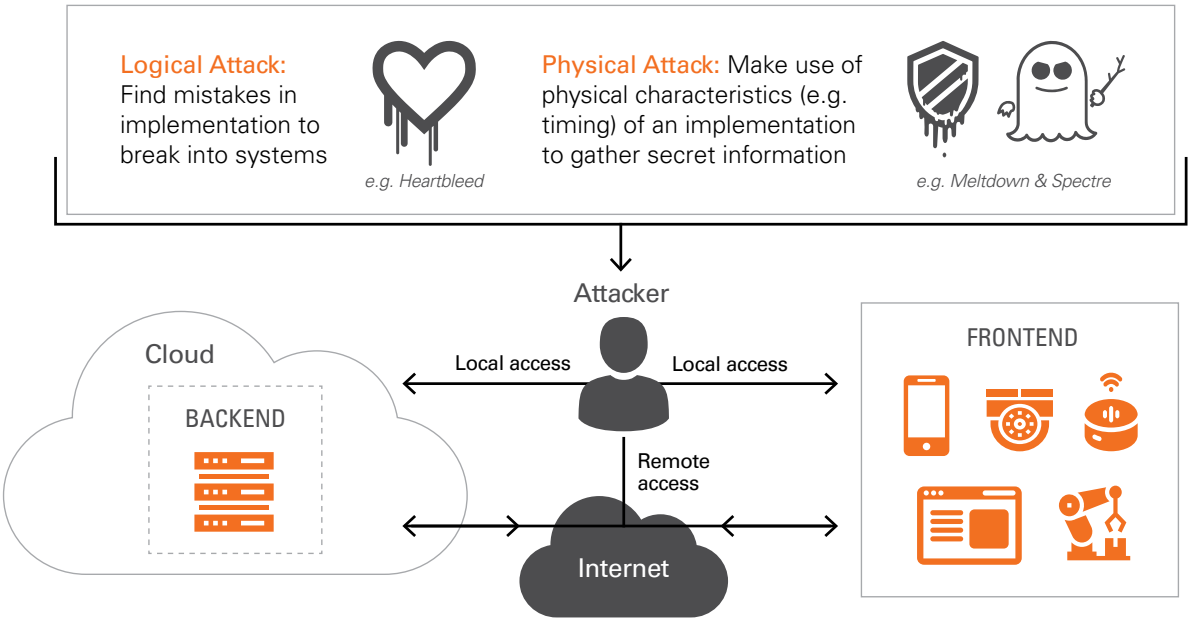
# Protect your business with SGS Cybersecurity Services

# Connected digital solutions offer an unprecedented level of convenience but create new opportunities for criminals

Traditional business and the digital world are increasingly intertwined. From the automation of production plants to smart homes and autonomous vehicles, the Internet of Things (IoT), where computers, systems and all kinds of smart devices communicate wirelessly, is no longer science fiction – but science fact!

Today, the IoT brings convenience to everyone's life – professional and personal. But at the same time, it opens up new ways for criminals to cause significant financial damage, breach privacy or even harm lives.

# ATTACKS




When hackers try to break a system, they carry out implementation attacks on hardware or software, thereby using logical or physical attack principles applied locally or remotely.

Local attacks - hackers study a device they acquired to find weak spots and develop ways to exploit them.

Remote attacks - hackers then use what they have learned on the same types of devices operating in the field to meet their objectives, such as disclosing personal information, gaining a financial benefit or even compromising people's lives by impacting safety measures.

Accordingly, devices need to be protected against local and remote implementation attacks.

