

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 !

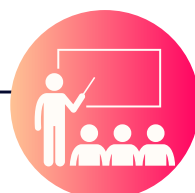


OUR TRAININGS

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



500
trainees
trained
each year



Nearly
100
training
courses
every year



Nearly
50
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**.



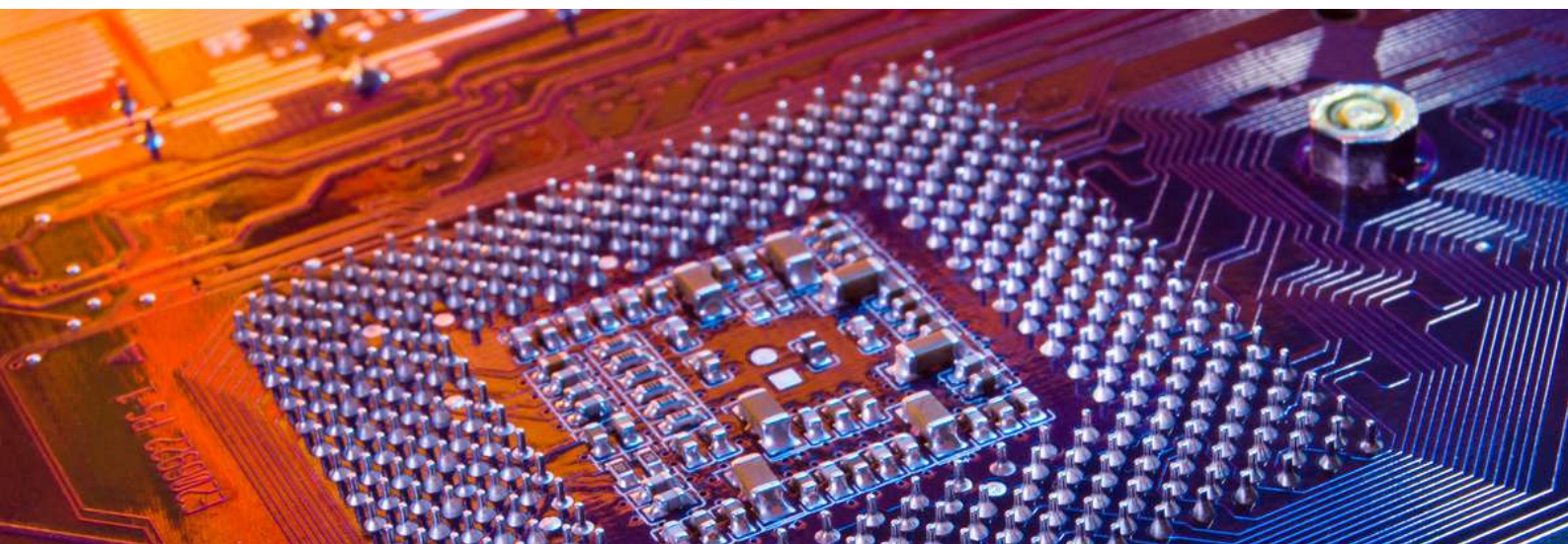
REMOTE LEARNING

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

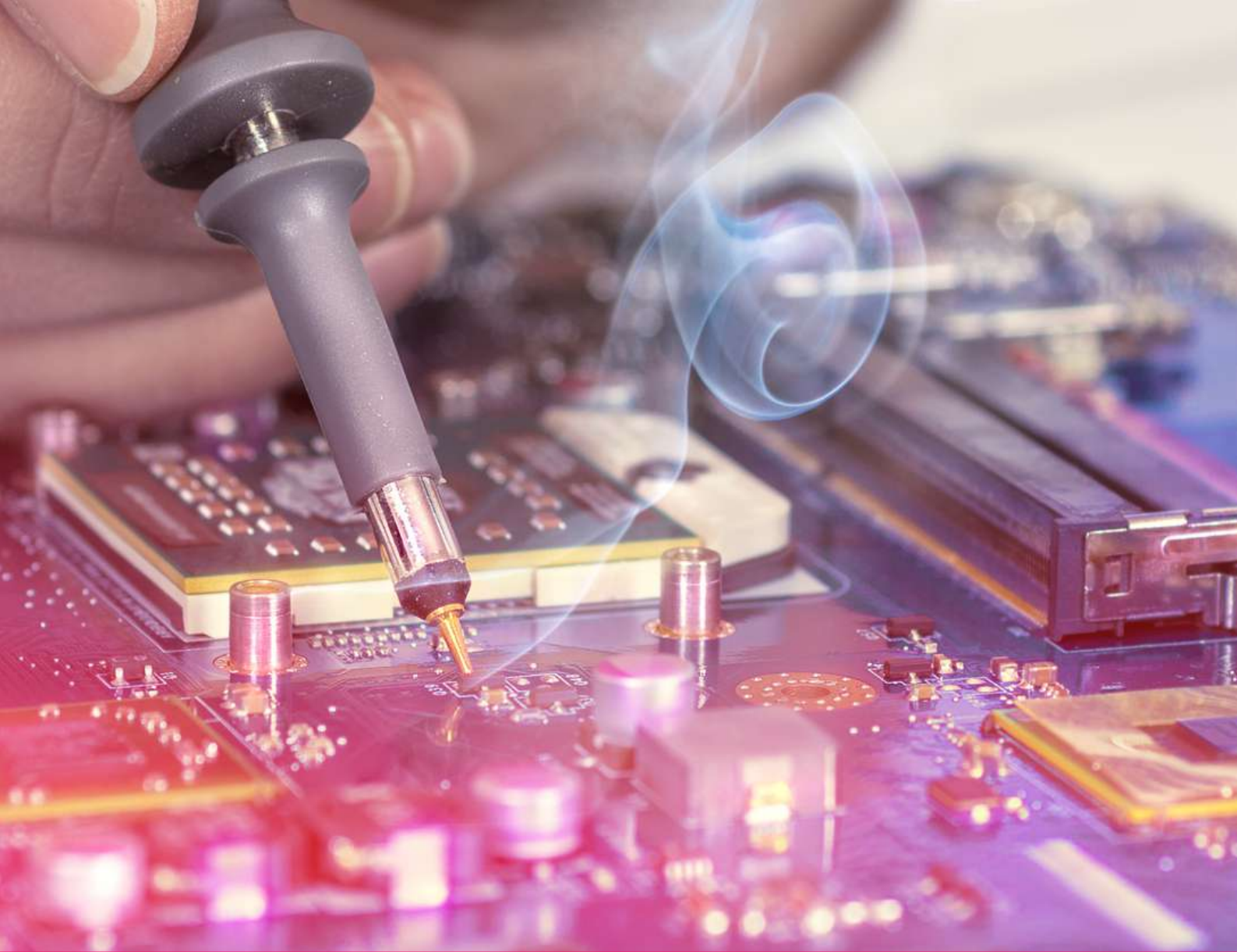
- **By cheque:** Made out to SERMA Technologies for the total cost including tax indicated on the invoice.

