Brightsight industrial cybersecurity evaluation services

DELIVERING CYBERSECURE DEVICES AND COMPONENTS TO GLOBAL INDUSTRIAL MARKETS

brightsight

By SGS

brightsight.com

INDUSTRIAL DRIVERS

In a rapidly evolving security landscape, regulations are beginning to require more and more evidence of cybersecurity management in IoT – e.g. EU Radio Equipment Directive (RED) in 2025. The IoT sector falls under the provisions of a wide variety of legislation and standards, including the NIS2 Directive, the Cyber Security Act (EU), the Cyber Resilience Act (EU) and NIST 8425 (USA). Certification against recognized industrial IoT standards, such as ISA/IEC 62443, demonstrates cybersecurity management, while also helping developers mitigate risk in their value chain and enabling market differentiation for their products.

Compliance – does your product conform to recognized standards for security and performance?

Risk management – has due diligence been performed during development and manufacture?

Market differentiation – can you demonstrate your product is safer and more secure than your competitors?

ISA/IEC 62443 STANDARD

The ISA/IEC 62443 series of standards establishes guidelines and procedures for ensuring secure industrial automation and control systems (IACS). These standards set best practices for security and provide a way to assess the level of security performance; bridging the gap between operations and information technology, as well as between process safety and cybersecurity.

This holistic approach to cybersecurity encompasses:

- Defining organizational and technical requirements for stakeholders (manufacturers, integrators, operators and industry)
- Targeting various aspects like people, processes, systems, solutions, and components across all industries and facilities
- Supporting tailored security solutions by offering varying levels of security assurance
- Being utilized for certifying security processes and the security capabilities of solutions in a repeatable and objective way

SGS EVALUATION SERVICES

Our comprehensive pre-evaluation, training and developer support services help manufacturers and developers reduce the potential for failure during formal security evaluations. We evaluate amongst others: components of cybersecurity management systems, industrial routers, data diodes, software applications, embedded devices, host devices and network devices. Our post-evaluation services help you to stay compliant with the latest regulations.

PRE-EVALUATION

- Basic awareness workshop – an overview of cybersecurity for industrial IoT
- IEC 62443 introduction workshop – a comprehensive look at the standard, its framework and technical security requirements
- Workshop on Threat Analysis and Risk Assessment (TARA) – enabling customers to conduct their own TARA, this workshop offers advanced training in threat and risk analysis techniques applied practically to a client-provided example

The Internet of Things (IoT)

Smart technology is being incorporated into everything from energy systems, processes, factories and buildings to urban infrastructures and transport systems. It enables greater efficiencies and improves sustainability and interoperability, but these benefits can only be realized if the system is cybersecure. SGS Brightsight offers comprehensive solutions to help you successfully access target markets with compliant and cyber secure products, enabling risk mitigation and helping your products stand out.

- Secure product development, vulnerability scan and testing – with the goal of providing guidance for developers to increase the overall maturity level of their implementation process. This includes secure coding guidelines and other state-of-the-art best practices
- Technical system development life cycle advice
- Evidence readiness and document support – pre-assessment preparation for full security evaluations, including gap analysis, maturity assessment and guidance on laboratory and certification body requirements

SECURITY EVALUATION

- Threat Analysis and Risk Assessment (TARA)
- RED Article 3.3. (d),(e),(f)
- Assessment against:
  - IEC 62443 2-4 – IACS policy and procedures assessment
  - IEC 62443-3-3 – System integration assessment. Examples: SCADA systems, consisting of multiple sensors, control units, HMIs and software applications)
  - IEC 62443 4-1 – assessing the secure development procedures implemented by product manufacturers
  - IEC 62443-4-2 – assessing the security capabilities of the individual system components. Examples: local programmable logic controllers (PLCs) or the control unit of a building's smart lights
  - Evaluation through our SGS Brightsight IECEE CB Testing Laboratory (CBTL) in Madrid

