CYBER SECURITY TRAINING & PERSONAL CERTIFICATION

IN DORTMUND 22 - 24 MAY 2019 (GERMAN)
IN MUNICH 02 - 04 JULY 2019
IN DORTMUND 15 - 17 OCTOBER 2019 (GERMAN)

MODULE CS1
Introduction Cyber Security in Industry

+

MODULE CS2A
CS2 – SAE J3061 Best Practices from the USA – Cyber Security for the Automotive Industry

+

MODULE CS2B
ISO/SAE CD 21434 Road vehicles – Cybersecurity engineering

→ Designation as **CACSP** Certified Automotive Cyber Security Professional (Automotive)

MODULE CS1
Introduction Cyber Security in Industry

+

MODULE CS3
Cyber Security for Industrial Automation and Control Systems

→ Designation as **CICSP** Certified Industry Cyber Security Professional (Industry)

CYBER SECURITY

Protect your assets and security-related systems against attacks and the potential threats posed by criminal actions with the IT Security Analysis Services from SGS-TÜV Saar.

EXPERIENCED STAFF OF TRAINERS

SGS-TÜV Saar is the first body world-wide to have been accredited for SAE J3061 and an active member of related standardization bodies, e.g., ISO 21434.

MODULAR TRAINING CONCEPT

Participation in Modules CS1, CS2a and CS2b, and CS1 and CS3, respectively, is required to take the CACSP and CICSP tests.

TRAINING SCHEDULE

The training sessions are held on two days (CACSP) and three days (CICSP) from 9 a.m. to 5 p.m.

OUR PERSONAL QUALIFICATION PROGRAMME

SGS-TÜV Saar as an accredited services provider offers you the opportunity to teach personnel in specialised Cyber Security knowledge and to qualify individuals as:

- CACSP – Personal Qualification Programme Cyber Security (Automotive)
- CICSP – Personal Qualification Programme Cyber Security (Industry)

These qualifications will expand your expertise in Cyber Security-relevant topics. As a company you will have the opportunity to have your staff independently qualified and to secure your specialised knowledge for the long term.

Your CACSP and CICSP qualifications will be valid for three years. Your CACSP or CICSP may be requalified for another three years by participating in an update workshop and successfully taking a test (short version).

SECURE YOUR PLACE NOW!

For all bookings received 6 weeks prior to the beginning of the training, we offer a 10% early bird discount.

SGS TÜV SAAR

SGS

CS0 – OVERVIEW CYBER SECURITY IN INDUSTRY

Our webinar provides a quick introduction to Cyber Security and gives an outlook on all further training modules. This will make it easier for you to decide in what areas you will have to take action in order to avoid future risks

Contents

- Motivation
- Presentation of Cyber Security concepts for:
  - Vehicles (SAE J3061 and ISO/SAE 21434)
  - Industrial automation and control systems (IEC 62443)

DATES AND ATTENDANCE FEE

18 March 2019, starts at 2:00 p.m. – conducted in German

03 June 2019, starts at 8:30 a.m. – conducted in English

03 June 2019, starts at 6 p.m. – conducted in English

30 September 2019, starts at 2:00 p.m. – conducted in German

Free webinar

CS1 – INTRODUCTION CYBER SECURITY IN INDUSTRY

Familiarise yourself in one day with the Cyber Security concepts and related terms and definitions, to get a good understanding of basic challenges and a fundamental preparation for the following modules. This includes an extract of attack generic types, example threats and a quick overview of cyber security standards and guidelines.

Contents

- Introduction to Cyber Security
- Key Definitions of Terms
- Example Threats
- Overview of Cyber Security Standards
  - SAE J3061
  - ISO/SAE CD 21434
  - IEC 62443

DATES AND ATTENDANCE FEE

22 May 2019 in Dortmund, Germany – conducted in German

02 July 2019 in Munich, Germany – conducted in English

15 October 2019 in Dortmund, Germany – conducted in German

598 euros (plus VAT)
538 euros (plus VAT) early bird rate*

*For all bookings received up until 6 weeks prior to the training

CS2A – SAE J3061 BEST PRACTICES FROM THE UNITED STATES – CYBER SECURITY FOR THE AUTOMOTIVE INDUSTRY

Gain an advantage by learning about the best practices from the United States. Find a way to implement Cyber Security requirements into practice by comparing your processes with those presented in our seminar. After this day you will have an overview of the key requirements and be fit for the future.

Contents

- Introduction to Cyber Security concepts for vehicles according to SAE J3061 (Cyber Security principles)
- Security management
- Security requirements for the product, HW and SW development process

DATES AND ATTENDANCE FEE

23 May 2019 in Dortmund, Germany – conducted in German

03 July 2019 in Munich, Germany – conducted in English

16 October 2019 in Dortmund, Germany – conducted in German

798 euros (plus VAT)
718 euros (plus VAT) early bird rate*

*For all bookings received up until 6 weeks prior to the training

VENUES

Holiday Inn München-Süd
Kistlerhofstraße 142
81379 Munich, Germany

Technologiezentrum Dortmund GmbH
Emil-Figge-Straße 76-80
D-44227 Dortmund

ADMINISTRATIVE

For all questions regarding the registration as well as the venue, please contact:

SGS-TÜV Saar GmbH
Hofmannstr. 50
81379 Munich, Germany
t +49 89 787475 -283/288
f +49 89 787475 -217
fs.training@sgs.com
www.sgs-tuev-saar.com/fs

For questions about Cyber Security, please contact:

SGS-TÜV Saar GmbH
Joseph-von-Fraunhofer Str. 13
44227 Dortmund, Germany
t +49 231 9742-7337
cybersecurity@sgs.com
www.sgs-tuev-saar.com/fs-training

ONLINE REGISTRATION

http://www.sgs-tuev-saar.com/en/it-security/it-security-training-en/online-registration-it-security.html

SGS TÜV SAAR

SGS

CS2B – ISO/SAE CD 21434 – ROAD VEHICLES – CYBERSECURITY ENGINEERING

The upcoming cyber security standard for road vehicles is a joint development of ISO and SAE. Learn about the definition of cyber security management systems and get an understanding of the underlying cyber security lifecycle. The application of this lifecycle is presented by an example, including potential challenges and solutions.