- **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.



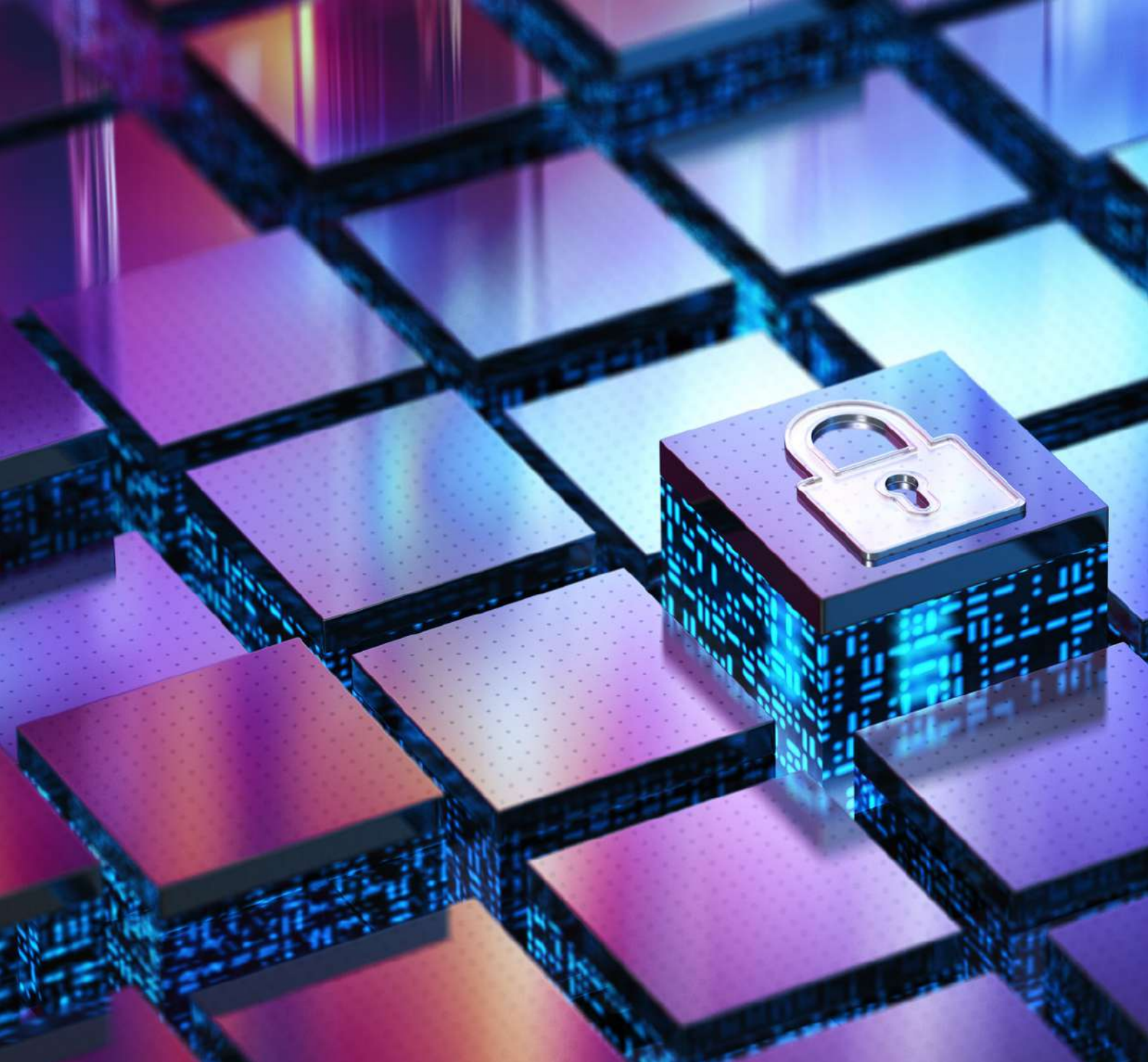
Course postponement

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  .