## EXAMPLES OF HACKS

### SEMICONDUCTORS

- Meltdown & Spectre (New York Times, 01.03.2018)
- Extract memory content via side-channel attack

### MEDICAL

- Cyberattack on a hospital (New York Times, 18.09.2020)
- Ransomware attack forced hospital to turn away patients, one of which died

### CONSUMER IOT

- Mirai Botnet (The Guardian, 21.10.2016)
- Largest distributed denial of service attack using IoT devices

### AUTOMOTIVE

- Tesla Model S Hack (Hollywoodreporter, 8.7.2015)
- Multiple local and remote exploits to take control of car remotely via a mobile phone

### INDUSTRIAL

- Triton (The Guardian, 15.12.2017)
- Malware on Triconex safety controller model can trigger fails of highly safety critical systems in chemical or even nuclear plants

# How can you mitigate the risk of being hacked and convince others that you did it right?

Perfect security in a usable form does not exist in practice due to the ever changing risks posed by criminal activities. However, there are ways to reduce the risks of being hacked, limit the impact if an attack happens, and to quickly recover from it.

Governments, stakeholders and regulators across all industries around the world are working on standards and regulations to tackle the cybersecurity challenge with a focus on the complete supply chain, life cycle of components, products, networks and systems.

## CYBER SECURITY SERVICES

SGS has concentrated its cybersecurity capabilities under one single umbrella: SGS Cybersecurity Services.

Our technical expertise and capabilities, global footprint and market leadership in testing, inspection and certification across all industries puts us in a unique position to deliver best in class cybersecurity services.

With a focus on standardization, regulation and research, we can deliver programs according to customer needs, across all regions and in a consistent and timely manner. Our comprehensive service offering around cybersecurity related aspects, allows our customers to demonstrate that the measures taken to mitigate cybersecurity risks are effective.

### WE EXCEED EXPECTATIONS

- Trusted for impartiality, inspection, testing, verification, certification solutions
- Working across industries covering supply chains
- Leading think tanks together with key partners
- Driving cybersecurity research solutions made available for all
- Operating highly secured cyberlabs around the globe

### WE ARE LEADING CYBERSECURITY EXPERTS

- Hardware security analysis from transistor to system level
- Software security analysis from firmware to cloud
- Network security assessments from smallest components to Internet-level
- Cryptanalysis from primitives to protocol level
- Applied research for efficiency, usability and verifiability of secure solutions

# OUR GENERAL SERVICE OFFERING

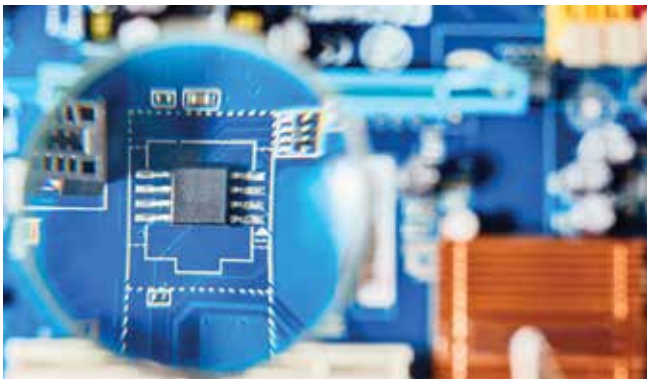
Cybersecurity is an issue, that, for many industries, is new and changes the way connected digital solutions and services must be developed and maintained. Consequently, the security maturity level available in companies for their solutions and infrastructure is often low compared to the capabilities of most adversaries. Our service portfolio is tailored to address this situation holistically, helping our customers to raise their security maturity to the level required to meet the cybersecurity challenge.

## TRAINING

Our training portfolio provides insights on various cybersecurity related aspects, from basic awareness creation, regulation and standardization landscape, to technical aspects at an expert level, such as best practices on secure designs and testing approaches.

## ASSESSMENT

Assessment services provide the means to identify and evaluate your cybersecurity gaps in hardware or software, within networks or infrastructure, in production facilities, or in organizational structures.



