems - Internal network security

## DEMONSTRATION

- Classic Mifare case
- Brute force WPA2 attack and ARP spoofing
- Crypto: poorly implemented encryption

## CRYPTOGRAPHY

- Symmetric and asymmetric
- Certificate and PKI (Public Key Infrastructure)
- Hash function with salt and pepper

## WORKSHOPS

- WS4 - Detailed risk assessment (1/2) - Threat scenarios

## DAY 3

### ISA/IEC 62443 STANDARD

- Secure product development lifecycle
- Fundamental requirements

### DEFENSE IN DEPTH

- Product - Host security
- Product - Application security
- Product - Data security

### DEMONSTRATION

- Rubber Ducky - USB attack
- Radio frequency - Replay attack

### WORKSHOPS

- WS5 - Detailed risk assessment (2/2) - Risk estimation
- WS6 - Definition of security levels
- WS7 - Specification of cybersecurity requirements

### VULNERABILITY DETAILS

- MCS, CVE & CVSS