Contents

- Introduction to ISO/SAE CD 21434
- Cyber Security Management
- Risk Assessment
- Cyber security lifecycle
  - Concept phase
  - Product development

DATES AND ATTENDANCE FEE

24 May 2019 in Dortmund, Germany – conducted in German

04 July 2019 in Munich, Germany – conducted in English

17 October 2019 in Dortmund, Germany – conducted in German

798 euros (plus VAT)
718 euros (plus VAT) early bird rate*

*For all bookings received up until 6 weeks prior to the training

CS3 – CYBER SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS

Protect your investment against risks resulting from IoT and IIoT ('smart factory'). Decide what terms like security level and zones mean for your daily work. After this day you will have learned an approach to assessing how great the risk is to your systems and what documentation has to be prepared.

Contents

- Introduction to the Cyber Security concepts for industrial automation and control systems (IEC 62443)
- Security levels and their life cycles
- Security risk analyses and required documentation
- Reference model acc. to IEC 62443 and security zones
- Overview of IEC 62443 volumes and reference to other standards

DATES AND ATTENDANCE FEE

23 May 2019 in Dortmund, Germany – conducted in German

03 July 2019 in Munich, Germany – conducted in English

16 October 2019 in Dortmund, Germany – conducted in German

798 euros (plus VAT)
718 euros (plus VAT) early bird rate*

*For all bookings received up until 6 weeks prior to the training

CS4 – DATA AND COMMUNICATIONS SECURITY IN THE ENERGY SECTOR

Protect your investments by an analysis of the threat posed by security risks. Secure a competitive advantage by protecting your customers against cyberattacks. This seminar will help you to take major steps into the world of IoT and IIoT ('smart factory'). It will provide you with an overview of the security risks and countermeasures addressed in IEC 62351. As a result, you will be prepared for future challenges.

Contents

- Introduction to Cyber Security acc. to IEC 62351 for the energy sector
- Analysis of the security risks
- Security requirements and their implementation
- The security process in five steps
- Overview of IEC 62351 volumes and reference to other standards

DATES AND ATTENDANCE FEE

Please request.
All courses may be booked as in-house events as well.

979 euros (plus VAT)
881 euros (plus VAT) early bird rate*

*For all bookings received up until 6 weeks prior to the training

SGS TÜV SAAR

SGS

CS6 – ATTACK TREE DRIVEN CYBERSECURITY RISK ASSESSMENT (ATDCRA)

This course is to educate students on a unique approach to Attack Tree Modelling developed for the modelling and analysis of cybersecurity risks in systems and devices. Students will be provided with the tools and knowledge necessary to perform comprehensive cybersecurity vulnerability assessment using ATDCRA and will be capable of producing comprehensive graphical Attack Tree Models of systems after completion of this training course.

Contents

- Guided hands-on approach
- Applicable for cyber risk assessments of any system
- Provides a methodology that can be integrated directly with a business' current risk assessment processes
- Provides a basis for businesses to make justified investments in cybersecurity risk prevention and mitigation

DATES AND ATTENDANCE FEE

Please request.

CS7 – HARDWARE CYBERSECURITY DEEP DIVE (HCDD) TRAINING

The purpose of the HCDD course is to educate students about the methods of secure hardware design, physical layer vulnerability analysis, reverse engineering and exploitation. Students will be provided with the tools and knowledge necessary to perform a physical layer cybersecurity vulnerability analysis of an embedded system after completion of this training course.

Contents

- Guided hands-on training for automotive hardware exploitation
- Provides the knowledge necessary to define and identify meaningful cybersecurity requirements
- Provides a basis for students to independently advance their hardware exploitation capabilities following the course
  - Fundamental knowledge of hardware exploitation concepts
  - Knowledge of low-cost tools and resources necessary to perform advanced exploitation
- Hands-on practical experience performing hardware reverse engineering

DATES AND ATTENDANCE FEE

Please request.

CS8 – SOFTWARE CYBERSECURITY DEEP DIVE (SCDD) TRAINING

The purpose of the SCDD course is to educate students on the fundamentals of the secure design of software, software reverse engineering and basic software exploitation. Students will be provided with the tools and knowledge necessary to analyse application-layer software for cybersecurity vulnerabilities and will be capable of exploiting common forms of software after completion of this of this training course.

Contents

- Provides the knowledge necessary to define and identify meaningful cybersecurity requirements for secure software systems
- Hands-on practical experience performing software reverse engineering and exploitation
- Provides a basis for students to independently advance their software exploitation capabilities following the course
  - Fundamental knowledge of software exploitation concepts
  - Knowledge of low-cost tools and resources necessary to perform advanced exploitation

DATES AND ATTENDANCE FEE

Please request.

SGS IS THE WORLD'S LEADING INSPECTION, VERIFICATION, TESTING AND CERTIFICATION COMPANY. AS A JOINT VENTURE OF SGS AND TÜV SAARLAND E. V., SGS-TÜV SAAR ENSURES THE RELIABILITY AND QUALITY OF PROCESSES, PRODUCTS AND TECHNICAL SERVICES.