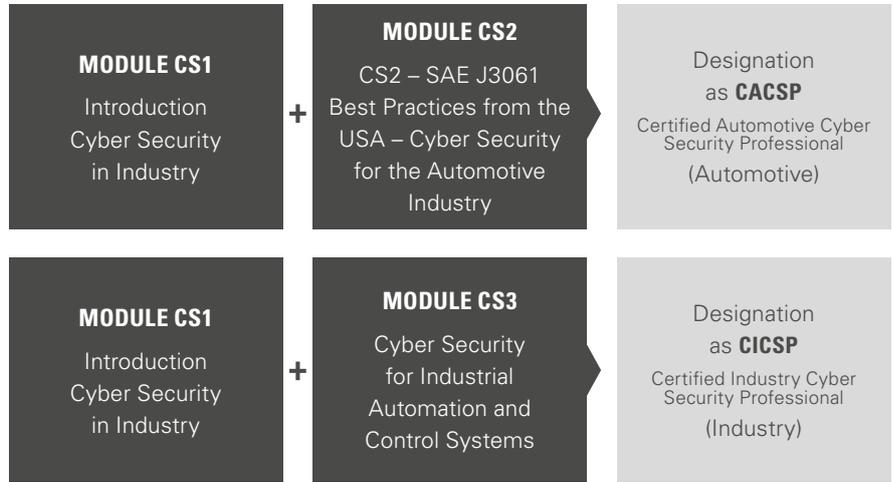


# CYBER SECURITY TRAINING & PERSONAL CERTIFICATION

IN MUNICH

02-03 JULY 2019



## CYBER SECURITY

As a result of the increasing level of digitalisation in all conceivable sectors of industry, the relevance of understanding the related risks and possible protection concept is continually growing. Protect your IT systems against malware and the potential threats posed by criminal attacks with the IT Security Analysis Services from SGS-TÜV Saar.

## EXPERIENCED STAFF OF TRAINERS

SGS-TÜV Saar GmbH is a company of the SGS Group and TÜV Saarland e.V. that supports you in all matters relating to Cyber Security. SGS-TÜV Saar is the first body worldwide to have been accredited for SAE J3061. The long-standing experience of our experts has been fed into the training programmes we offer, which reflect all current developments in the field of Cyber Security.

## MODULAR TRAINING CONCEPT

We have designed our training concept in the form of modules. This allows you to individually select your programme and to personally make it as effective as possible. Participation in Modules CS1 and CS2, and CS1 and CS3, respectively, is required to take the CACSP and CICSP tests.

## TRAINING SCHEDULE

The training sessions are held on two days 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.

## CS0 – OVERVIEW CYBER SECURITY IN INDUSTRY

Familiarise yourself in 1 hour with the Cyber Security concepts for IIoT/ Smart Factory and Connected Cars. In our webinar we will provide you with everything you need to get an overview of this topic. 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

Presentation of Cyber Security concepts for:

- Vehicles (SAE J3061)
- The energy sector (IEC 62351)
- Industrial automation and control systems (IEC 62443)

## DATES AND ATTENDANCE FEE

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

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

Free webinar

## CS1 – INTRODUCTION CYBER SECURITY IN INDUSTRY

Familiarise yourself in one day with the Cyber Security concepts for IIoT/ Smart Factory and Connected Cars. After a detailed introduction to the topic of Cyber Security, the two relevant standards and their underlying requirements are presented.

### Contents

- Introduction to Cyber Security
- Presentation of Cyber Security concepts for:
  - Vehicles (SAE J3061)
  - Industrial automation and control systems (IEC 62443)

## DATES AND ATTENDANCE FEE

02 July 2019 in Munich, Germany – conducted in English

598 euros (plus VAT)

538 euros (plus VAT) early bird rate\*

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

## CS2 – 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
- Tips for practical implementation and reference to other standards

## DATES AND ATTENDANCE FEE

03 July 2019 in Munich, Germany – conducted in English

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](mailto:fs.training@sgs.com)  
[www.sgs-tuev-saar.com/fs](http://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](mailto:cybersecurity@sgs.com)  
[www.sgs-tuev-saar.com/fs-training](http://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>

### 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

03 July 2019 in Munich, Germany – conducted in English  
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 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.**

WHEN YOU NEED TO BE SURE