## CERTIFICATION

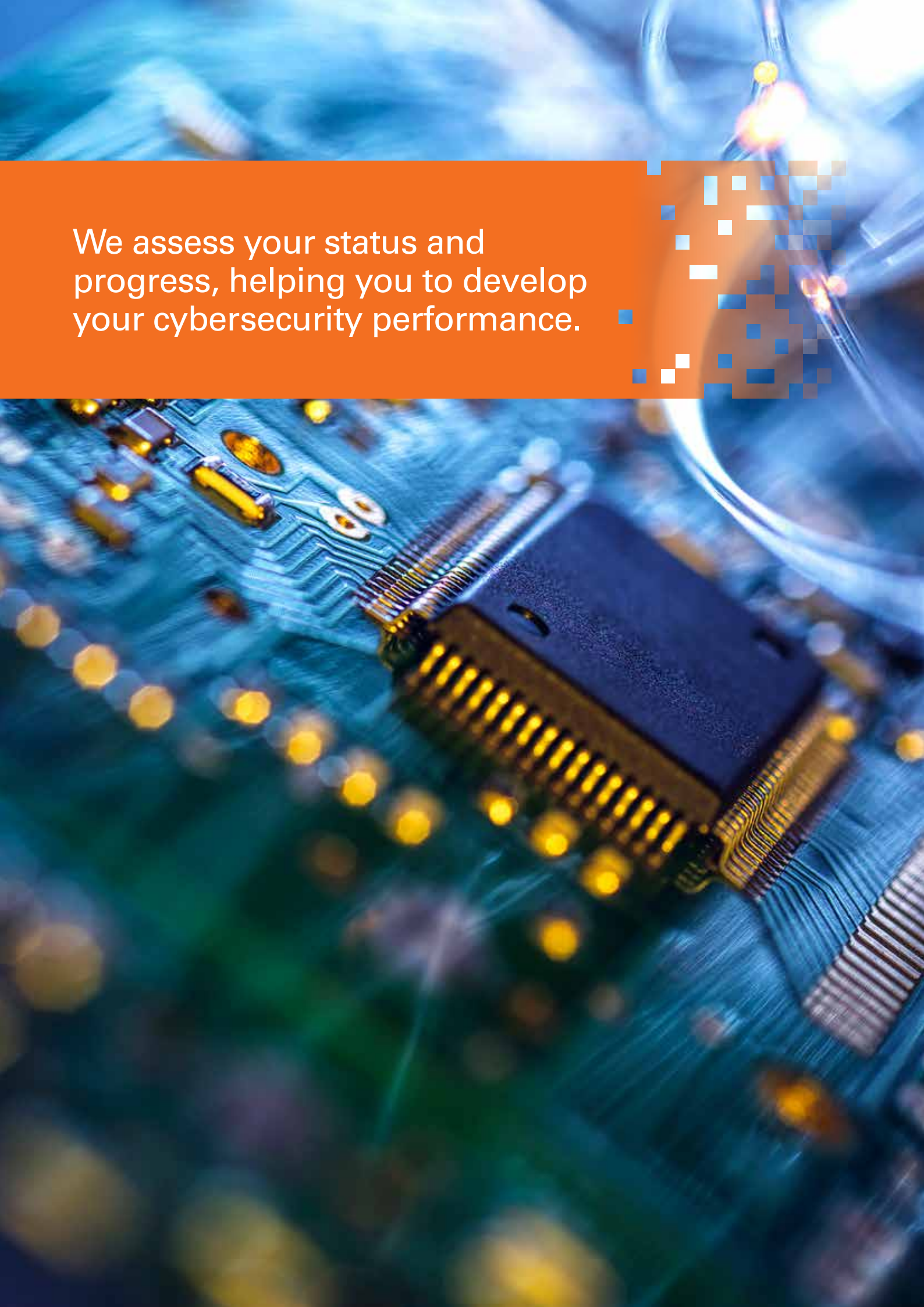
Our portfolio of cybersecurity certification services provide independent proof points that your solutions and assets fulfill industry standards, regulations or proprietary security specifications.

We help you understand the cybersecurity challenges ahead and ways to respond.

# TRAINING

Besides awareness and introductory cybersecurity training for a broad audience, tailored to vertical needs, we also offer professional and expert level training covering cybersecurity aspects such as:

- Security risk management
- Secure development and product life cycle
- Communication and network security
- Secure design and coding
- Security assessment and testing
- Cybersecurity related standards, regulation and certification per vertical


We assess your status and
progress, helping you to develop
your cybersecurity performance.

