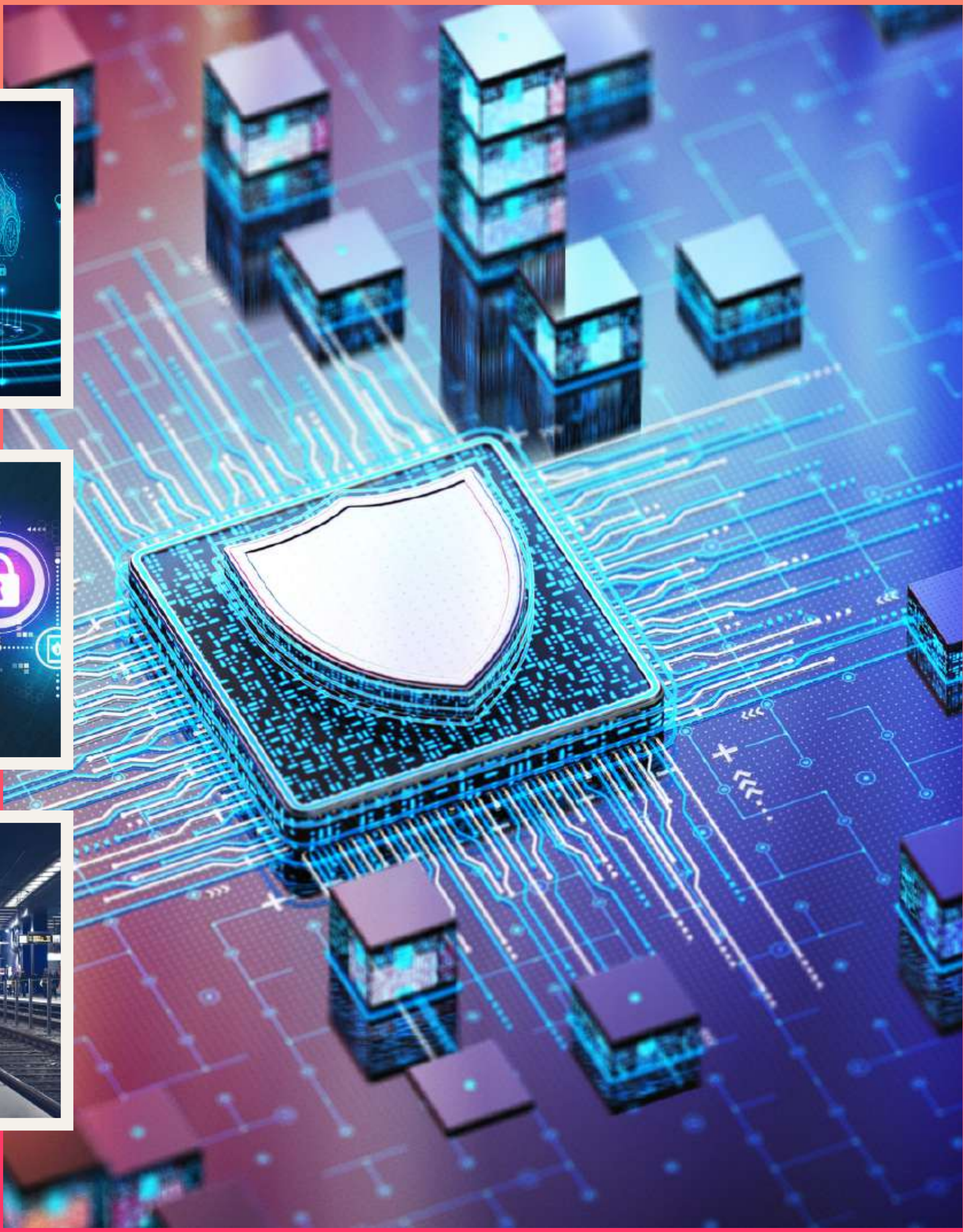
SECURE YOUR FUTURE



SERMA ACADEMY

TRAINING COURSES 2024

SERMA GROUP

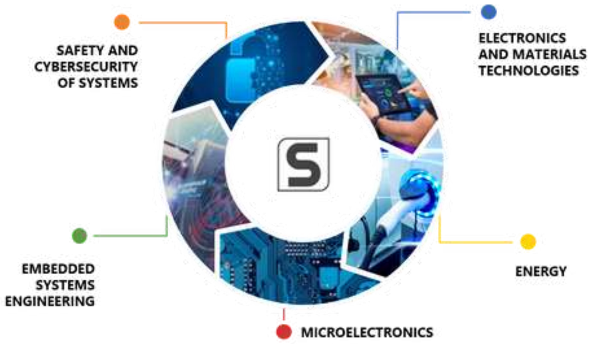
ABOUT SERMA GROUP

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.


