BUREAU VERITAS

CYBERSECURITY SERVICES

Secura
A BUREAU VERITAS COMPANY

BUREAU VERITAS

Cybersecurity Risks:
Past, Present and Future

Over the last decade, **it has become clear that cybersecurity needs to be addressed in a holistic way**. It is not simply a technological issue but rather a field that requires the constant and continuous involvement and commitment of multiple stakeholders and includes disciplines as diverse as physics and psychology.

There are many ways in which cybersecurity can be viewed in order to understand the subject better. One possible way is to look at **market-specific areas** such as **consumer products, medical systems, industrial control systems, automotive, networks and telecommunications,** etcetera. All of these possible domains come with their own relevant particularities, standards, regulations or focus points.

Ultimately, no matter how one chooses to visualize and categorize cybersecurity, one thing always stands out: attacks and attackers are becoming more sophisticated, the relevant threats and risks are present and growing, and developers and asset owners need to fight back by developing and implementing better security controls.

BUREAU VERITAS IS YOUR TRUSTED PARTNER TO HELP YOU TAKE CONTROL OF YOUR CYBERSECURITY RISKS

How to communicate & raise your **Cybersecurity Maturity Level?**

In this fast-paced ever-changing digital world, **you need to take control of your digital security with a holistic security approach** to meet the appropriate level of conformity from a **people, process and technology perspective**.

We achieve this through:

1. a comprehensive portfolio of cybersecurity assessment services per and across industries;
2. a set of accreditations and licenses to operate;
3. a global network of leading cybersecurity experts, extended notably through the acquisition of Secura in January 2021.

We focus our services on:

- **Industrial security** (OT)
- **Information technology security** (IT)
- **Connected products security** (IoT)

In the next chapters we will describe our services for each of these domains

86%
of breaches were financially motivated[1]

43%
Web applications were involved in breaches[2]

37%
Of breaches stole or used credentials[3]

1,2 & 3: https://enterprise.verizon.com/en-nl/resources/reports/dbir/

Table of Contents

1. Industrial Security (OT) **4**

1.1 Critical Infrastructure and Cyberphysical System **5**

1.2 Industrial OT Security Services **6**

2. Information Technology Security (IT) **8**

2.1 The Backbone of Technology Development **9**

2.2 Information Technology (IT) Security **10**

3. Connected Products Security (IoT) **13**

3.1 What are the Relevant Standards, Certifications & Regulations? **14**

3.2 Connected Products Security Services **15**

3.2.1. Consumer Products **15**

3.2.2. Medical Devices **16**

3.2.3. Network and Telecommunications Equipment **17**

3.2.4. Connected Vehicles **18**

3.2.5. Industrial Products **19**

1. Industrial Security
(OT)

1.1 Critical Infrastructure and Cyberphysical Systems

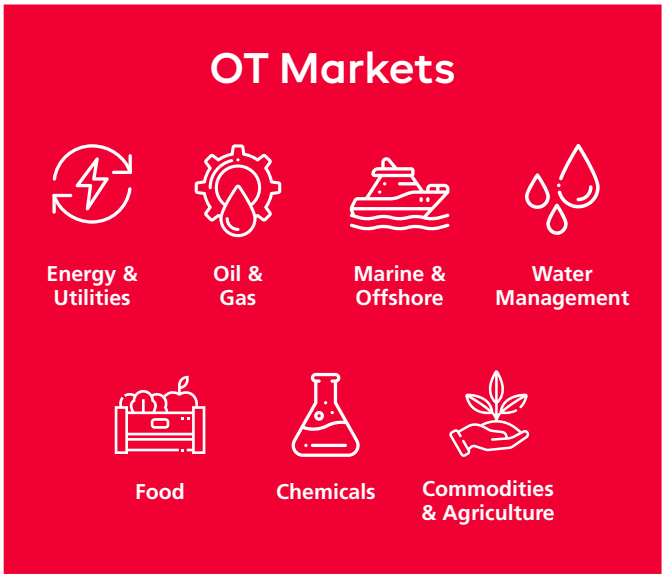
Industrial organizations are of vital importance to our society. Whether you operate an energy company, an oil & gas distributor, a water management organization, a chemical plant or a railway: all such critical infrastructure is controlled through operational technology (OT) and information technology (IT) systems.