SUMMARY

ELECTRONICS TECHNOLOGIES

Passive component technology.....	1
Active component technology.....	3
Failure mechanisms.....	5
Failure analysis (RCA) of electronic circuit boards.....	7

ELECTRONIC BOARDS AND SYSTEMS

Introduction to circuit board assembly.....	10
Circuit board assembly.....	12
Circuit board assembly line audit.....	15
Electronic assembly reliability.....	18
Electronic components qualifications.....	21
Electronic systems qualifications (applied to the automotive industry).....	23
Reliability and electronics power.....	26

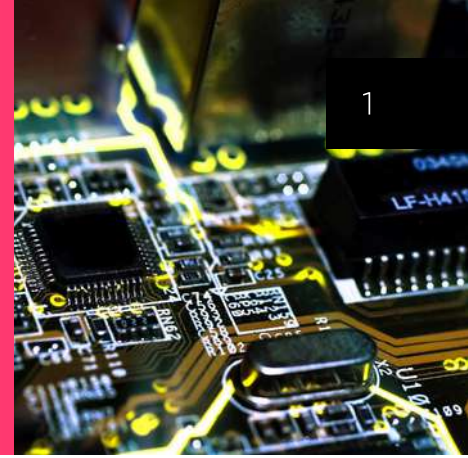
HYDROGEN

Hydrogen systems awareness.....	28
Liquid Hydrogen Basics.....	30
H2 fundamentals - FC focus.....	32
Operability and Maintenance.....	34
H2 fundamentals - Bipolar plates focus.....	36

CYBERSECURITY

Cybersecurity and Compliance IoT RED Directive.....	38
Cybersecurity and automotive compliance UN R155 & ISO 21434.....	40
Cybersecurity and railway compliance TS 50701.....	42
Cybersecurity of embedded systems and connected devices.....	45
Web Application Cybersecurity - OWASP Top 10:2021.....	48
Cybersecurity of industrial systems IEC-62443.....	51

PASSIVE COMPONENT TECHNOLOGY



DATES & LOCATIONS

- March 12 – Pessac
- October 15 – Pessac

DURATION

- 1 day

PRICE

750 €

PREREQUISITES

Basic knowledge of passive component technology.

TARGET AUDIENCE

Quality managers, laboratory staff, design office, purchasing, etc.

OBJECTIVE

Understand the technologies covered in the course.

INSTRUCTOR

Laboratory Skills Department Head.

TEACHING METHODS

Projection and printed copies of Powerpoint presentations, practical case studies, exercises, situational examples, theoretical examples, video materials, etc.

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

CAPACITORS

- General topics, critical electrical settings, different types of capacitors, applications, ranges, choosing a type
- Ceramic capacitors: manufacturing procedures, typical failure modes, risks during assembly (film)
- Tantalum capacitors: same as above
- Other capacitors: electrolytic, aluminium, films, etc.

FIXED RESISTORS

- General information, electrical parameters, different types of resistors, applications.
- Thick film resistors: manufacturing principles, typical failure modes, assembly risks.
- Thin film resistors: manufacturing principles, typical failure modes, assembly risks.
- Wire wound resistors: manufacturing principles, typical failure modes, assembly risks.

QUARTZ RESONATORS

- General information, electrical parameters, applications.
- Technology, construction
- Manufacturing process
- Main faults and mechanisms

SELF (INDUCTORS)

- General information, electrical parameters, applications.
- Technology, construction
- Manufacturing process
- Main faults and mechanisms

ACTIVE COMPONENT TECHNOLOGY

3

DATES & LOCATIONS

- March 13 – Pessac
- October 16 – Pessac

DURATION

- 1 day

PRICE

750 €

PREREQUISITES

Basic knowledge of active component technology.

TARGET AUDIENCE

Quality managers, project managers, laboratory and design office staff.

OBJECTIVES

Understand the principles of chip fabrication and encapsulation, and grasp failure analysis through concerted case study examples.

INSTRUCTOR

Engineer or project manager.

TEACHING METHODS

Projection and printed copies of Powerpoint presentations, practical case studies, exercises, situational examples, theoretical examples, video materials, etc.

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

CHIP MANUFACTURING PRINCIPLES

- Introduction
- Materials (semiconductors, conductors and insulators)
- Manufacturing processes
- Technologies
 - CMOS process
 - Bipolar process
 - BICMOS process
- Examples of manufacturing defects

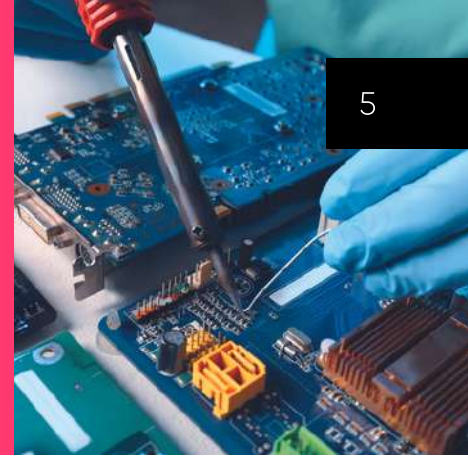
PACKAGING

- General aspects of packaging
- Assembly technology
 - Wafer cutting
 - Chip attachment
 - Wired cabling
- Encapsulation

FAILURE ANALYSIS

- Failure analysis goal and steps on active circuits
- Techniques and methods
- Examples of manufacturing defects on active components (diodes, transistors, ICs and optoelectronic components ...)

FAILURE MECHANISMS



5

DATES & LOCATIONS

- May 15 to 16 - Pessac
- Sept. 17 to 18 - Remote
- Nov. 5 to 6 - Pessac
- Dec. 3 to 4 - Remote

DURATION

- 2 days

PRICE

1 460 €

PREREQUISITES

Basic knowledge of general electronics.

TARGET AUDIENCE

Quality or technical manager, field analysis/SAV engineer.

OBJECTIVES

Understand the weaknesses of passive, discrete and active components through their main failure mechanisms. Concrete cases of failure and some techniques for revealing them are presented.

INSTRUCTOR

Electronic component/board reliability engineer.

TEACHING METHODS

Projection and printed copies of Powerpoint presentations, practical case studies, exercises, situational examples, theoretical examples, video materials, etc.