# ASSESSMENT

Our services cover cybersecurity, from the transistor level for semiconductors, ranging over embedded firmware and software, to web, mobile and cloud applications, covering IoT solutions, as well as IT- and cloud-network security services. We also assess secure management systems, policies, business processes and professionals.

## HARDWARE

- Hardware security reviews
- Hardware security analysis applying below listed methods and covering highest attack potential (representing CC AVA_VAN.5) from chip level to product level (e.g. IoT HW)
- Methods applied include:
  - Fault injection (e.g. laser, EM, glitch)
  - Side channel analysis (e.g. power, EM, timing, single photon emission)
  - IR and photo emission imaging
  - Micro probing
  - Hardware reverse engineering
  - Embedded firmware and software analysis

## CRYPTO ALGORITHMS AND PROTOCOLS

- Cryptanalysis of primitives: symmetric and asymmetric schemes, hash-functions and random number generators
- Cryptanalysis of protocols: basic authentication, privacy and secure communication protocols

## IT- AND CLOUD-INFRASTRUCTURE

Network security assessments such as:

- Enterprise vulnerability assessments covering network technologies, components and web services
- Penetration testing against IT-networks, cloud platforms or IoT backends
- Advanced penetration testing such as Red Teaming tailored for specific industry needs
- Monitoring of specific and critical assets

## SOFTWARE

- Software security reviews
- Static Code Analysis (SCA) and reviews related to security features and measures
- Binary Code Analysis (BCA)
- Software reverse engineering
- Fuzzing
- Application security assessment, considering for example least privilege assessment, security architecture review, and applied system hardening
- Application penetration testing against applications running on (IoT) devices, web servers or local machines
- Mobile app security analysis

## GOVERNANCE, RISK AND COMPLIANCE (GRC)

Covering gap analysis, risk assessment, preparatory audits, compliance projects, training and advisory for all governance, risk and compliance topics related to cybersecurity schemes, processes, standards and regulations such as:

- Industrial Automation and Control Systems (IEC 62443)
- Network security
- ISMS according to the ISO 27k-family
- Regulations such as GDPR and the Network and Information Security Directive
- NIST-Framework
- Secure Development Life Cycles (SDLC)
- Cybersecurity Maturity Model Certification (CMMC)

We independently confirm that you meet regulations & standardized criteria.

# CERTIFICATION

We provide certification services against standards and regulations across all industries.

- Independent 3rd party conformity assessments against generic, proprietary or vertical specific cybersecurity standards (e.g. for medical devices, automotive or industrial IoT devices)
- Consumer IoT conformity assessments issuing SGS certificates, supported by the product labeling program "IoT-Security Checked"
- Compliance assessments and certifications for information security management systems and processes, policies and regulations (e.g. ISO 27001 or IEC 62443-4-1)
- Common Criteria evaluation and certification services up to EAL7 (German scheme, BSI)
- EMVCo evaluation and certification (in preparation)
- LINCE evaluation and certification governed by the CCN, Spain
- BSZ evaluation and certification governed by the BSI, Germany (in preparation)
- SESIP evaluation and certification governed by GlobalPlatform (in preparation)
- CTIA IoT security evaluation and certification
- In preparation for required re-certifications, we offer attack landscape monitoring services for tested products

# INDUSTRY SPECIFIC CYBERSECURITY SERVICES

In general, cybersecurity methodologies and best practices are nonspecific and can be applied across all industries. However, depending on the risk exposure of use cases, the technologies considered and effort spent to develop and maintain secure solutions, as well as the depth of analysis required to independently assess the quality of security implementations, vary significantly. Therefore, security standards, regulations and certification schemes differ from industry to industry.