In industrial organizations, **safety, reliability and availability** are of utmost importance. The vision of Bureau Veritas for OT and IT is: there is no safety, reliability and availability without cybersecurity. It is therefore fundamental that such systems are protected from attackers, including those who have an interest in degrading national security.

Digital security is of increasing importance, because more and more OT/IT systems (PLC's, ICS/SCADA devices and supporting components) are connected to IP networks. For instance to monitor and control processes, (predictive) maintenance or billing purposes. Moreover, with "Industry 4.0" (IIot) we see many new, smart and data-driven systems and infrastructures being developed. This has great advantages, but introduces significant risks as well.

All your systems, sensors and networks need to be sufficiently protected. Cybercrime is growing, especially in the world of industrial infrastructure. Nation-state actors have already used cyber attacks to sabotage industrial infrastructure, hitting for instance energy production (in the Ukraine) or oil production (in Saudi Arabia). Criminal ransomware gangs are moving into the industrial space also.

Regulators see the need for better security in the world of industrial organizations. In Europe, the Network and Information Security (NIS) directive was adopted by the EU parliament in 2016 and converted to law in most European Countries in 2018. This is complemented by ENISA guidelines and by the IEC 62443 standard. In the United States several guidelines and standards in the domain of OT and ICS/SCADA were released by the NIST, NERC and the DHS. In the maritime industry, IMO has also released some guidelines for ships in service that should soon be expanded to requirements for newbuilts. This snapshot of regulatory developments illustrate that regulations exist and are supported by sufficient standards and guidelines on how to assess and improve the security of industrial infrastructure.



1.2 Industrial (OT)
Security Services

There are many legacy systems, which were never designed to be connected to networks and/or the internet. Many installations need to operate without interruptions. Sometimes it takes years before systems can be patched. This results in many challenges in the world of industrial infrastructure. Bureau Veritas' portfolio of services focused on Industrial security aims to cover both IT and OT specific services, based on the three pillars **"People", "Process" and "Technology".**

People

- Security Awareness and Behavior (SAFE including an OT e-learning module)
- Phishing tests
- Social Engineering
- Training Courses: ICS/SCADA Security and hands-on training
- Secure Software Development Lifecycle (SSDLC)

Security Awareness in OT

Good security, as does good safety, starts with strong awareness of the applicable threats and risks. The awareness service offered by Bureau Veritas (**SAFE**) is designed not only as an awareness training, but as a program aimed to achieve behavioral change. The main pillars that the program aims to address are the ability of people to understand the risks, their motivation to adopt a certain behavior and the opportunity of performing an action. The SAFE program can be executed for an entire organization, as well as for selected focus groups, and the outcome includes a clear insight into the current status and into which of the factors require extra attention.

Process

- IT/OT Security Maturity Review including roadmap creation
- NIS / WBNI Compliance Review and Assessment
- IT/OT Risk/Site Assessment – Per site security assessment against relevant standards (IEC 62443 and others)
- Design Review / Threat Modeling / Code Review
- Definition of OT Governance (strategies, policies and processes)
- Definition of Incident Response Planning and Business Continuity Planning
- Support in building OT cyber security teams and a cyber-ready governance structures
- Support in OT cyber tenders: technical specifications for RFPs, evaluation of offers, etc.
- Vendor (3rd party) Review/Assessments
- Maritime cybersecurity assessment and classification

OT Site Assessments

The OT site security assessment follows internationally recognized standards and best practices such as **IEC 62443, NIST SP 800-82 and ALARP** which are specifically tailored to industrial control, automation and other systems.

The OT site assessment is specifically designed to identify site-level risks as opposed to organizational level risks. The OT risk assessment service is tailored to the foundational requirements of the IEC 62443 standard and addresses subject areas such as insider threats, external exposure, OT network traffic analysis, cyber resilience, data exfiltration risks and network/system security.