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

Definition and methodological introduction

Introduction of the technology (materials involved) for each component family

Presentation of the main weaknesses and ways of revealing them for each component family

Application exercise

Quizzes/Assessment of acquired knowledge

DAY 1

Component family concerned :

- Printed circuit boards (PCB)
- Solder: Sn/Pb, SAC
- Resistors: thick film, thin film
- Capacitors: Ceramic, Tantalum, Electrolytic, Film
- Quartz: PTH and SMD
- Coils

DAY 2

Component family concerned :

- Discrete semiconductors: diodes, LEDs and MOS transistors
- Active semiconductors: Si integrated circuits
- Discrete and integrated circuit packages
- Optocouplers

FAILURE ANALYSIS (RCA) OF ELECTRONIC CIRCUIT BOARDS



7

DATES & LOCATIONS

- Fev. 6 to 7 – Remote
- June 4 to 5 - Pessac

DURATION

- 2 days

PRICE

1 460 €

PREREQUISITES

Basic knowledge of general electronics.

TARGET AUDIENCE

Quality or technical managers, field/SAV analysis engineers or those faced with a need to improve electronic board reliability.

OBJECTIVE

Learn a practical method for troubleshooting electronic boards.

INSTRUCTOR

Process engineers, project managers.

TEACHING METHODS

Projection and printed copies of Powerpoint presentations, practical case studies, exercises, situational examples, theoretical examples, video materials, etc.

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

DEFINITIONS

- Defect, failure mode, degradation, failure mechanism, failure cause, root cause

INTRODUCTION TO CAUSE-FINDING STEPS

- Situation analysis: description of the fault and the context in which it occurred
- Fault confirmation/characterization
- Locating the fault at board and component level
- Observation/expertise of the fault
- Search for and weighting of failure mechanism
- Search and weighting of failure causes

FAULT DESCRIPTION AND CONTEXT OF OCCURRENCE

- Product and fault description
- The product: its design, manufacturing process, history, etc.
- The fault: facts (data), conditions of occurrence, feedback, etc.
- Methods: QOQC, 5W, IS-IS NOT, Graph, ...
- Examples

METHODS FOR LOCATING/CHARACTERIZING FAULTS ON A MAP

- Failure modes and their special cases (intermittence, instability, combustion, etc.)
- Location tools (objectives, limits and risks of altering the fault)
- Introduction to families of degradation mechanisms
- Fault characterization methods
- Consistency analysis of results

INTRODUCTION TO FAILURE MECHANISMS

FORMALIZING ASSUMPTIONS AND WEIGHTING CRITERIA (OBJECTIVES, METHODS, MEANS, LIMITS)

- Application example

ELECTRONIC BOARD FAILURE CAUSES AND WEIGHTING

- Reminder of definition: what is / is not a cause
- Review of electronic board failure cause families
- Hypothesis review methods: Brainstorming, Fault tree, Cause-effect diagram, Mind mapping, ...
- Weighting tools and criteria (objectives, methods, means, limits) :
 - Experimental design
 - Laboratory expertise
 - Robustness testing
 - Manufacturing process audit
 - Field measurements
 - Expert opinion, etc.
- Example

CAUSE AND ROOT CAUSE OF ELECTRONIC BOARD FAILURE

MCQ AND CORRECTION

INTRODUCTION TO CIRCUIT BOARD ASSEMBLY

10



DURATION

- 0,5 day

TARIF

On request

PREREQUISITES

Knowledge of electronics.

TARGET AUDIENCE

Project manager, buyer, business coordinator, warehouseman, laboratory technician...

OBJECTIVES

- Define what an electronic board is and what it's made of
- Teach the basics of manufacturing processes
- Explain physical phenomena (soldering)
- Provide an overview of the trades involved, so you're familiar with common technical vocabulary.

INSTRUCTOR

Project Manager Engineer.

TEACHING METHODS

Projection and printed copies of Powerpoint presentations, practical case studies, exercises, situational examples, theoretical examples, video materials, etc.

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

OVERVIEW OF INDUSTRIAL ELECTRONICS

WHAT IS AN ELECTRONIC BOARD?

ENVIRONMENTAL CONSTRAINTS IN PRODUCTION

- MSL
- ESD
- Storage
- Handling

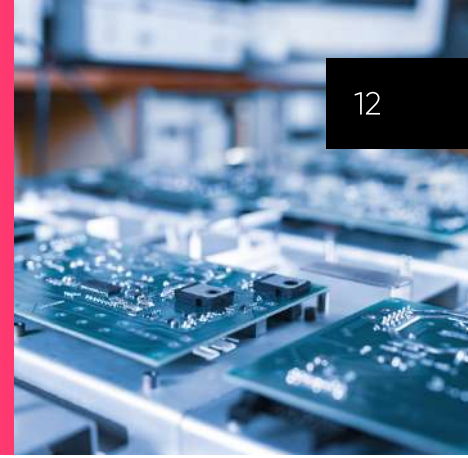
THE PRODUCTION OF AN ELECTRONIC BOARD

- Production and control equipment.

TESTING AN ELECTRONIC BOARD

- Electrical test and inspection equipment.

CIRCUIT BOARD ASSEMBLY



DATES & LOCATIONS

- March 12 to 14 - Toulouse
- Sept. 17 to 19 - Pessac

DURATION

- 3 jours

PRICE

2 160 €

PREREQUISITES

Basic knowledge of card assembly.

TARGET AUDIENCE

AQF quality engineers, product managers, auditors, project managers, engineers, assembly process technicians... This training course is specific to assemblers, and focuses on materials and process control.

OBJECTIVES

- Acquire the information required for the controlled implementation of assembly processes for electronic components.
- Assess the quality of assemblies by studying the various elements involved in the manufacture of the final product: printed circuits, hybrid circuits, components, leaded and lead-free soldering materials, bonding materials and others.
- Application skills: assembly (PTH, SMT), fluxing, soldering, profiling, packaging, storage, cleaning, etc.
- Control and failure analysis aspects, as well as essential rules to ensure process control.