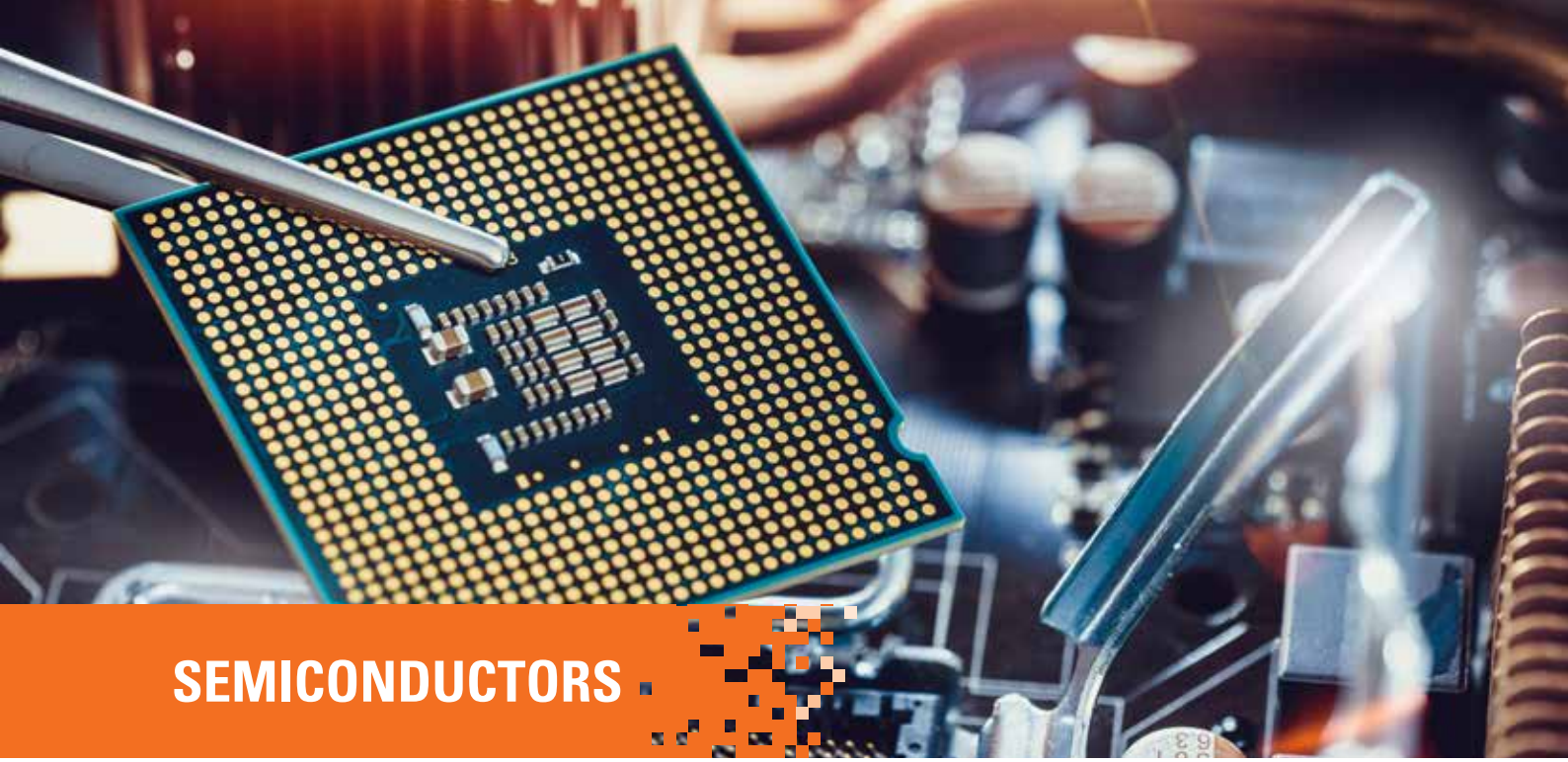
In the following, we introduce our services which meet the needs of industries with growing demand for cybersecurity services.

