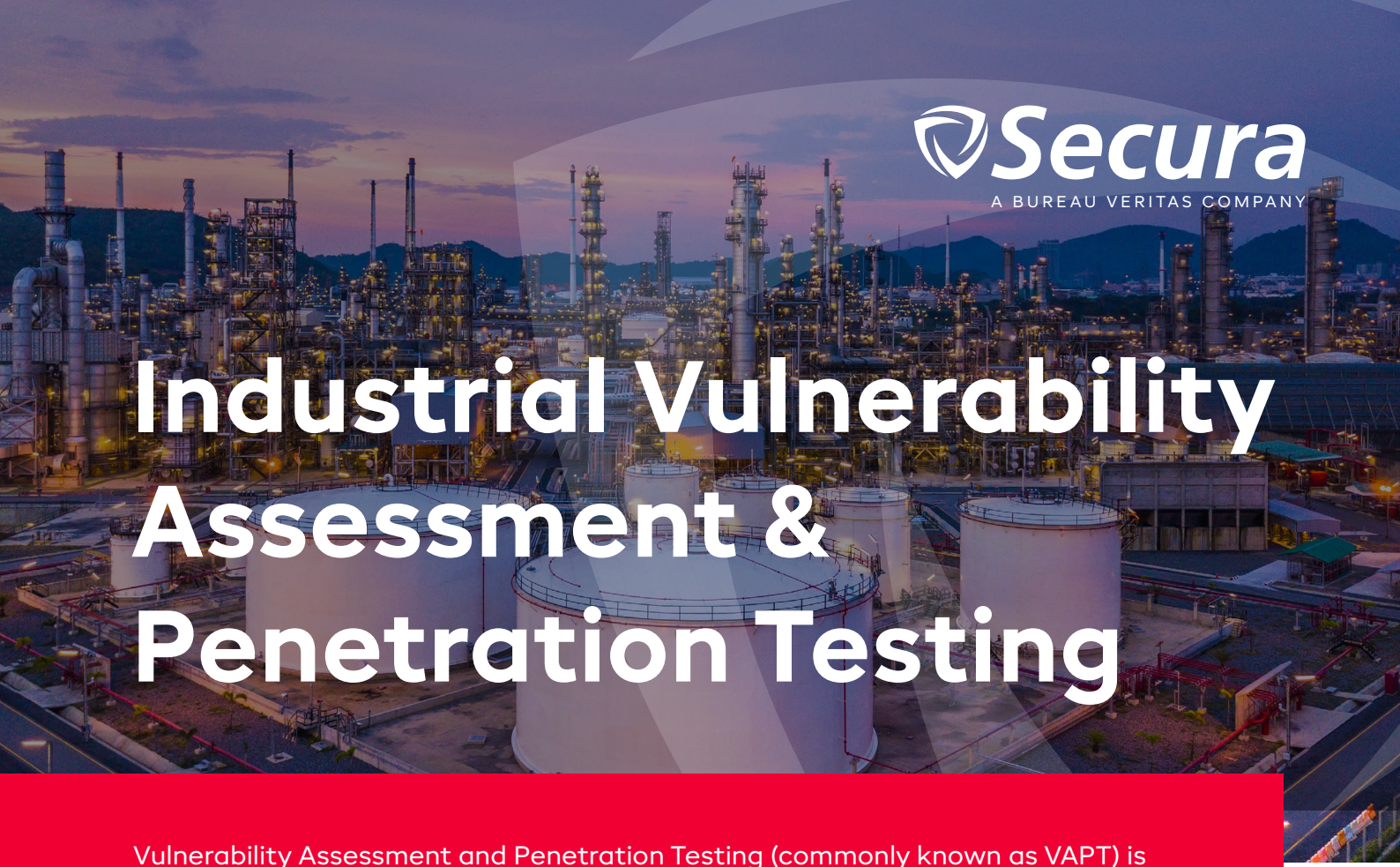


Secura
A BUREAU VERITAS COMPANY

Industrial Vulnerability Assessment & Penetration Testing

Vulnerability Assessment and Penetration Testing (commonly known as VAPT) is one of Secura's most valued services and the service with the longest history within Secura (since 2000). **Our services span all domains, from IT and OT to IoT, and encompass a huge variety of types of tests.** Within industrial environments, these tests require a specialized approach. This is mainly due to the different risks and threat models within Operational Technology (OT).

Vulnerability Assessment & Penetration Testing

There are many types of testing that are collectively known as **'Vulnerability Assessments and Penetration Testing' (VAPT)**. Classical **'Penetration Testing'** means that tests are performed from the perspective of an attacker, and vulnerabilities are exploited to see **'how far can an attacker get'**. However, this is not always the most effective way of testing because **it often makes more sense to perform a Vulnerability Assessment:** test in such a way that as many vulnerabilities as possible are found without wasting time trying to exploit them to see how far you can get. Finding more vulnerabilities is often more valuable because it allows to reduce risks more effectively: **exploring wide, instead of (only) deep.**

What is the value of Industrial VAPT?