SAFETY AND CYBERSECURITY OF SYSTEMS
ELECTRONICS AND MATERIALS TECHNOLOGIES
ENERGY
MICROELECTRONICS
EMBEDDED SYSTEMS ENGINEERING

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

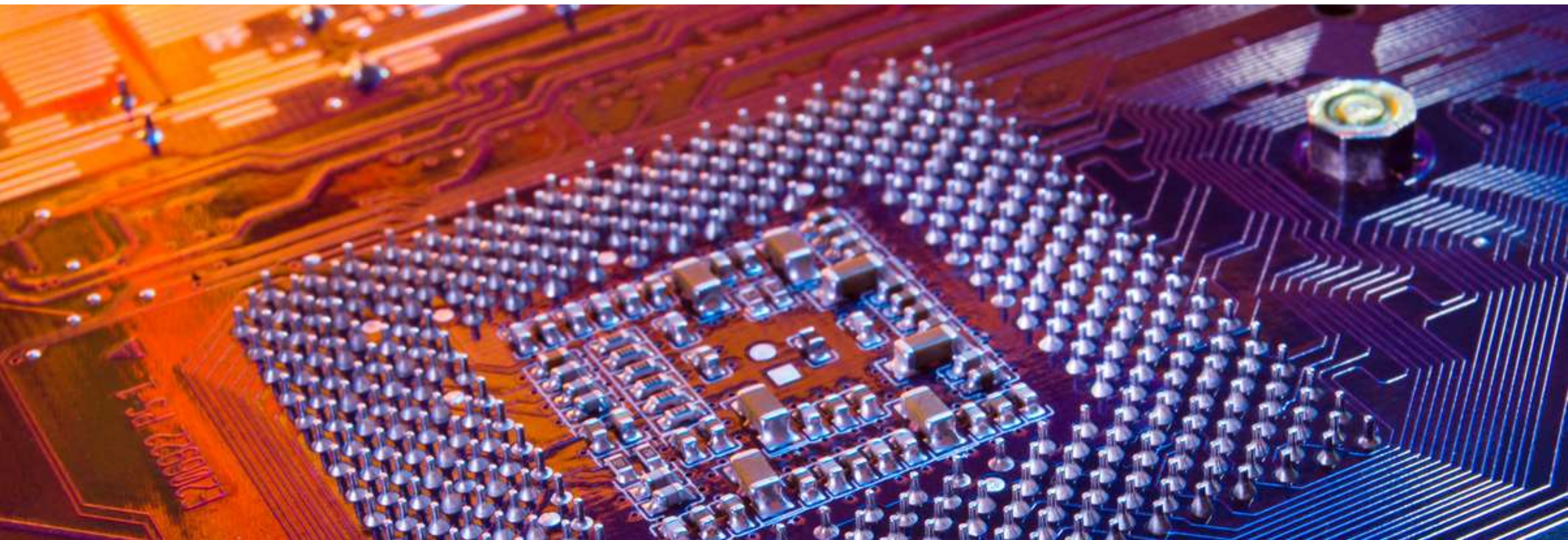
Sessions are planned in our catalogue and delivered **throughout France**.