INSTRUCTOR

Process Engineer Project Manager.

TEACHING METHODS

Projection and printed copies of Powerpoint presentations, practical case studies, exercises, situational examples, theoretical examples, video materials, etc.

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

- Industrial environment
- Reliability risks

SOLDERING

- Terminology and definitions: brazing, soldering, brazed joints, etc.
- Phase diagram (lead-tin)
- Lead/tin alloys used
- Lead-free solders
- Melting and reflowing
- Phases: morphologies and evolution
- Intermetallics
- Wettability
- Solder creams
- Impact of lead-free on components and alloys
- Backward process

PRINTED CIRCUIT BOARDS AND MAIN ELECTRONIC COMPONENTS

Printed circuit boards :

- Technologies: double-sided, multilayer
- Physical characteristics: coefficient of thermal expansion, buckling, T_g
- Metallurgical finishes of soldering surfaces
- Sensitivity to humidity

Electronic components :

- Capacitors
- Relays
- Quartz

Plastic-cased components:

- Pin termination materials, balls (LED, BGA, μ BGA and flip chip)
- Humidity sensitivity
- Non-destructive testing: visual, optical, acoustic and X-ray

MANAGING THE RISK OF ELECTROSTATIC DISCHARGE

- Definition
- Sensitive components
- EPA zone

ELECTRONIC BOARD ASSEMBLY LINE

- Process Flow
- Influence of board design on process choice
- Storage of electronic components and printed circuit boards
- Deposition methods: silkscreen, syringe
- Placement machines (transfer)
- Temperature profile and control (reflow)
- Manufacturing controls
- Through-hole components
- Press Fit
- Wave soldering
- Other brazing methods
- Troubleshooting
- Cleaning
- Test
- Varnish
- System integration
- Packaging

PROCESS CONTROL

- Machine and process qualification
- Control of influencing parameters
- Manpower and work instructions
- Capability
- Gage R&R
- Failure mechanisms

MAIN STANDARDS AND ACRONYMS

AUDIT DIGEST

Included in Day 3 if this training is given in Pessac:

Visit to a board assembly workshop (SMT, through-hole (PTH), manual soldering).

CIRCUIT BOARD ASSEMBLY LINE AUDIT

15



DATES & LOCATIONS

- May 22 to 23 - Pessac
- Nov. 19 to 20 - Remote

DURATION

- 2 days

PRICE

1 460 €

PREREQUISITES

Basic knowledge of electronics.

TARGET AUDIENCE

QAF quality engineers, product managers, assembly process technicians, auditors.

OBJECTIVES

Evaluate technical and organizational skills for those whose activities include visiting or auditing suppliers of assembled boards. This training is based on our long experience in auditing, our knowledge of assembly techniques and their failure mechanisms.

INSTRUCTOR

Process Engineer Project Manager.

TEACHING METHODS

Projection and printed copies of Powerpoint presentations, practical case studies, exercises, situational examples, theoretical examples, video materials, etc.

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

- Industrial environment
- Reliability issues

SOLDERING

- Soldering
- Lead solder
- Wettability
- Intermetallic
- Phase evolution
- RoHS and REACH
- Control
- Lead-free solder
- Leaded and lead-free solder
- Whiskers

PRINTED CIRCUIT BOARDS AND MAIN ELECTRONIC COMPONENTS

- Printed circuit boards
- Capacitors
- Quartz
- Plastic-cased components

ELECTROSTATIC DISCHARGES

- EOS and ESD
- Component sensitivity
- Workshop environment
- Transport of sensitive parts
- Checking fixtures

PCB ASSEMBLY LINE

- Process Flow
- SMD line
- Through-hole components (PTH) only
- 1-sided SMD components
- 1-sided SMD components + some PTHs
- Pin In Paste
- SMD components on 2 sides
- SMD and through-hole: mixed technology

INTRODUCTION TO PROCESS CONTROL

- Qualification
- Parameter controls
- SPC, CP, CPK, control chart

AUDIT TECHNIQUE

- General
- Preparation
- Organization
- Agenda
- Attitude
- On-line procedure

FINALIZING THE AUDIT

- Audit grid
- Wrap up

DESCRIPTION AND DETAILED AUDIT OF ASSEMBLY PROCESS STEPS

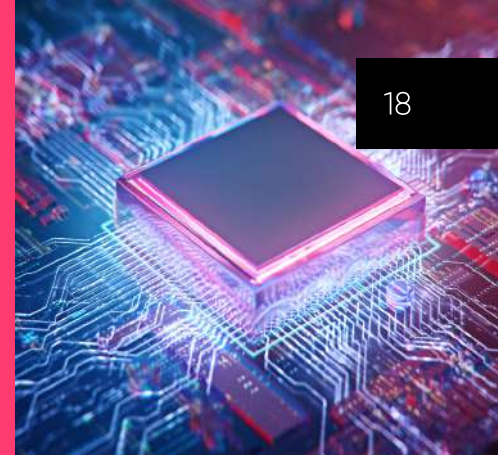
- Cleanliness and visual management
- Receiving and storage
- Screen printing
- Report
- Reflow
- Control
- Through-hole
- Wave soldering
- Other brazing methods
- Varnish
- Test
- System integration
- Packaging

ANNEXES

- Main standards and acronyms
- Audit digest

ELECTRONIC ASSEMBLY RELIABILITY

18



DATES & LOCATIONS

- Sept. 10 to 12 – Pessac
- Nov. 19 to 21 – Pessac

DURATION

- 3 days

PRICE

2 160€

PREREQUISITES

Level of experienced senior technician or engineer working on the quality or reliability of a product, either at the manufacturing or selection level.

TARGET AUDIENCE

Technical or design office manager, engineer or project manager, reliability manager.