**SEMICONDUCTORS**
Seen as the root of trust that secure applications can be built on

**MEDICAL DEVICES** AND **AUTOMOTIVE**
Where connectivity makes devices prone to cyberattacks, potentially putting even lives at risk


**CONSUMER IOT**
Where data privacy and functional safety are big concerns

**INDUSTRIAL**
Where industry 4.0 equipment and systems are critical infrastructure for companies and nations



# SEMICONDUCTORS

Secure microcontrollers have been used as secure hardware platforms in eGovernment and payment applications for many years. Those microcontrollers are especially protected against local physical attacks, where an attacker can apply techniques such as side-channel and fault attacks to reveal secret information (e.g. a PIN). Recent discoveries like Meltdown and Spectre (New York Times, 01.03.2018), however, show that a new trend is emerging where physical attacks are performed remotely, therefore becoming relevant for a broad range of applications.
The strong growth of IoT applications drives the need for physical attack resistance also for general purpose microcontrollers, affecting IP providers, IC design houses and embedded software developers supplying industries such as Automotive, MedTech, Industrial and Consumer IoT.

SGS offers training, assessment and certification services to manufacturers and embedded software developers, laying special focus on µC/µP Design and the related physical attacks requiring resistance against side-channel and fault attacks.

## TRAINING

- Hardware-related standards, regulation and certifications, such as Common Criteria
- µC/µP Principles: security concepts & architectures, system partitioning
- Secure design & coding principles
- Local and remote side-channel and fault resistance
- Common Criteria Training, with special focus on hardware-related protection profiles such as the Security IC Platform Protection Profile, the Java Card Protection Profile, Machine Readable Travel Document with "ICAO Application", Extended Access Control with PACE, IoT Secure Element Protection Profile or the upcoming Secure Subsystem for SoC Protection Profile
- Secure Hardware/Software development life cycle

## ASSESSMENT

- Asset-based vulnerability analysis of hardware and embedded software
- Pre- and post-silicon security analysis & security design reviews
- Countermeasure characterization
- Side-channel analysis (e.g. power, EM, timing, single photon emission)
- Fault injection (e.g. laser, EM, glitch)
- IR and photo emission imaging
- Micro probing
- Hardware reverse engineering
- Fuzzing
- Binary code analysis
- Static code analysis

## CERTIFICATION

- Common Criteria for security ICs, platforms and applications up to EAL7 and AVA_VAN.5
- Development site and production facility auditing according to Common Criteria and alike
- EMVCo IC & Platform (in preparation)
- SESIP (in preparation)
- ARM PSA (in preparation)

# CONNECTED MEDICAL DEVICES

The medical device and health industry has been heavily hit by hackers in the past. This was again sadly demonstrated by a cyberattack against a Düsseldorf hospital in September 2020, where a woman died because the hospital systems were not available due to the attack (New York Times, 18.09.2020).

Cybersecurity is of fundamental importance for medical devices and hospital systems to safeguard functional safety, effectiveness and availability. Accordingly, cybersecurity regulations are being developed and implemented across all regions and so manufacturers must provide evidence of compliance with these standards before medical devices can enter markets. Similar is true for hospital networks since they are considered critical infrastructure.

SGS offers a tailored cybersecurity service portfolio for manufacturers and hospitals helping them to comply with regulations and corresponding standards, and to generate requested evidence and proof points that cybersecurity related risks have been considered, evaluated and mitigated for the complete life cycle for devices, systems and networks.

We provide training, assessment and certification services, paying special focus on the intertwined relationship of cybersecurity and functional safety.

## TRAINING

- Introductory Cybersecurity Training for Medical Device Manufacturers introducing the current market situation, incidents, threats and risks, regulation, standards, certifications and best practices
- Cybersecurity Risk Management for Medical Device Manufacturers according to ISO 14971, AAMI TIR57 or AAMI SW 96
- Cybersecurity related post market activities
- Secure Hardware/Software Development Life Cycle
- Training covering secure design & coding principles, security assessment and testing
- Communication & network security

## ASSESSMENT

- Cybersecurity threat and risk analysis for medical devices, hospital networks, policies and processes
- Security capability maturity assessments for organizations and business processes
- Security related Gap Assessments and Design Reviews for Medical Devices covering the complete product life cycle
- Review and assessment of applied cybersecurity risk management for medical devices (e.g. acc. to ISO 14971, AAMI TIR57 or AAMI SW 96)
- Vulnerability assessments for hardware and software, as well as network and cloud solutions
- Customized security assessment and test campaigns in preparation for product approvals (e.g. FDA 510k application) and against relevant standards