REMOTE LEARNING

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

CUSTOMISED

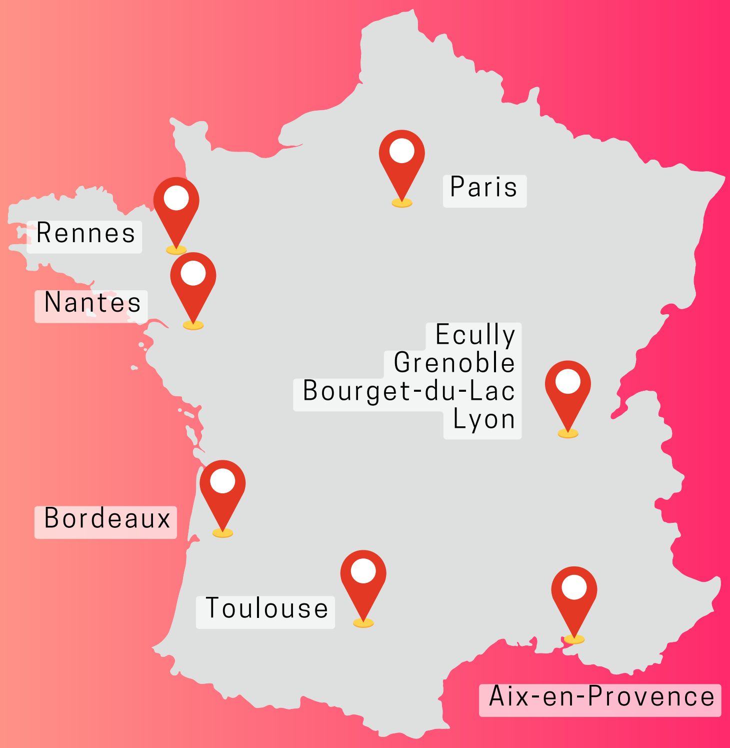
We accompany you in the transformation of your company by creating solutions with you that are **as close as possible to your needs.**



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** https://www.serma.com/en/training/training-courses/

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.