OT Red Teaming

Red Teaming allows a full spectrum cyber-attack to be simulated in an OT-environment. Such an exercise provides detailed insight into the attack paths that external attackers have, and also trains cyber defenders.

How would an attacker approach our critical infrastructure, could we detect this early enough, what are our weaknesses and how can we fix them? If these are questions that you need to address for your industrial environments, an OT Red Teaming exercise can be the answer.

Technology

- Threat Modeling, Design/Capabilities Review, Configuration Review, Code Review
- Red Teaming in OT environments
- IT/OT Vulnerability Assessments (penetration testing, robustness testing)
- Detection and response capability and maturity testing

2. Information Technology Security (IT)

2.1 The Backbone of Technology Development

We depend more and more on IT to manage our key business processes in our companies, to perform our work and also at home. Everything is connected through IT systems, networks, software and the internet.

Security and privacy are of crucial importance in our new way of living, considering that there is a constant threat that criminals can abuse vulnerable products and services. They may compromise our systems at work or at home and obtain intellectual property or our personal data. They may commit fraud or misuse our infrastructure to attack other systems. Security and data protection are therefore of increasing importance.

Software developers and manufacturers need to take care of the security of their products and services. When it comes to software, it is strongly recommended to start early on in the software development life cycle, and to have an independent security assessment carried out at least once a year.

In addition, the organization must actively deal with information security and prevent its intellectual property from being stolen. How to secure your organization and systems? There are many standards, best practices and guidelines which can be used to ensure security within an organization, a product or a service, such as **ISO 27001, ISO 27017 for Cloud Security, PCI/DSS, OWASP Guidelines, NIST Guidelines and the CIS baselines** for secure configuration.

Regulators also focus more and more on the domain of (cyber)security and privacy. In Europe, privacy is regulated through the General Data Protection Regulation (GDPR). Operators of Essential Services (OESs) and Digital Service Providers (DSPs) have to comply with the EU Network and Information Security (NIS) directive. The USA and the EU regulate the security of medical devices through various directives and regulations. UNECE helps regulating the security of new automobile types. Over time we expect more regulations to come into effect which push us to develop and maintain more secure products and systems.

So, for business reasons and for compliance reasons it is key to secure products and systems to well-defined levels and assess conformity to those levels.

2.2 Information Technology
(IT) security services

How to Secure your organization? Bureau Veritas is your security partner in the world of information technology. Our portfolio of services focused on IT security aims to cover all IT services, based on the three pillars **"People", "Process" and "Technology"**.

People

- Security Awareness and Behavior (SAFE e-learning modules)
- Phishing tests
- Social Engineering
- Training Courses (e.g. Cloud Security, Mobile App Security, Hands-on Hacking)

Process

- Information Security Management System implementation (ISO 27001, ISO 27017, ISO 27018, ISO 27031)
- IT Service Management Systems – ISO 20000-1 ITSMS, ITIL, TickIT
- TISAX, eIDAS Certification
- Security Maturity Review
- Risk Assessments
- Vendor Security
- Privacy / Data protection / GDPR services / ISO 27701
- ISAE 3000 / 3402 Assurance
- Forensics Readiness

Security Training Courses

One of the best ways for an organization to improve its security posture is enhancing their technical knowledge. Bureau Veritas can offer a broad range of training programs, with a dedicated focus on cybersecurity. Trainings can be provided for instance for **threat modeling, mobile application security, cloud security or hands-on hacking.**

Risk Assessments

Organizations with critical business functions face endless security threats that can range from vandalism, theft, on-site security breaches, insider risk, and even terrorism. Concerns can be whether their **crown jewel**s are sufficiently protected from various threat actors such as organized crime, industrial espionage, malicious insiders or hacktivists. These threat actors bring various threats forth such as theft of intellectual property, corporate secrets or financial information and disruption of business operations.

Our Risk Assessment services adheres to internationally recognized standards on information security such as **ISO 27005, COBIT 5, and the NIST Cyber Security Framework**. Risk Assessments are specifically designed to help organizations in identifying security risks in an early stage and to recognize and resolve previously overlooked blind spots.