## CERTIFICATION

- Independent conformity assessments against cybersecurity guidance documents issued by the FDA or issued in connection to the European MDR/IVDR regulations
- Independent conformity assessments against the standards AAMI TIR57, AAMI TIR97, AAMI SW96, UL2900-2-1
- Security evaluation and certification according to the upcoming BSZ Certification Scheme governed by the BSI in Germany (in preparation)
- Security evaluation and certification according to the SESIP scheme suitable for IoT devices governed by GlobalPlatform (in preparation)


# CONSUMER IOT

Security of consumer IoT is becoming more and more critical driven by the exponential growth of devices shipped to global markets. This is underpinned by the vast number of vulnerable consumer IoT devices reported, be it hacked IP-cameras allowing hackers to spy into private households or devices being captured by hackers and implemented into botnets (The Guardian, 21.10.2016).

Baseline security requirements for consumer IoT devices have been defined and issued in standards by numerous organizations but so far inadequately implemented in products. Latest regulations, such as the EU Cybersecurity Act, GDPR, the California Consumer Privacy Act and state bills across the US are putting pressure on manufacturers and retailers to take action.

Our services are tailored to help manufactures and retailers to develop their cybersecurity capabilities. We offer training, gap analysis, security reviews, assessments and testing services, starting in early design phases and along the complete lifecycle. We do this for IoT hardware and software, for mobile apps and IoT backend platforms, but also for business processes like a Secure Development Life Cycle (SDLC).

Our "IOT-Security Checked" program provides a leveled security and conformity assessment program for consumer IoT devices. The approach considers the risk exposure of the use case and offers an adequate assurance level in line with international regulation. The test program is accompanied by a product labeling program that supports manufacturers and retailers to market their investment into cybersecurity.


## TRAINING

- Cybersecurity for consumer IoT manufacturers introducing the current market situation, incidents, threats and risks, regulation, standards and best practices
- Secure hardware/software development life cycle
- Training covering secure design & coding principles, security assessment and testing
- Communication & network security

## ASSESSMENT

- Gap assessment and design reviews for hardware, software, mobile apps and IoT backend platforms
- Asset-based vulnerability analysis
- Security assessment and testing services
- Attack landscape monitoring services for tested products

## CERTIFICATION

- Conformity assessment program for consumer IoT manufacturers offering four assessment levels M0 up to M3 that allows alignment of the risk exposure of the application to an appropriate assurance level. Standards covered include: ETSI EN 303 645 and NISTIR 8259A
- Sample test program R1 and R2 for retailers
- "IOT-Security Checked" product labeling program (details see www.sgs.com/iot)
- Re-assessments and re-certifications for products in the field
- SESIP security evaluation & certification governed by GlobalPlatform (in preparation)
- LINCE security evaluation & certification governed by CCN, Spain
- BSZ security evaluation & certification governed by BSI, Germany (in preparation)

# INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS

Industrial Automation and Control Systems (IACS) and Operational Technology (OT) networks are critical infrastructure not only for manufacturers, but also on the national level when it comes to e.g. chemical or power plants. Cybersecure implementation and operation of these systems have become a strong requirement (The Guardian, 15.12.2017).

Industrial security enables automatic operation and control of industrial processes in a secure manner, ensuring that these systems are not subject to a loss of availability, integrity and/or confidentiality. Ensuring availability through effective security controls also ensures a safe environment without hostile or accidental security breaches.

It is the application of sustainable methodologies that not only ensures effective security, but also makes it possible to communicate with corporate networks or cloud services without negative impacts on the operational technology.

Through the application and certification of security for industrial control and automation systems we ensure efficient operations and prevent major economic damage and collateral damage spread through networks and conduits due to hostility, malfeasance or accident.

Our approach to industrial control and automation security is through internationally accredited standards such as IEC 62443 or also IEC 62351 applicable for the energy sector, using renowned certification schemes and potent security methodology.

