# CYBERSECURITY SOLUTIONS FOR INDUSTRY

## CONTEXT & CHALLENGE

Cyber-attacks are about to become more aggressive and complex, especially within the Industry 4.0 and IoT market. By 2020, around 50 billion connected products & technologies will be launched into markets, and more than one out of two devices will face a cyber-attack. It is critical for companies embarking on this digital transformation to clearly define their needs with regards to new technologies and decide how to integrate them in their value chain processes. Protecting your products and your business against cyber threats is becoming vital to prevent: human and production damage, loss of revenue, theft of data, environmental impact and notoriety.

## CYBERSECURITY PORTFOLIO

As a trusted third party, Bureau Veritas brings support to developers, manufacturers and decision makers targeting products more secure and performant throughout the whole lifecycle: from design to operations.

With Bureau Veritas, benefit from a single source solution provider addressing system, hardware, software, Iot, people and process. Whatever your needs and level of maturity related to your cybersecurity roadmap, our experts help you handle with the following aspects:

- Cybersecurity **conformity assessment**
  [diagnostic, threat analysis & risk assessment]
- **Certification** services according to standards
  [ISO 27001 IEC 62443, CYBER ESSENTIALS]
- Certification services according to Bureau Veritas Guidelines
  [BV-SW-200, BV-CAR-CYBERSEC]
- **Surveillance** audits
- **Testing** against known Vulnerabilities (CVE, CWE)
- Cybersecurity corporate framework **consultancy**
  [dedicated support, cybersecurity strategy, security by design, suppliers capability qualification and monitoring, EBIOS analysis]
- **Training** and awareness regarding IEC 62443 requirements and other standards

BUREAU VERITAS 1828
L C I E

BUREAU VERITAS 1828
BUREAU VERITAS

# IoT NEED SECURITY ASSESSMENT

## TESTING CONNECTED
## devices against known vulnerabilities

Automated framework for testing vulnerabilities detection & protocol implementation defects on communication channels (Zigbee, Bluetooth, Wifi, etc.) « BlackBox Approach »

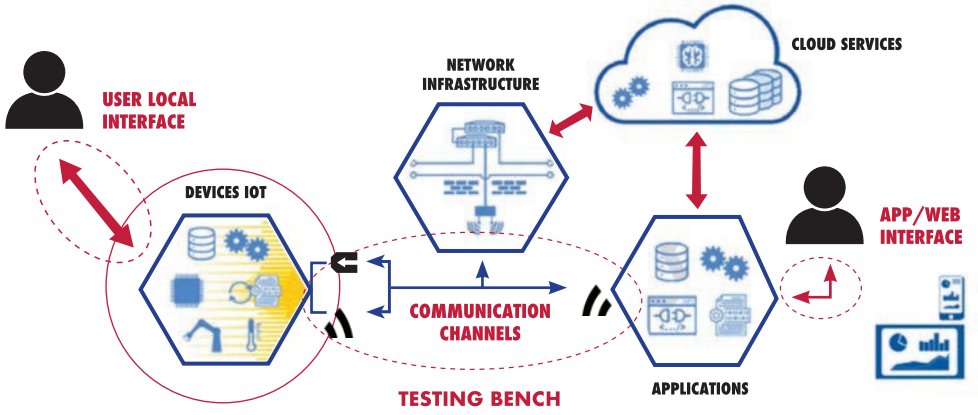
A. Defined approach to the nature of connected objects and their cyber risk profiles

B. Approach centered on the Communication Channel and its security

C. Categorization of security tests:

- #1 – Known Vulnerabilities *(generic)*
- #2 – Communication Channel Security Conformance *(generic)*
- #3 – Applicative Security Functions *(specific)* & Adaptability to different services *(safety targets)*

- Low to mid-end assessment complexity
- Fast in time
- New assessment service in addition to existing offers of safety / Conformity certification services
- Repeatable & reproducible evaluation
- A common understanding of minimum IoT security
- Monitor changes along with product evolutions




## EVALUATION STEPS

| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|
| CREATION | DISCOVERY | TEST PLAN CREATION | TEST PLAN EXECUTION | RESULTS | REPORTING | DELIVERY |

# IEC 62443 CERTIFICATION
# addressing production sites and industrial assets

The IEC 62443 is the KEY standard for cybersecurity which was originally developed for Industrial Automation & Control Systems. Today, it has been adopted by many sectors such as: Railway, Smart building, Smart city, Energy, Utilities, etc.

IECEE is an international system of conformity assessment schemes – in particular it specifies how to manage certification with the IEC 62443 standard. With a representativeness in more than 50 countries, its recognition is ensured for more than 30 years – on all electronical components.

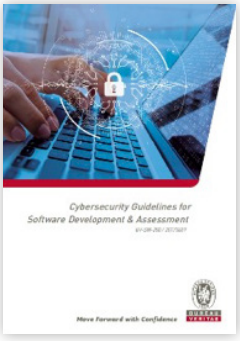
The starting point is always a risk analysis, to understand what to protect and with what level of protection. Then are implemented good practices such as: security governance, risk mapping and security systems, plan maintenance, tools detection, defense in depth, to finally achieve IEC 62443 certification to demonstrate your cybersecurity compliance.

Through LCIE, BUREAU VERITAS is a notified body able to certify industrial automations and control products and systems within this scheme.

## BV-SW-200

### SOFTWARE GUIDELINES DEVELOPMENT & ASSESSMENT

Bureau Veritas and CEA List built a cyber security guideline for software development and assessment addressing all domains (IoT, Automotive, Industry…). Download it for free: http://www.bureauveritas.com/white-papers/cybersecurity-guidelines-for-development-and-assessment-bv-sw-200




## WHY CHOOSE BUREAU VERITAS ?

- A world leader in Testing, Inspection and Certification
- Delivering innovative solutions in a cost-effective manner
- A global approach covering: people, hardware, software, process, system, OT (Operational Technology), IoT (Internet of things)
- A deep expertise: black box [securing end users] and white box [securing design and development]
- Third Party Laboratory providing impartiality, consistency and confidentiality
- Partnership testing with CEA Leti, CEA List
- International network of laboratories and technical centers
- Recognition from IECEE

BUREAU VERITAS 1828 — list cea tech | BUREAU VERITAS 1828 LCIE — leti cea tech

YOUR CONTACTS

TESTING SOLUTIONS
contact@lcie.fr - +33.1.40.95.60.60

ASSISTANCE & COMPLIANCE
software@fr.bureauveritas.com - +33.1.47.14.42.68