Training, workshops and pre-evaluation services for Industrial IoT

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

brightsight

BRIGHTSIGHT.COM

By SGS

brightsight

By SGS

OUR NUMBERS >

10
Locations around the globe

50+
Security standards and schemes recognitions

40+
Years of experience in security evaluations

220+
Security evaluation experts

700+
Security projects performed each year

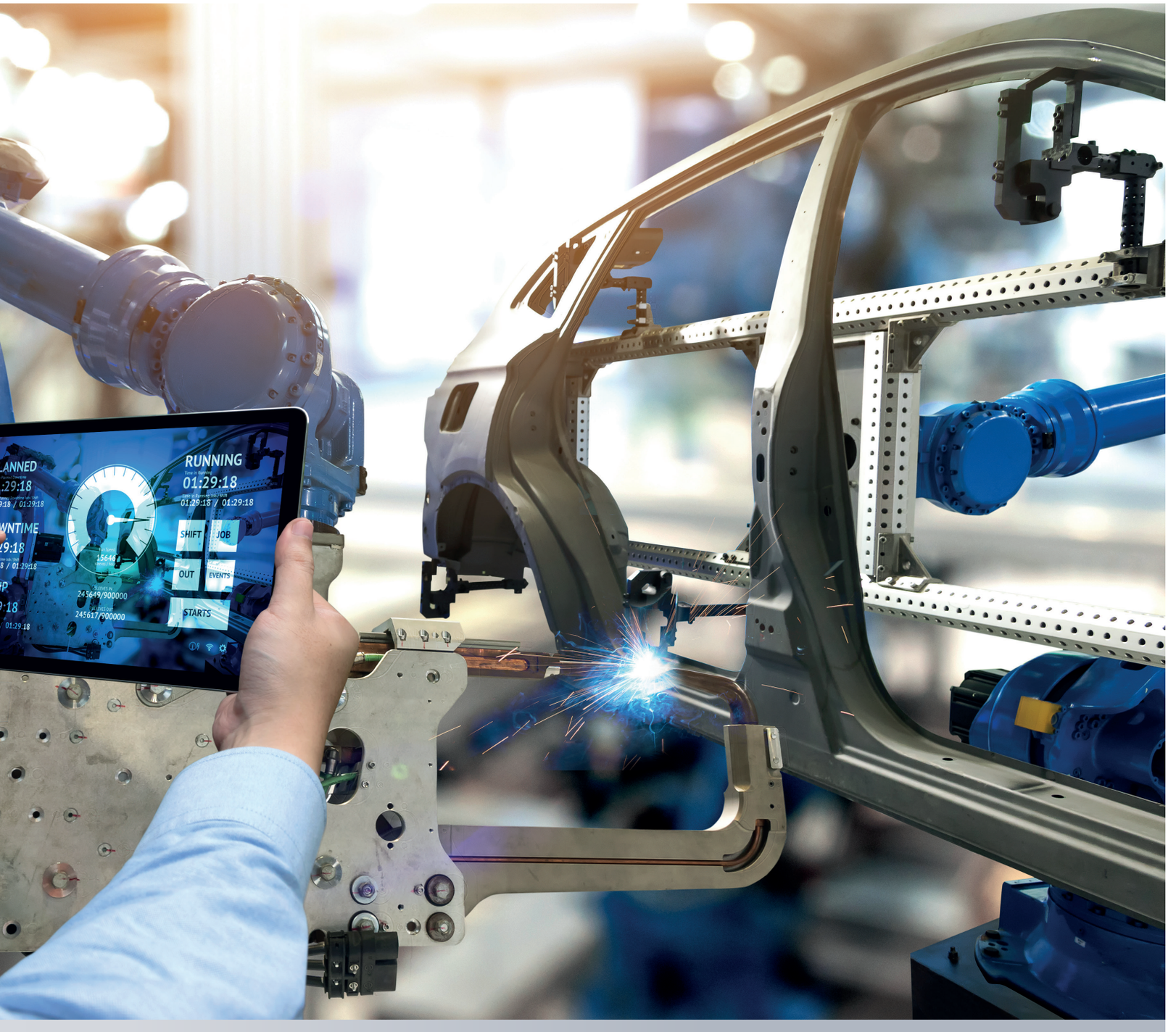
INDUSTRIAL

Common Criteria

SESIP™

IEC

ISO



psacertified™

One evaluation
Multiple certifications

SGS Cybersecurity
ETSI EN 303645
NIST IR 8259A

ATTACKS ON CRITICAL INFRASTRUCTURE ARE REAL AND SECURITY MEASURES NEED TO BE TAKEN INTO ACCOUNT IN INDUSTRIAL NETWORKS.

SGS Cybersecurity: What we do

High, medium and low assurance security evaluations to assess a product's compliance

We carry security evaluations out as an accredited lab under many different certification and conformance bodies, issuing security certifications

We work with 50+ schemes worldwide

Close and intensive cooperation between customer and lab

SGS - YOUR TRUSTED CYBERSECURITY LAB

Brightsight: covering product security at each level

OEM's offloading cybersecurity capabilities to SGS experts

PRE-EVALUATION SERVICES

Training

- Awareness training
- Secure product development and testing workshop
- Gap analysis workshop

Pre-evaluation

- Technical SDLC analysis
- Evidence readiness
- Vulnerability scans

SECURITY EVALUATION SERVICES

- IEC 62443-4-1
- IEC 62443-4-2
- IEC 62443-3-3
- ARM-PSA
- SESIP
- In depth testing
- SGS cybersecurity mark