## TRAINING

- Introductory Cybersecurity Training for Manufacturers, integrators and operators of IACS components and systems introducing into most relevant standards, regulation, incidents, best practices and certifications
- IEC 62443 framework
- Secure HW/SW Development Life Cycle (IEC 62443-4-1)
- Technical security requirements for IACS components (IEC 62443-4-2)
- Secure design & coding principles, security assessment and testing
- Communication & network security

## ASSESSMENT

- Cybersecurity threat and risk analysis
- Customized security assessment and penetration test campaigns for IACS components, systems and networks against relevant standards (i.e. IEC 62443)
- Security related gap assessments and design reviews
- Security capability maturity assessments for organizations and business processes (i.e. IEC 62443-4-1)

## CERTIFICATION

- Audits and certification against IEC 62443 and IEC 62351 standards
- BSZ security evaluation and certification governed by the BSI, Germany (in preparation)
- SESIP security evaluation and certification suitable for IIoT devices governed by GlobalPlatform (in preparation)
- Common Criteria evaluation and certification up to EAL7 (German Scheme, BSI)


# AUTOMOTIVE

Connectivity has become ubiquitous in automotive applications. System complexity on hardware and software, several bus systems and communication protocols, and a fragmented supplier landscape create a challenge for automotive manufacturers and suppliers to meet cybersecurity requirements.

Cybersecurity is key for applications like Advanced Driver Assistance Systems (ADAS), Firmware Over The Air (FOTA) Updates or Vehicle to Vehicle and Infrastructure (V2X) communication. Recent hacks (e.g. see Hollywoodreporter, 8.7.2015) demonstrated drastically what can happen when vulnerabilities are exploited.

Standards are under way and regulation is already in place for several applications. For example, the ISO/SAE 21434 standard (Road vehicles — Cybersecurity engineering) is expected to become the guiding secure development life cycle process document for automotive manufacturers and suppliers. As a result, there is an increasing demand for cybersecurity services in the automotive industry.

We offer a full set of services helping players in this industry to develop cybersecurity capabilities via training, gap assessments and audits for hardware, software and business processes. Our testing and certification services allow manufacturers and suppliers to testify that their solutions meet cybersecurity requirements put in place in proprietary and bilateral specifications, standards and regulations.

## TRAINING

- Introductory Cybersecurity Training for Automotive Manufacturers introducing most relevant standards, regulations, incidents, best practices and certifications
- SAE J3061 and ISO/SAE 21434 standard, secure hardware/software development life cycle for automotive
- Secure design & coding principles, security assessment and testing
- Penetration testing for automotive systems
- Common Criteria for automotive applications and available protection profiles (e.g. V2X)

## ASSESSMENT

- Cybersecurity threat and risk analysis
- Security related gap assessments and design reviews
- Customized security assessment and penetration test campaigns for automotive components (ECUs, hardware and software)
- Security capability maturity assessments for organizations and business processes against ISO/SAE 21434
- Pre-testing services in the course of certification activities

## CERTIFICATION

- Audits and certification against ISO/SAE 21434 (in preparation)
- Common Criteria evaluation and certification (German Scheme, BSI)
- SESIP security evaluation and certification suitable for automotive IoT devices governed by GlobalPlatform (in preparation)

Contact us:

**CYBERSECURITYSERVICES@SGS.COM**

**WWW.SGS.COM/CYBERSECURITY-SERVICES**

## SOURCES


- Researchers discover two major flaws in the world's Computers
  https://www.nytimes.com/2018/01/03/business/computer-flaws.html
- Cyber attack suspected in German woman's death
  https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html
- Major cyber attack disrupts internet service across Europe and US
  https://www.theguardian.com/technology/2016/oct/21/ddos-attack-dyn-internet-denial-service
- Security experts reveal how a Tesla Model S was hacked
  https://www.hollywoodreporter.com/news/security-experts-reveal-how-a-814062
- Triton: hackers take out safety systems in 'watershed' attack on energy plant
  https://www.theguardian.com/technology/2017/dec/15/triton-hackers-malware-attack-safety-systems-energy-plant

WWW.SGS.COM

WHEN YOU NEED TO BE SURE