During the risk assessment, many areas are covered, including: environmental security assessment, physical security, asset management security, access control, privacy and data, human resource security and communications security.

Technology

- Threat Modeling / Design Review / Code Review
- Vulnerability Assessment & Penetration Testing
- Cloud Security testing
- Red Teaming
- Secure Software Development Lifecycle (S-SDLC)
- SIEM/SOC Testing

Vulnerability Assessment & Penetration Testing

Regardless of the application, data is accessed by authorised users through applications that contain business logic and security functions. If any weaknesses exists in these access layers, then risks exist. In order to be in control of these risks, it is necessary to assess the security measures by testing their effectiveness in the same way that hackers or criminals do.

Within Bureau Veritas' **Vulnerability Assessment and Penetration Testing (VA/PT) service**, various tooling and stages are employed, such as for reconnaissance, vulnerability assessment and exploitation.

The outcome of the security tests are recorded in a clear, written report with a concise management summary, an extensive risk analysis for each outcome and recommendations on a strategic, tactical and operational level. VA/PT serv ices can be performed in several manners, including **Black Box, Grey Box and Crystal Box,** depending on the volume and type of information that is available to the testers at the start of the investigation.

VA/PT services are essential to any organization offering online services using web technology, as well as for organizations with business critical functional on an internal corporate network.

IT Red Teaming

With a large number of risks that belong to the category of **'unknown unknowns'** and pushed by sophisticated cyber criminals and nation state threat actors, companies and states are combating an ongoing flood of attacks. Dealing with such events requires more than a dedicated Security Operations Center (SOC), it requires hands-on training and learning by doing. **An increasingly popular way of testing and training in a controlled way is 'Red Teaming'.**

Originating in the military arena, **Red Teaming** is a security discipline that is gaining popularity in all sectors of critical national functions, the financial sector, highly secured private companies and governments. **By simulating full-spectrum cyber attacks, defenders get to practice their detection and response capabilities against high impact, low frequency events.**

The Blue Team, responsible for defending, can be involved in various ways (or not at all). **The White** Team (the observers) can escalate and de-escalate when necessary.

With the experts of Bureau Veritas in the role of attacker, you can discover how well-prepared your organization is for real cyber criminals. You decide, in consultation with the red team, against which components of your digital business you would like to deploy a Red Teaming exercise.

Subsequently, the consultants will go on the attack and attempt to make off with the so-called **'crown jewels'** in any way possible (but controlled and managed for risks). Depending on the target, a mixture of offensive and testing techniques are used, such as phishing, social engineering, malware, compromising physical access controls, penetration testing and exploiting, etc.