OBJECTIVES

Learn how to make an electronic system reliable. The approach enables you to understand how to identify the product's life profile, carry out technological risk analyses in order to build a targeted risk removal plan (environmental tests accelerated by the use of mathematical models, robustness tests, component qualification, etc.).

INSTRUCTOR

Project Manager Engineer.

TEACHING METHODS

Projection and printed copies of Powerpoint presentations, practical case studies, exercises, situational examples, theoretical examples, video materials, etc.

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

- Reliability definitions
- Failure, failure mode and failure mechanism
- Abrupt (catalectic) and wear failure
- Example of failure mechanisms
- Resistance/stress theory

SOME MATHEMATICAL NOTIONS

- Failure rate function $l(t)$
- Evolution of failure rate over time (bathtub curve)
- MTBF, MTTF
- Use of statistical laws and their limitations :
 - Exponential
 - Weibull
- Sampling :
 - Ki^2
 - Binomial

OUR APPROACH: "RELIABILITY THROUGH TECHNOLOGY"

- Definition of product life profile
- Risk analysis (technologies versus life profile)
 - Components and technologies : AEC-Q-XXX, PPAP, aeronautics, space...
 - Design
 - Industrialization
- Robustness testing
 - HALT
 - Development and implementation of a test plan
- Durability testing
 - Acceleration laws (Arrhenius, Coffin Manson and Norris Landzberg, Hallberg Peck ...)
 - Building a test plan and sequencing tests
- Manufacturing process qualification
 - Process control
 - Supplier audit

BURN-IN

- Definition of burn-in
- HASS, HASA, ESS
- POS and SOS
- Burn-in effectiveness

CLASSICAL RELIABILITY ASSESSMENT METHODS

- Theoretical calculations (MIL-HDBK-217, IEC 62380, FIDES)
- Test methods (D0 160, EN 50155, ESA...)
- Field feedback (REX)

PRACTICAL EXERCISES ON A CASE STUDY

Throughout the training course, trainees are offered a number of exercises:

- Mathematical exercises (exponential, Weibull...)
- Life profile definition
- Technological risk analysis and industrialization
- Definition of a robustness plan
- Definition of a durability test plan (calculation of accelerated tests)

QUESTIONS/ANSWERS

ELECTRONIC COMPONENTS QUALIFICATIONS

21



DATES & LOCATIONS

- June 5 – Remote

DURATION

- 1 day

PRICE

750€

PREREQUISITES

Level of experienced senior technician or engineer working on the quality or reliability of a product, either at the manufacturing or selection level.

TARGET AUDIENCE

Technical or design office manager, engineer or project manager, reliability manager, test laboratory manager.

OBJECTIVES

- Understand the objectives of qualification testing of electronic boards and systems (automotive environment), from the theoretical aspects of defining tests to the practical aspects of carrying them out (good rules, reaction in the event of problems, drafting test reports, etc.).
- The main standards in force will be reviewed (ISO 16750, automotive manufacturers' standards, etc.). Mathematical aspects will be covered, on the one hand for calculating acceleration factors, and on the other, for calculating the number of samples required according to reliability objectives.

INSTRUCTOR

Engineer Project Manager.

TEACHING METHODS

Projection and printed copies of Powerpoint presentations, practical case studies, exercises, situational examples, theoretical examples, video materials, etc.

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

GENERAL INTRODUCTION

RAISING AWARENESS OF ELECTRONIC COMPONENT FAILURE MECHANISMS (TARGETED AT EXPECTATIONS)

- Links with qualification testing

BASIC CONCEPTS USEFUL FOR QUALIFICATION

- Reliability parameters and laws
- Typical tests (HTOL, TC, THB...)
- Acceleration factors (Arrhenius, Black, Coffin, Peck...)

QUALIFICATION METHODS AND STANDARDS (MORE OR LESS IN-DEPTH, DEPENDING ON REQUIREMENTS)

- Knowledge based vs Stress based
- JESD47 (industrial)
- MIL-STD
- ECSS (Spacial)
- AEC-Q (Automotive)
- JESD94 / JEP148 (electromigration example)

ELECTRONIC SYSTEMS QUALIFICATIONS (APPLIED TO THE AUTOMOTIVE INDUSTRY)



23

DURATION

- 2 days

PRICE

On request.

PREREQUISITES

Level of experienced senior technician or engineer working on the quality or reliability of components, either at the manufacturing or selection level.

TARGET AUDIENCE

Technical or design office manager, engineer or project manager, reliability manager, test technician, test laboratory manager.

OBJECTIVES

- Understand the objectives of component qualification testing, from the theoretical aspects of test definition (failure mechanisms, parameters and reliability laws) to the practical aspects of test execution (acceleration factors, sampling, etc.).
- Understand the main standards in force (MIL, JEDEC, AEC, ESCC, JESD, etc.).

INSTRUCTOR

Project Manager Engineer.

TEACHING METHODS

Projection and printed copies of Powerpoint presentations, practical case studies, exercises, situational examples, theoretical examples, video materials, etc.

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

- Reliability definitions
- Failure, failure mode and failure mechanism
- Abrupt (catalectic) and wear failure
- Example of failure mechanisms
- Resistance/stress theory

SOME MATHEMATICAL NOTIONS

- Failure rate function $I(t)$
- Evolution of failure rate over time (bathtub curve)
- MTBF, MTTF
- Use of statistical laws and their limitations :
- Exponential
- Weibull

ACCELERATION LAWS / BUILDING A TEST PLAN

- Acceleration laws (Arrhenius, Coffin Manson and Norris Landzberg, Hallberg Peck ...)
- Test plan construction and test sequencing
- Qualification of manufacturing processes

TEST PLAN DEFINITION METHOD

- Definition of product life profile
- Risk analysis (technologies versus life profile)
 - Components and technologies : PPAP...
 - Design
 - Industrialization
- Stress Based Testing (AEC Qxxx)
- Robustness testing
 - HALT
 - Development and implementation of a test plan
- Durability testing
- Review of the various tests proposed in the standards (definition and purpose of each type of test)
 - HTOL/THB/STORAGE/PC/TC/ESD/THB/T&H cyclic/mechanical tests, salt spray, etc.