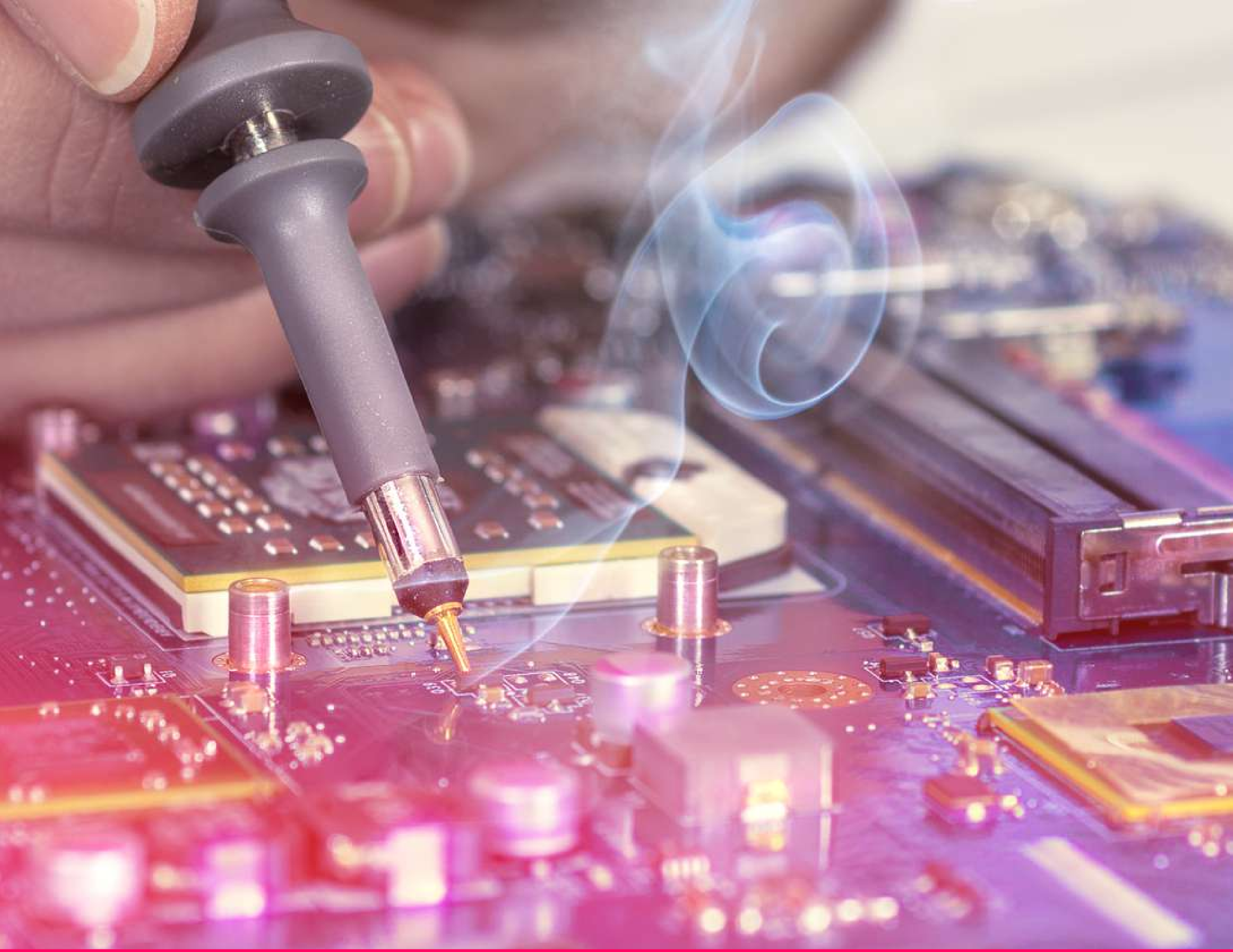
Terms of payment

- **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 in .

SUMMARY

CYBERSECURITY

Cybersecurity and Compliance IoT RED Directive..1
Cybersecurity and automotive compliance UN R155 & ISO 21434...3
Cybersecurity and railway compliance TS 50701...5
Cybersecurity of embedded systems and connected devices...8
Web Application Cybersecurity - OWASP Top 10:2021...11
Cybersecurity of industrial systems IEC-62443...14

CYBERSECURITY AND COMPLIANCE IOT DIRECTIVE RED

Introduction to Cybersecurity and Application of ETSI EN 303 645

DURATION

- 2 days

PRICE

On request

PREREQUISITES

No experience in in-car safety is required. However, some knowledge of automotive infrastructure is desirable. If remote :
• Stable internet access via Ethernet or Wi-Fi with a good data rate (1.2 Mb/s minimum downstream is recommended).
• A PC / MAC with the Teams tool installed and unrestricted access to the internet.

TARGET AUDIENCE

TThis training is intended for individuals working in the field of connected devices, particularly those involved in projects that need to comply with the new RED directive. It can be delivered to an audience without prior knowledge of cybersecurity.

OBJECTIVES

The objective of this training is, initially, to instill the basics and fundamental principles of cybersecurity and then to present the ETSI EN 303 645 standard, its implementation guide ETSI TR 103 621, and the assessment methodology ETSI TS 103 701. This is aimed at preparing you thoroughly for the certification of your product

INSTRUCTOR

Expert in IoT and embedded cybersecurity

TEACHING METHODS

- PowerPoint presentation
- Interactive web platform (Klaxoon)

ASSESSMENT METHODS

Evaluation at the beginning and end of the course, quiz...

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

PROGRAM

DAY 1

INTRODUCTION TO CYBERSECURITY

- Why cybersecurity?
- “Internet of Things”
- Practical: Define the architecture of a connected biometric lock

CYBERSECURITY FUNDAMENTALS

- The triforce of protection criteria
- New technologies, new threats

CYBERSECURITY RISKS

- Cybersecurity market
- Security mechanisms
- Practical: Define the attack surface of a connected biometric lock

CYBERSECURITY BY DESIGN

- Case studies
- 12 principles of cyber security

THE RED DIRECTIVE

- Legal, regulatory and standards aspects
- EN 18031-1: Protection of networks 3(3)(d)
- EN 18031-2: Protection of personal data and privacy 3(3)(e)
- EN 18031-3: Protection against fraud 3(3)(f)
- Practical: Identify potential vulnerabilities in a connected biometric lock

DAY 2

ETSI STANDARD EN 303 645

- Scope of application
- The 13+1 requirements of the standard
- Practical: Define the provisions applying to a connected biometric lock

ETSI TR 103 621 IMPLEMENTATION GUIDE

- Risk analysis and security assessment
- Secure Development Life Cycle (SDLC)
- Proposed implementations