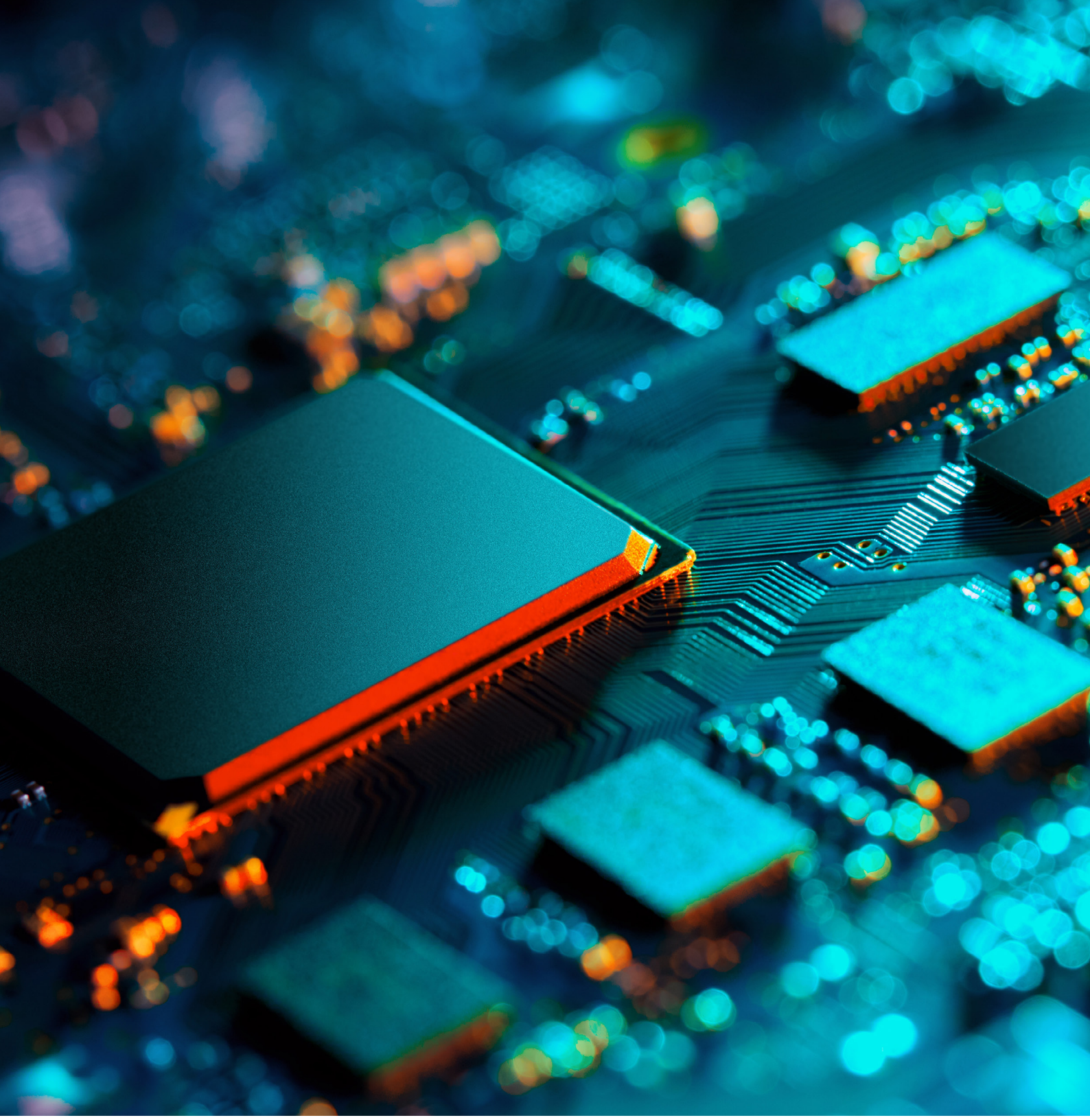
ISO 27001 Holistic Approach

ISO 27001 is the main global standard for Information Security Management. It describes how to organize information security in your organization and how to manage the risks. Bureau Veritas can help you to certify against this standard.

However, Bureau Veritas can do more for you:

- Security awareness of employees is a clear ISO 27k requirement. Therefore BV offers security awareness services, incl. assessments, e-learning, and other interventions to measure and improve awareness and secure behavior within your organization.
- ISO 27001 requires an organization to prevent the exploitation of technical vulnerabilities. This can be done through our Vulnerability Assessment and Penetration Testing Services, for instance by periodically testing the infrastructure and external web interfaces of your key assets (also for mobile apps and software in the cloud).

As you see we approach security holistically: it is a matter of People, Process and Technology.