SAMPLING

- Acceleration laws (Arrhenius, Coffin Manson and Norris Landzberg, Hallberg Peck ...)
- Building a test plan and sequencing tests
- Qualification of manufacturing processes

MSL AND ESD LEVELS

- MSL
- ESD

BURN-IN

- Definition
- Implementation (SOS, POS, surveillance, monitoring, etc.)

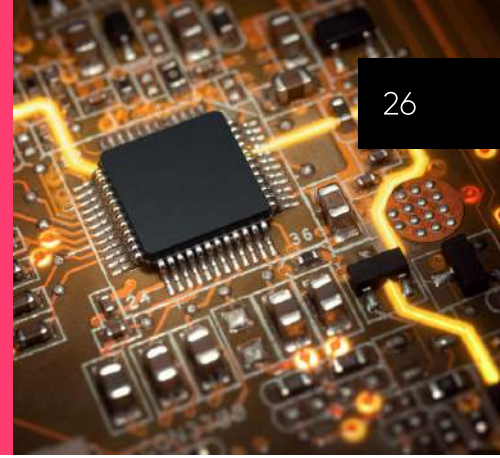
SYNTHESIS

AUTOMOTIVE FOCUS, REVIEW OF EXISTING STANDARDS (EXAMPLES)

- ISO 16750
- Test specifications of major automotive manufacturers

RELIABILITY AND ELECTRONICS POWER

26



DATES & LOCATIONS

- October 2 to 3 - Pessac

DURATION

- 2 days

PRICE

1460€

PREREQUISITES

Experienced technician or engineer with basic knowledge of electronics.

TARGET AUDIENCE

Experienced senior technician, engineer or project manager, technical or design office manager, quality or reliability manager.

OBJECTIVES

Know the technologies involved (diode, MOSFET, IGBT in Si, SiC and GaN) and learn a method for "reliability through technology" of a power module, from life profile to risk mitigation plan (performance, robustness, lifetime, process variability), via risk analysis (failure mechanisms).

INSTRUCTOR

Project Manager Engineer.

TEACHING METHODS

Projection and printed copies of Powerpoint presentations, practical case studies, exercises, situational examples, theoretical examples, video materials, etc.

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

- General information on power electronics (history, definitions)
- Scope of power modules covered in the course (6500V - 500A)

PRESENTATION OF POWER MODULE TECHNOLOGIES

- Chips
 - Diodes
 - MOSFET
 - IGBT
 - New SiC and GaN technologies
- Connectors
 - Chip top connectors (wires, ribbons, etc.)
 - Connections on the underside of chips and substrates (soldering, sintering, etc.)
 - Power connections (brazed, screwed pins, etc.)
- Substrates/Embases
 - Nature and characteristics of substrates (SMI, AL₂O₃, AlN, Si₃N₄, DBC, AMB, etc.)
 - Nature and characteristics of bases (Cu, AlSiC, etc.)

OUR "RELIABILIZATION THROUGH TECHNOLOGY" APPROACH

- Product life profile
- Risk analysis
 - Failure mechanisms (lifting of wires, delamination in solder joints, etc.)
- Risk elimination plan
 - Performance (standard / specification)
 - Automotive (AECQ, AQG-324...), aeronautics (DO), space (ESCC...), rail (IEC...), ...
- Robustness
 - Defining robustness
 - Building a test plan, sequencing tests
 - HALT example
- Service life
 - Review of tests and their acceleration laws (Arrhenius, Coffin Manson, etc.)
 - Building a test plan, sequencing tests
- Process variability
 - Process control
 - Supplier audit

HYDROGEN SYSTEMS AWARENESS

28



DURATION

- April 3 - Toulouse
- Sept. 18 - Remote
- Dec. 4 - Pessac

PRICE

On request

PREREQUISITES

No prerequisites, initial awareness-raising.

TARGET AUDIENCE

All audiences.

OBJECTIVE

Have an overview, a big picture of the hydrogen (H₂) value chain and H₂-based systems.

TEACHING METHODS

Projected Powerpoint presentation, discussion, project examples, video supports.

ASSESSMENT METHODS

Quiz at the beginning and end of the course

REGISTRATION DEADLINE

2 months.

ATTENDANCE CERTIFICATE

Issued to trainee (upon demand)

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

GENERAL PROPERTIES OF H₂

- Physical properties
- General implications (safety, systems, etc.)

HYDROGEN VALUE CHAIN

- Hydrogen production
- Industrial H₂ vs. energy H₂
- H₂ storage
- H₂ transport

ELECTROCHEMICAL SYSTEMS

- Introduction to the component: The fuel cell
- Presentations of fuel cell auxiliaries
- Electrolyzers - an introduction to common technologies

H₂ COMBUSTION - AN INTRODUCTION

- Combustion
- Examples of H₂
- Combustion-related phenomena

INITIATIVES, PROJECTS, DEMONSTRATORS

- Hydrogen gas
- Liquid hydrogen
- Combustion
- European, national, and private companies' initiatives

LIQUID HYDROGEN BASICS

30



DATES & LOCATIONS

TBD and France / Europe (on customer premises or by videoconference, as required)

DURATION

- 2 days

PRICE

On request

PREREQUISITES

Basic engineering knowledge: electrochemistry, thermodynamics, physics.

TARGET AUDIENCE

Engineers / Technicians

OBJECTIVE

Have an overview of cryogenics, the properties of liquid hydrogen and associated phenomena (phase change, liquefaction process etc.).

TEACHING METHODS

Projected Powerpoint presentation, discussion, project examples, video supports.