ETSI TS 103 701 EVALUATION SPECIFICATIONS

- How the assessment works
- Implementation Conformance Statement (ICS)
- Implementation eXtra Information for Testing (IXIT)
- Practical: Prepare the evaluation file for a connected biometric lock

FIND OUT MORE

- NIST 8425
- ioXt certification
- GSMA Evaluation
- PSA Certified Scheme
- SESIP Scheme

PROGRAM

CYBERSECURITY AND AUTOMOTIVE COMPLIANCE UN R155 & ISO 21434

Understanding the stakes to implement it better

DURATION

- 2 days

PRICE

On request

PREREQUISITES

No experience in in-car safety is required. However, some knowledge of automotive infrastructure is desirable. If remote :
• Stable internet access via Ethernet or Wi-Fi with a good data rate (1.2 Mb/s minimum downstream is recommended).
• A PC / MAC with the Teams tool installed and unrestricted access to the internet.

TARGET AUDIENCE

This course targets people interested in cybersecurity issues related to the automotive domain. It is aimed at professionals involved in one or more stages of the automotive systems life cycle, as well as developers, architects, integrators, designers, project managers or management in the field.

OBJECTIVES

This training aims to understand how to carry out a coherent and effective safety policy in the automotive field. The objective is to understand and become aware through the ISO/SAE 21434 standard of what is :
• A cyber security policy, specific rules and processes
• Establishing and maintaining a cyber security culture (continuous improvement)
• Risk management and assessment
• Integration of cybersecurity within the life cycle phases

INSTRUCTOR

Expert in automotive cybersecurity

TEACHING METHODS

- PowerPoint presentation
- Interactive web platform (Klaxoon)

ASSESSMENT METHODS

Evaluation at the beginning and end of the course, quiz...

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

PROGRAM

CONTEXT OF CYBERSECURITY

- Definitions
- Background review
- Vehicle networks
- The attack surface
- Legal/regulatory aspects
- Protecting data
- Protection criteria
- Security & Cybersecurity
- New technologies

FUNDAMENTALS OF CYBERSECURITY

- Cybersecurity risk
- Cybersecurity market
- Cybersecurity by design

UN REGULATION 155

- Introduction
- Setting up a CSMS
- Application for approval

THE ISO/SAE 21434 STANDARD

- Introduction / Definitions
- Organisational CS management
- Project-based CS management
- Distributed CS activities
- Continuous CS activities
- Concept phase
- Risk analysis
- Product development
- CS validation
- Production
- Operation and maintenance
- Decommissioning

CYBERSECURITY AND COMPLIANCE RAILWAY TS 50701

Understanding the stakes to implement it better

DURATION

- 2 days

PRICE

On request

PREREQUISITES

No experience in in-car safety is required. However, some knowledge of automotive infrastructure is desirable. If remote :

• Stable internet access via Ethernet or Wi-Fi with a good data rate (1.2 Mb/s minimum downstream is recommended).

• A PC / MAC with the Teams tool installed and unrestricted access to the internet.

TARGET AUDIENCE

This course is aimed at people working in the railway environment and in particular those involved in projects including digital aspects and automated data processing systems. It can be given to people with no prior knowledge of cybersecurity or from the world of railway safety.

OBJECTIVES

The objective of this training is first to inculcate the basics and fundamental principles of cyber security and then to develop the Technical Specification 50701 specific to cyber security in railway projects.

INSTRUCTOR

Expert in railway cybersecurity

TEACHING METHODS

- PowerPoint presentation
- Interactive web platform (Klaxoon)

ASSESSMENT METHODS

Evaluation at the beginning and end of the course, quiz...