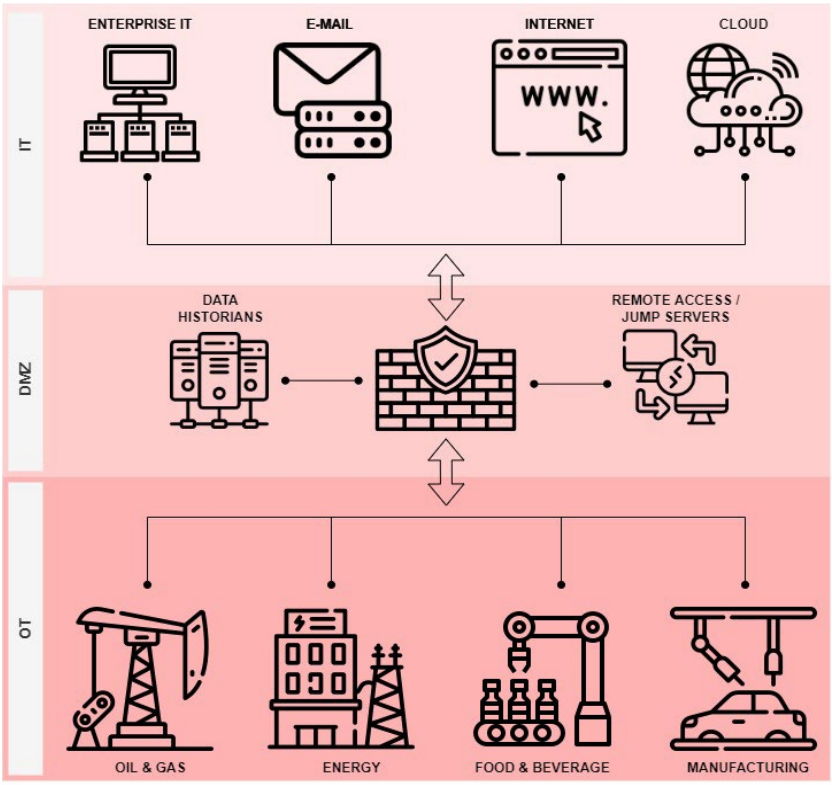
The aim of a penetration test is to illustrate as clearly as possible what **the consequences of a certain issue with your cybersecurity** could be, and **what that would mean to your organization**. For example, the risk that an IT security incident, like ransomware, could also affect the OT network, threat actors breaking into the OT network to access intellectual property, supply chain risks caused by remote vendor connectivity or the potential impact of a cyber-physical attack.

VAPT provides insight into the current cyber resilience of the IT and/ or OT networks for these kinds of threats and if improvements might be required. Secura records the outcomes of the VAPT test in a clear report with a concise management summary, an extensive risk analysis for each outcome, and recommendations on a strategic, tactical, and operational level. The results of the assessment can be used to **take steps to close security gaps and reduce the risk in your organization.**

What is different for the industrial sector and why is this important?

Within industrial environments many critical business processes depend on OT. Networks with **Industrial Controls Systems (ICS)** such as **DCS, PLC's and SCADA systems** manage and automate critical processes. Still, the enterprise IT services are just as important for daily operations. Moreover, due to the convergence of IT and OT and Industry 4.0-initiatives, the dependency between these two environments is also increasing. In the end a successful business depends on reliable systems in both IT and OT and therefore VAPT testing is important for all these systems. As different technologies are used across these environments, and it is collectively known that **OT systems might not be resilient against VAPT scans**, it is obvious that each area requires a different approach.

Scoping the VAPT assessment is therefore very important. The different approaches for specific parts of the infrastructure are briefly described below by using a common reference model. In reality, each infrastructure will different and therefore Secura will always start by reviewing the network topology together with the customer to tailor our approach to the systems in scope.



INFORMATION TECHNOLOGY (IT)

Industrial security is not the same as OT security. All industrial companies have a regular IT-network that is just as critical to their business as the OT network. VAPT testing in IT is one of the core capabilities of Secura and is this approach is described in more detail in our VAPT factsheet.

Besides all the regular components found in any modern IT-network (and their related vulnerabilities), industrial organizations might face additional challenges. Services that depend on data received from the OT layer or vice versa. A good example is a connection between the **IT ERP system** and **OT applications**, often using **unencrypted SQL or HTTP connections**.
Even **OT-cloud services** or **OT-remote access** might be routed through the IT domain. This connectivity and dependency increase the risk that cyber incidents traverse between these domains. Incidents within the IT-environment could affect the OT-environment, but the opposite is also true.

This additional scope is added to our service portfolio. Of course, we can perform our regular VAPT services within the IT-domain but is also possible to extend this with the question if vulnerabilities in the IT-domain could be abused to reach or affect the OT systems. In this case we try to exploit the discovered vulnerabilities to gain access to servers in the IT/OT-DMZ or potentially directly in the OT network.