3. Connected Products Security (IoT)

3.1 What are the Relevant
Standards, Certifications & Regulations?

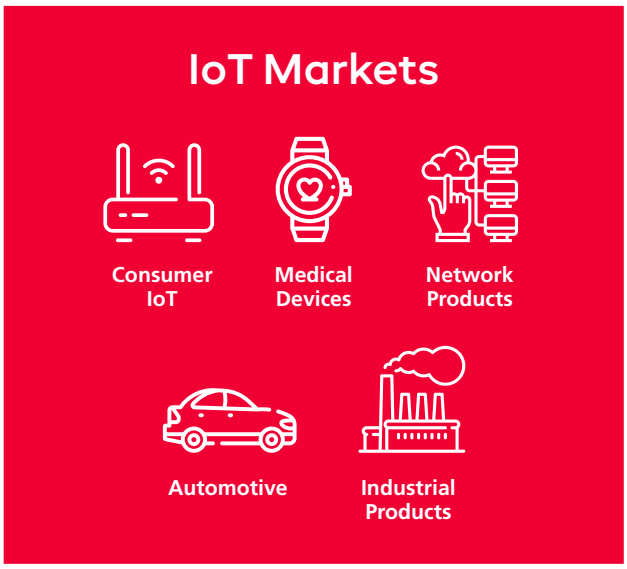
With the introduction and continuous expansion of the Internet of Things (IoT), the world becomes more and more connected. The combination of **"smart" devices, mobile or web applications** used to interact with them and cloud services allowing them connect with each other lead to the development of overlapped IoT ecosystems.
Historically, the world of IoT products has been driven in the past years strongly by functionality. However, we are at a point where cybersecurity issues associated with these products are not theoretical anymore, and can very well impact the products that we use in our daily life.

Currently, there are multiple internationally recognized standards, frameworks and certification schemes that could help manufacturers decide which set of security functionalities they would like to include into their products. For instance, the **IEC 62443 family** has become the reference standard for industrial cybersecurity, covering components and systems. **ANSI UL 2900** is seen as a reference family for security in medical devices. **ETSI EN 303 645** is a recently finalized standard seen as the main reference for consumer IoT products. Finally, **ISO SAE 21434** is becoming a recognized standard for cybersecurity processes and functionalities in connected vehicles.

From a regulatory point of view, cybersecurity is also seen as a leading topic, with the first examples already in place, or in a final drafting state. Connected vehicles have their cybersecurity and software updates processes and functionalities mandated through the international **UNECE regulations.**

Medical devices need to pass extensive requirements in order to enter various markets, including the USA (**FDA regulation**) and EU (**MDR regulation**). Finally, regulatory requirements targeting the area of consumer products will be set in place through the **Radio Equipment Directive (RED).**

Bureau Veritas has a solid view on the standards and regulatory landscape across IoT, by actively researching and contributing in this field. Because of this, we are happy to support IoT product manufacturers with the best options of security compliance, tailored to their specific needs.
To conclude: Bureau Veritas helps you to verify the cybersecurity on your product at each stage of your development with consultancy and offers a Cybersecurity Assessment program for Connected Devices, to help address these concerns.



3.2 Connected Products
Security Services

Bureau Veritas is your partner in the world of product security evaluation, compliance and certification. Our portfolio of possible services includes a broad selection of standards and certification schemes, covering multiple product domains. Because of this, we define our services in line with Development, **support and preparation, Compliance and Testing and Certification**, for various types of connected products. This is summarized below.

3.2.1. Consumer Products

For most of the time, consumer products have been regarded and rated only based on their functionalities, and of course their price. However, recently discovered security vulnerabilities and attacks on such products such as the Mirai botnet are making users more aware about the cybersecurity risks. Moreover, the fact that these products are connected to the same network to which other sensitive services or data is being stored or processes, makes their security impact much larger. Developers and architects determine the security of these products, and international standards and best practices are the best ways to guide security implementations.

Bureau Veritas can support with testing and certification based on the most relevant international publications in the domain of consumer products.

Consumer IoT Certification

Consumer IoT products need to have a very well-thought-out approach towards security assessments and certification. It requires efficient and effective testing, with limited effort and costs. Moreover, such a certification program needs to take into account the high-paced software update process associated with these products. Certification for IoT products (based on **Common Criteria or ETSI EN 303 645**) is currently voluntary.

On the other hand, there are international discussions on mandating (by regulation) a minimum of security features linked to these connected products. For example, in the EU, the **Radio Equipment Directive (RED)** will shortly incorporate requirements linked to cybersecurity. These requirements will ask for protection of software updates, confidentiality of personal data, as well as protection against malicious impact on the other components connected to the same network.

Bureau Veritas can support with consumer IoT certification based on ETSI EN 303 645 and Common Criteria, as well as tailored testing in line with the security requirements of the RED.