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

PROGRAM

INTRODUCTION TO CYBERSECURITY

- Vocabulary and definition
- Understanding the need and how it changes over time
- The notion of "attack surface"

LEGAL, REGULATORY, AND NORMATIVE ASPECTS

- The different organizations
- NIS 2 Directive
- Initiatives at the European and international levels

FUNDAMENTALS OF CYBERSECURITY

- Security, safety and cyber security
- How to protect the data
- Value of our data

CYBERSECURITY RISK

- Definitions and concepts
- New technologies, new threats
- Risk analysis

THE CYBERSECURITY MARKET

- The price of data
- Bug bounty

CYBERSECURITY BY DESIGN

- Case study
- 12 cybersecurity principles

PROGRAM

TS 50701

- TS 50701, what, who, how?
- Modelling and mapping
- Life cycle of a system
- Cybersecurity activities during a cybersecurity life cycle
  - Concept
  - Definition of a system
  - Simple and detailed risk analysis
  - Specifications
  - Cybersecurity architecture
  - Integration
  - Validation & Acceptance
  - Operation, maintenance and monitoring
  - Decommissioning

CYBERSECURITY OF EMBEDDED SYSTEMS AND CONNECTED DEVICES

Understanding hardware/software attacks and how to protect against them

DURATION

- 3 days

PRICE

On request

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
- Hardsploit 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 Hardsploit 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 ↓

PROGRAM

UNDERSTAND THE BASICS OF HARDWARE HACKING

- Understand the historical context of attacks on connected device
- 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 DEVICE (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

PROGRAM

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

WEB APPLICATION CYBERSECURITY OWASP TOP 10:2021

Discovering popular attacks to better guard against them

DURATION

- 2 days

PRICE

On request

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 web cybersecuity

TEACHING METHODS

- Projected PowerPoint presentation
- Interactive web platform (Klaxoon)
- Practical scenario of an attack on a vulnerable WEB application

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 ↓

PROGRAM

INTRODUCTION TO CYBERSECURITY

- Vocabulary and Definitions
- Understanding the need and its evolution over time
- The concept of 'attack surface'

FRAMEWORKS

- OWASP Top 10 Presentation
- CWE Top 25 Presentation

VULNERABILITY ECOSYSTEME

- CVE: Common Vulnerability Enumeration
- CVSS: Common Vulnerability Scoring System
- Find and report a vulnerability