IEC psacertified™ SESIP™

SGS Cybersecurity
ETSI EN 303645
NIST IR 8259A

POST EVALUATION SERVICES

- Continuous monitoring
- Continuous conformance
- Certification health check

PRE-EVALUATION SOLUTIONS: TRAINING AND WORKSHOPS FOR IIOT

1) IEC 62443-4-2 and SESIP	Approaching the security starting from platforms; SESIP: definition, levels, targets, requirements and benefits; Mapping IEC 62443 requirements via SESIP	1 day remote workshop
2) Threat Modeling Risk Assessment (62443-4-1)	Workshop on Threat Analysis & Risk Assessment (TARA) The goal of this workshop is to provide a basis that allows the Client to carry out a threat analysis and risk assessment (TARA) by itself. It includes an advanced training on threat and risk analysis techniques and the practical application thereof to an example given by the Client. The workshop is usually split into 4 half day sessions distributed over 4 weeks. Document Feedback In parallel to the workshop phase, the client will perform an initial threat & risk analysis of its product and provide intermediate results. SGS Brightsight will review these intermediate results and discuss them in the next workshop session. As a result the client will obtain a baseline TARA document and the knowledge to complete this on their own.	2 day remote workshop + Document feedback
3) Secure Development Trainings (62443-4-1)	The goal of these trainings is to provide guidance for developers to increase the overall maturity level of their implementation process. This includes secure coding guidelines and best practices as well as other state- of-the-art. Supplemented by practical workshops that allow developers to consolidate the theoretical parts. Available Trainings include: • Application Security Best Practices • Container Security Hot Spots • Secure Coding By Examples • Secure Coding in C, C++ and .NET • Standards, Best Practices and Background • Web Security Concepts	1/2 day remote training (each)

PRE-EVALUATION SOLUTIONS: ASSESSMENTS FOR IIOT

4) Gap Analysis for Secure Product Development Lifecycle (IEC 62443-4-1)	Information collection In the first step SGS will review the current state of client's secure development process for coverage of the standard. Missing information can be collected in a workshop in form of a discussion between the security experts from SGS and the client where the client should present all necessary information to the security experts. During the discussion, we will also shortly tackle related standards putting light on the bigger picture (e.g., ISO 27001 and relation to other parts of IEC 62443). Gap Analysis report* Based on the collected information, SGS will identify any existing gaps in the processes with respect to IEC 62443-4-1 and the Secure Development Lifecycle. The results of the analysis will be summarized in a gap analysis report together with best practice suggestions to close the gaps. Agenda: Security management; Specification of security requirements; Security by design; Secure implementation; Management of security related issues; Security update management; Security guidelines	Interviews + Gap Analysis
5) Gap Analysis for Secure design (IEC 62443-4-2)	Information collection In the first step SGS will review the current state of client's design documentation, especially the security architecture for coverage of the standard. Missing information can be collected in a workshop in form of a discussion between the security experts from SGS and the client where the client should present all necessary information to the security experts. Gap Analysis report* Based on the collected information, SGS will identify any existing gaps in the processes with respect to IEC 62443-4-2 and the Secure Design. The results of the analysis will be summarized in a gap analysis report together with best practice suggestions to close the gaps. Agenda: Product specification; Design and architecture; Security threat and risk analysis; Security architecture; Security controls and mechanisms.	Interviews + Gap Analysis

*In general, the workshop will be a discussion between the security experts from SGS and the client where the client should present all necessary information to the security experts. The security experts will then challenge the client with detailed questions.

PRE-EVALUATION SOLUTIONS FOR IIOT

6) Development Life Cycle pre-evaluation (62443-4-1)	SGS will review the Client's development life cycle documents for the device in scope and evaluate them from a security perspective for completeness, correctness, and alignment with IEC 62443-4-1. This activity also encompasses a final evaluation of the Client's process descriptions for the threat model, risk assessment, security architecture, interface design, and design of internal sub-systems. At the end, SGS will provide a report on the evaluation result against the practices required by IEC 62443-4-1.	Pre-Evaluation
7) Design pre-evaluation (62443-4-2)	SGS will review the Client's design documents for the device in scope and supporting infrastructure and evaluate them from a security perspective for completeness, correctness, and alignment with IEC 62443-4-2. This activity also encompasses a final evaluation of the Client's product specific threat model, risk assessment, security architecture, interface design, and design of internal sub-systems with a focus on the implemented security features as required by IEC 62443-4-2. At the end, SGS will provide a report on the evaluation result.	Pre-Evaluation
8) implementation review (62443-4-2)	SGS will review the Client's implementation, which includes static code analyses of security-relevant source code of one variant of the edge-device and the backend as well as a manual review of its findings. Moreover, SGS will look for insecure function calls and code constructs as well as for the adherence to best practice coding paradigms. At the end, SGS will provide a report on the evaluation result. The focus of the evaluation lies on the security features as required by IEC 62443-4-2.	Code Analysis
9) Vulnerability Analysis & Testing (62443-4-2)	Based on the provisions put forth by IEC 62443-4, we provide a final vulnerability analysis covering the following elements: • Tests against the provisions presented in IEC 62443-4-2. • A full grey-box penetration test against the device. • Test of security of data in transport.	Vulnerability Testing Campaign

ADDITIONAL SERVICES

Document support	SGS will provide support in the creation of relevant documents. This support will take the form of document assessments, trainings and workshops on the document requirements as well as verification of document content (document review)

BRIGHTSIGHT.COM

GET IN TOUCH FOR MORE INFORMATION

+31 (0)15 269 2500
brs.sales@sgs.com
brightsight.com

FOLLOW US

linkedin.com/company/brightsight

HEADQUARTERS

The Netherlands
Brassersplein 2
2612 CT
Delft

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

SGS brightsight