ASSESSMENT METHODS

Quizzes at the beginning and end of the course

REGISTRATION DEADLINE

2 months (France and Europe), 1 month if Toulouse.

ATTENDANCE CERTIFICATE

Issued to trainee (on request)

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

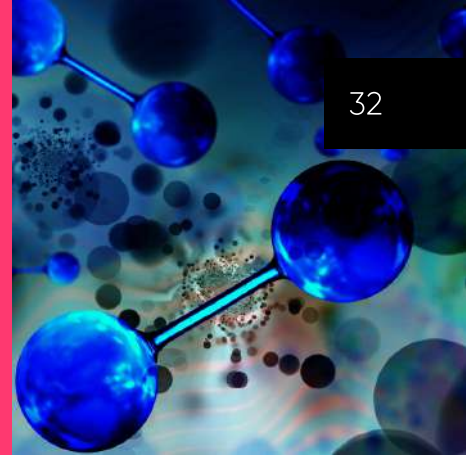
- General knowledge of liquid hydrogen: properties, liquefaction methods
- Cryogenic tanks - design challenges
- Cryogenic piping in aircraft
- Tank life cycle: filling, discharge, associated phenomena

DAY 2

- Tank life cycle: filling, discharge, associated phenomena
- The connection between the cryogenic tank and the propulsion system
- Safety aspects
- Questions, debriefing

H2 FUNDAMENTALS - FC FOCUS

32



DATES & LOCATIONS

TBD and France / Europe (on customer premises or by videoconference, as required)

DURATION

- 2 days

PRICE

On request

PREREQUISITES

Basic engineering knowledge: electrochemistry, thermodynamics, physics.

TARGET AUDIENCE

Engineers / Technicians

OBJECTIVE

Have a general overview of the hydrogen value chain and hydrogen-based systems, with a focus on the Fuel Cell (FC) system.

TEACHING METHODS

Projected Powerpoint presentation, discussion, project examples, video supports.

ASSESSMENT METHODS

Quizzes at the beginning and end of the course

REGISTRATION DEADLINE

2 months (France and Europe), 1 month if Toulouse.

ATTENDANCE CERTIFICATE

Issued to trainee (on request)

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
- Background: the hydrogen chain
- Aeronautical applications
- Introduction to the FC component
- Theoretical aspects of the FC – introduction 1st part

DAY 2

- Theoretical aspects of the FC – 2nd part
- The FC system
- General information on Liquid Hydrogen
- Hydrogen limits and safety aspects
- Question-and-answer session

OPERABILITY AND MAINTENANCE



DATES & LOCATIONS

Toulouse (Halle H2pulse at Francazal)

DURATION

- 3 days for 1 to 4 participants
- 4 days for 5 to 8 participants

PRICE

On request

PREREQUISITES

H2 fundamentals - FC focus (recommended)

TARGET AUDIENCE

Engineers / Technicians

OBJECTIVE

Introduction to the practical aspects of fuel cell system maintenance and operability. Practical sessions take place on the last day.

TEACHING METHODS

Powerpoint support for the practical part and test bench for the practical sessions.

ASSESSMENT METHODS

N/A (practice shows whether skills have been acquired or not).

REGISTRATION DEADLINE

2 months.

ATTENDANCE CERTIFICATE

Issued to trainee (on request)

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**DAY 1**

- Reminders on FC operations and composition
- FC characterization
- Aging of the FC
- FC diagnosis

DAY 2

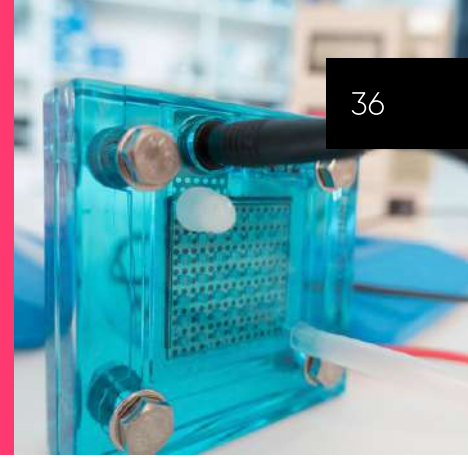
- Faults and ageing of the FC system
- FC system maintenance
- Questions, debriefing, practice preparation

DAY 3

- Facility visit
- Safety aspects
- Practice

FC FUNDAMENTALS - BIPOLAR PLATES FOCUS

36



DATES & LOCATIONS

TBD and France / Europe (on customer premises or by videoconference, as required)

DURATION

- 1 day

PRICE

On request

PREREQUISITES

H2 fundamentals - FC focus (recommended)

TARGET AUDIENCE

Engineers / Technicians

OBJECTIVE

Have an overview of the H2 fuel cell and the systems around the component, with a focus on bipolar plates and their relevance.

TEACHING METHODS

Projected Powerpoint presentation, discussions, theoretical examples of research studies, video support.

ASSESSMENT METHODS

Quizzes at the beginning and end of the course.

REGISTRATION DEADLINE

2 months (France and Europe), 1 month if Toulouse.

ATTENDANCE CERTIFICATE

Issued to trainee (upon request)

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
- Background: the hydrogen value chain
- Introduction to the component - the fuel cell (FC)
- Theoretical aspects of FC - introduction
- The FC system – Balance of Plant
- Bipolar plates: functions, design, manufacturing, ageing

CYBERSECURITY AND COMPLIANCE IOT DIRECTIVE RED

Introduction to Cybersecurity and Application of ETSI EN 303 645

38



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 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

CYBERSECURITY AND AUTOMOTIVE COMPLIANCE UN R155 & ISO 21434

Understanding the stakes to implement it better

40



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



42

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

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



45

DURATION

- 2 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
- 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 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 DEVICES (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

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 cybersecurity

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

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 AUTHENTICATION

- 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

51



DURATION

- 3 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 

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