A01:2021-FAULTY ACCESS CONTROL

- Presentation of Vulnerability Category
- Exercise/Demo
- Remediation/Tooling

A02:2021-CRYPTOGRAPHIC FAILURE

- Presentation of Vulnerability Category
- Exercise/Demo
- Remediation/Tooling

A03:2021-INJECTION

- Presentation of Vulnerability Category
- Exercise/Demo
- Remediation/Tooling

PROGRAM ↓

A04:2021-INSECURE DESIGN

- Presentation of Vulnerability Category
- Exercise/Demo
- Remediation/Tooling

A05:2021-SECURITY MISCONFIGURATION

- Presentation of Vulnerability Category
- Exercise/Demo
- Remediation/Tooling

A06:2021-VULNERABLE AND OBSOLETE COMPONENTS

- Presentation of Vulnerability Category
- Exercise/Demo
- Remediation/Tooling

A07:2021-FAILED IDENTIFICATION AND AUTHENTIFICATION

- Presentation of Vulnerability Category
- Exercise/Demo
- Remediation/Tooling

A08:2021-DATA AND SOFTWARE INTEGRITY DEFICIENCY

- Presentation of Vulnerability Category
- Exercise/Demo
- Remediation/Tooling

A09:2021-INSUFFICIENT MONITORING AND LOGGING

- Presentation of Vulnerability Category
- Exercise/Demo
- Remediation/Tooling

A10:2021-SERVER_SIDE REQUEST FORGERY

- Presentation of Vulnerability Category
- Exercise/Demo
- Remediation/Tooling

CYBERSECURITY OF INDUSTRIAL SYSTEMS IEC-62443

Understanding the standard to secure your architecture

DURATION

- 2 days

PRICE

On request

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

PROGRAM

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

PROGRAM ↓

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

PROGRAM ↓

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

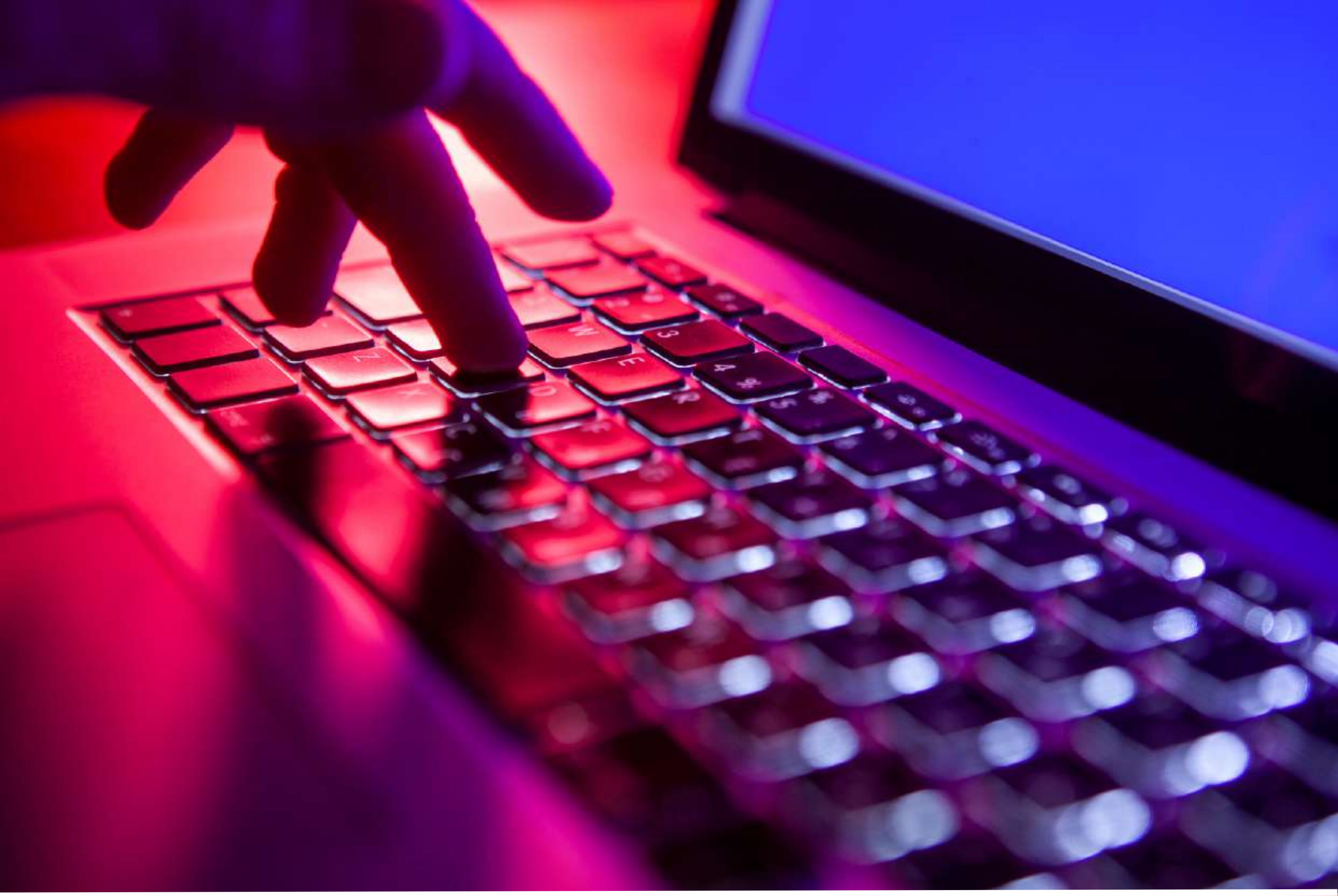
- Rubber Ducky - USB attack
- Radio frequency - Replay attack

WORKSHOPS

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

VULNERABILITY DETAILS

- MCS, CVE & CVSS



ABOUT SERMA SAFETY AND SECURITY

SERMA Safety and Security supports its clients in ensuring the security and operational safety of products and systems in the fields of IoT, embedded systems, industry, or information systems. The company possesses a unique expertise that allows it to intervene across the entire value chain of systems: from IoT products through network and system infrastructure to internal and external applications.

SERMA Safety and Security is recognized for its technical excellence, earning it numerous qualifications and certifications such as CESTI, PASSI RGS, SESIP, FIPS, SBMP, and more.

In addition to these activities, the company offers training programs covering its entire scope of expertise in operational safety and cybersecurity. With a presence on 8 sites in France, the company has more than 230 employees and generates a turnover of over 35 million euros. It is a subsidiary of the SERMA Group.