Development, Support & Preparation

- Design reviews
- Security Requirements development
- Threat Modeling
- Vulnerability assessments and penetration testing of hardware, software and infrastructure

Compliance & Testing

- ETSI EN 303 645
- P-SCAN (product vulnerability scanning)

Certification/Regulatory

- BV IoT Class 1, 2 & 3
- OWASP
- IoXT
- CTIA
- ETSI EN 303 645
- Common Criteria certification
- Radio Equipment Directive (RED)
- EUROSMART IoT certification

Medical Devices Regulations Certification

Medical devices are among the products with the most extensive set of regulations regarding local market access. For both the EU and USA, but also many other regions and countries, local regulations need to be satisfied by the developers. While these regulations historically focused on the clinical performance of the products, recent updates to the **FDA and EU MDR** have introduced specific requirements linked to cybersecurity. Developers are required to compile an evidence file aimed to demonstrate compliance with these requirements. The requirements include compliance with development processes, risk assessment, but also state of the art security controls (using standards such as **ANSI UL 2900 and IEC 62443** as reference) and evidence of conducted testing.

Bureau Veritas can support manufacturers of medical devices with testing and certification of their products based on ANSI UL 2900 and IEC 62443. At the same time, support can be given for identifying compliance gaps with the FDA and EU MDR regulations, as well as consultancy in closing these gaps.

3.2.2. Medical Devices

Medical devices are one of the most high-risk type of products, due to their direct use in human health or vital functions. Due to this important aspect, such devices need to pass extensive regulations and certifications programs, which are aimed to validate their clinical performance. Recent security vulnerabilities which were exploited in practice on some medical devices (such as for example pacemakers) raised the awareness of the importance of cybersecurity.

In response, most of the regulatory initiatives have added cybersecurity to the list of requirements that need to be addressed by the manufacturers. Such requirements address both the processes behind the development of the product, as well as testing and validation of the implemented security features.

Bureau Veritas can support medical device manufacturers with the regulatory compliance for US and/or EU, as well as testing and certification based on the most relevant international standards.

Support & Preparation

- Design reviews
- Validation and penetration testing
- Code reviews
- Processes reviews

Compliance & Testing

- IEC 62443 compliance
- UL 2900 compliance

Certification/Regulatory

- UL 2900 certification
- Common Criteria certification
- EU MDR compliance gap analysis
- FDA compliance gap analysis

Support & Preparation

- Design reviews
- Validation and penetration testing

Compliance & Testing

- IEC 62443 compliance

Certification/Regulatory

- Common Criteria certification
- BSPA certification

3.2.3. Network and Telecommunications Equipment

Network products and systems can be seen as the backbone of what we call IoT. While the "things" in IoT are related to the end products, it is network components and infrastructures which ensure that the products can connect and interact with each other in a proper manner. Due to this reason, the quality of the functionality of these products is essential.

Moreover, their security is critical as well, especially when we think about industrial or enterprise routing elements, on which the functionality or availability of a network depends. Due to this reason, network devices are among the products which are the most suitable for security testing and certification. Bureau Veritas can support with an extensive set of standards and security certifications for your network products and solutions.

Common Criteria Certification

Common Criteria (CC) is one of the most famous international certifications for products, being recognized across all continents and in more than 30 countries. CC can be applicable for a wide range of products, including software solutions, connected products, network and telecommunications equipment, etc. Only in 2020 there were more than 370 products which received the Common Criteria certification worldwide.

A CC evaluation can only be performed by a recognized laboratory, which ensures the value and high-quality of the test results. The resulting certificate can be used to increase market visibility, gain an edge over competitors, or satisfy specific requirements from local governments or high-end asset owners and integrators.

Bureau Veritas can support with Common Criteria certification on a wide range of products, including software, network equipment, medical and industrial devices or consumer IoT products.