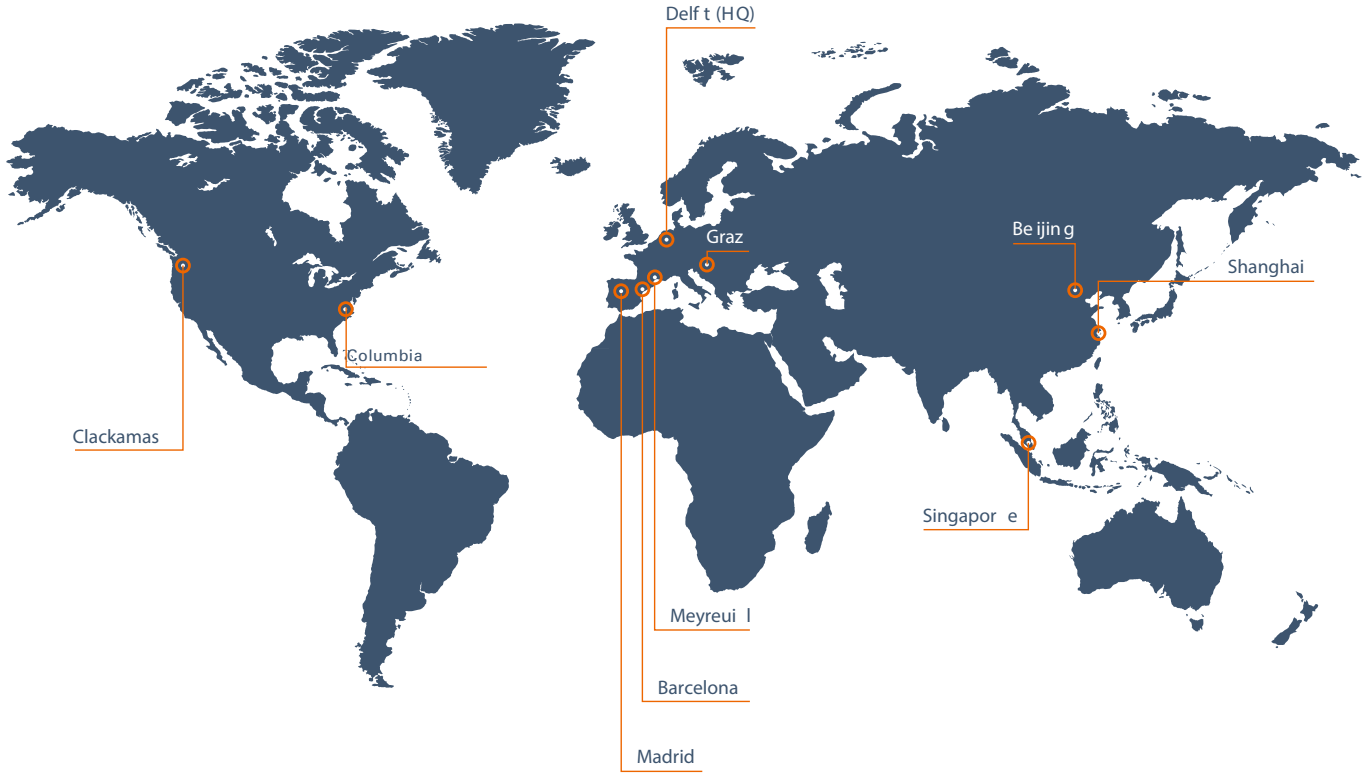
POST-EVALUATION

- Re-certification
- Certification health check

WHY CHOOSE SGS BRIGHTSIGHT AS YOUR SECURITY LABORATORY?

With over 40 years of experience in cybersecurity and a growing global network of specialist testing facilities, we are the world's largest security evaluation service provider with over 700 security evaluations completed every year. Specializing in Common Criteria, the globally recognized IT security standard, our expertise extends to certifying IT systems and devices, including verification up to the highest security evaluation assurance level, EAL 7. We understand the market and the technical requirements relevant to your component or device. Our dedicated team of security experts supports the streamlining of evaluation criteria into a single assessment process that incorporates all relevant global, regional and vendor requirements – one evaluation, multiple certifications. We are your first choice for independent testing and developer support services when you want to efficiently deliver safe and compliant industrial devices to global markets.

Our cybersecurity labs



- ISA/IEC 62443
- European Radio Equipment Directive (RED)

BRIGHTSIGHT IS PART OF SGS. THE WORLD'S LEADING TESTING, INSPECTION AND CERTIFICATION COMPANY.

CONTACT US

brs.industrial@sgs.com
www.brightsight.com

brightsight
By SGS