Support & Preparation

- Review of processes and consultancy in drafting/ implementation
- Workshops on cybersecurity and regulatory requirements
- Risk assessments on vehicles and components
- Penetration testing of components and systems

Compliance & Testing

- ISO/SAE 21434 compliance gap analysis

Certification/Regulatory

- UNECE Cybersecurity (R155) and Software Updates (R156) compliance gap analysis
- UNECE Cybersecurity (R155) and Software Updates (R156) type approval
- Common Criteria certification

3.2.4. Connected Vehicles

Modern vehicles include hundreds of connected components (ECUs) which have the mission to monitor and control the implemented functionality. While some of the ECUs are responsible for the operation of the main vehicle functionalities such as brakes or engine, others are linked to modern functionalities such as infotainment, vehicle to vehicle, vehicle to infrastructure, etc.

In total, all of these components together need to be robust and well designed from a cybersecurity point of view. In light of recent demonstrated security attacks on cars, cybersecurity is an element that became mandatory also in the landscape or international vehicle regulations. Bureau Veritas can support you along the way with consultancy in the development of the security features, as well as review of the processes and official regulatory audits.

UNECE Vehicle Regulations

The latest **UNECE regulations – on Cybersecurity (R155) and Software Updates (R156)** – were created to keep track with the threats associated with a modern vehicle. Such vehicles are designed to facilitate a broad range of external interfaces, car to car and car to infrastructure connectivity, as well as support for (Over The Air) software updates. The regulations put equal emphasize on the processes used by the OEM during the whole life cycle of the vehicle, as well as the testing and validation on the vehicle type itself. A typical audit in line with these regulations will contain a special focus on the documented and implemented services, as well as testing by sampling.

As an entity involved in the development and testing of the new regulations since their draft state, Bureau Veritas can support with a wide range of services, including gap analysis, consultancy and support in implementation, as well as official type approval audits.

Support & Preparation

- Design reviews
- Validation and penetration testing
- Review of development processes
- IEC 62443 workshops

Compliance & Testing

- IEC 62443 compliance

Certification/Regulatory

- IECEE certification (IEC 62443)
- Common Criteria certification

3.2.5. Industrial Products

The industrial connected products are sometimes referred to as Industrial IoT or IIoT. All these components feature in modern times multiple interfaces, both wired and wireless. The special thing about industrial components and systems is that they need to be reliable over a large period of time.

An industrial plant will not expect to update or replace the components or their systems every couple of years, therefore the capability of these products to be resistant to attacks, and also adapt and respond to future vulnerabilities is essential. Because of this, industrial products need to be secure along the whole life cycle, which includes their out of the box security capabilities, as well as the software updates and patch management processes. There are multiple relevant standards and certifications which can highlight the security embedded in such products, and Bureau Veritas can support you along the whole process.

IECEE Industrial Products Certification

IEC 62443 has been established as the reference standard for cybersecurity in the industrial domain. This standard comes with a holistic approach, providing requirements for the industrial components (e.g. PLCs, HMIs, industrial routers, etc.), as well as for the larger industrial systems. The development and deployment processes are also covered by the standard.

On top of it, developers and integrators can certify their products, processes or solutions based on the **IECEE scheme**, in line with the IEC 62443 requirements. An IECEE certificate will demonstrate that the products, process or solution has passed an extensive evaluation program, which included documentation review, testing and process auditing. Bureau Veritas can support along the whole IECEE certification process, with initial preparation, the evaluation work, and the certification step itself.

Want to learn more about our **Cybersecurity services?**

Bureau Veritas is a Business to Business to Society company, contributing to transforming the world we live in. A world leader in testing, inspection, certification, we help clients across all industries address challenges in quality, health & safety, environmental protection and social responsibility.

For more information, contact us today:

Secura: A Bureau Veritas Company
Karspeldreef 8
1101 CJ

Amsterdam
THE NETHERLANDS

W: www.secura.com

Bureau Veritas
Le Triangle de l'Arche
8 cours du Triangle
CS 90096

92937 Paris La Défense Cedex
FRANCE

W: www.bureauveritas.com
E: cybersecurityservices@bureauveritas.com

As a global leader, Bureau Veritas provides the independent cybersecurity assessment services you require for your systems, assets and products - including your supply chain - to help you to take control of your entire digital security.

Follow us on

Secura
A BUREAU VERITAS COMPANY

BUREAU VERITAS
Shaping a World of Trust