IT/OT-DMZ

This network zone is the separation between the enterprise IT-network and the OT-network. Often, this level consists of generic IT-components, but it could also contain specific OT-related applications, including specific OT communication protocols, like **Modbus, OPC** or **OPC-UA**. Some examples are: **remote access servers, patch update distribution servers** and data historian servers. It is often a crucial layer as this is one of the first layers of defense of the underlying OT-systems.

In general, these systems are more resilient against vulnerability scans. Therefore, we often suggest to make use of a "grey box" approach. We get some information in advance to prevent the use disruptive techniques on systems that might not be able cope with these attacks. At the same time most tests use a realistic "**hackers approach**". One of the main questions here is to check if vulnerabilities exist that could be leveraged by an attacker to **get access to OT-data or systems.**

During the penetration test we try to escape from the DMZ constraints, either by moving laterally to other systems in the DMZ, escalating privileges or by exploiting security or configuration vulnerabilities. We will investigate if it is possible to **manipulate communication between IT and OT** (like production setpoint changes, remote operations, etc.) but the ultimate goal is to **bypass the firewall and gain access to the OT domain.**

OPERATIONAL TECHNOLOGY (OT)

Within the OT environment, there are many more components like **DCS** controllers, **PLCs, RTUs, SCADA systems**, and possible other legacy systems that can't handle the disruptive scans or actions used during a conventional penetration test. Even a simple network scan could already be sufficient to disrupt the working of a PLC. This is one of the reasons why it's commonly said that it is not a good idea to perform VAPT assignments in live production networks. Meanwhile hackers might not know or care about this and we know that a lot of vulnerabilities exists in OT networks.

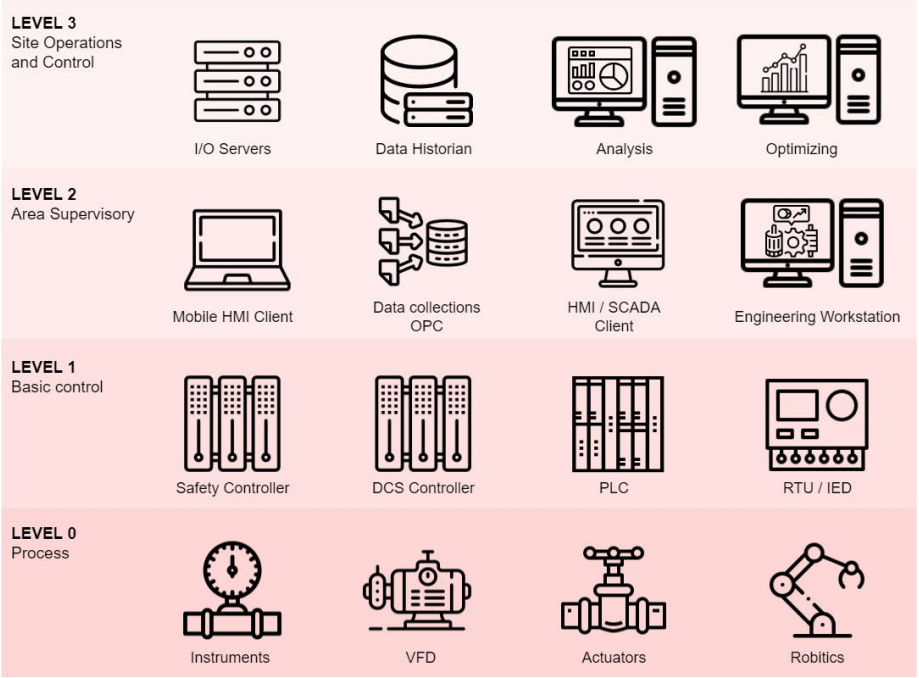
So, how can we manage this? Instead of just following the general consensus, Secura is experienced to **focus on tests that are possible in OT environments.** This totally depends on the specific infrastructure in scope but in general we prefer a "**crystal box**" approach. In this case the information about internal network is provided, maybe with some credentials and access to configuration examples. We need this information so we can tailor our approach for each device. A typical OT network consists of different levels (according to the **Purdue model**).

- **Level 0 – Process**
  This level contains devices that physically interact with the process. For example, field instruments, variable frequency drives (VDF), pumps, motors, actuators and robotics.

- **Level 1 – Basic Control**
  This level contains the controllers that interact with the field instruments and actuators. For example, DCS and Safety controllers, Programmable Logic Controllers (PLC) and Remote Terminal Units (RTU).

- **Level 2 – Area Supervisory**
  This level contains the devices used to monitor or interact with the controllers. For example, Human Machine Interfaces (HMI), Engineering workstations (EWS) and OPC data collectors.

- **Level 3 – Site Operations and Controls**
  This level contains system to support for site wide operations, maintenance and optimalisations. For example, data historians, I/O servers but also the more generic security services for the OT environment like Domain Controllers, backup servers and patch & AV distribution servers.



Our specific VAPT approach in the OT environment depends on which levels are in scope.

Purdue Level 2 & 3

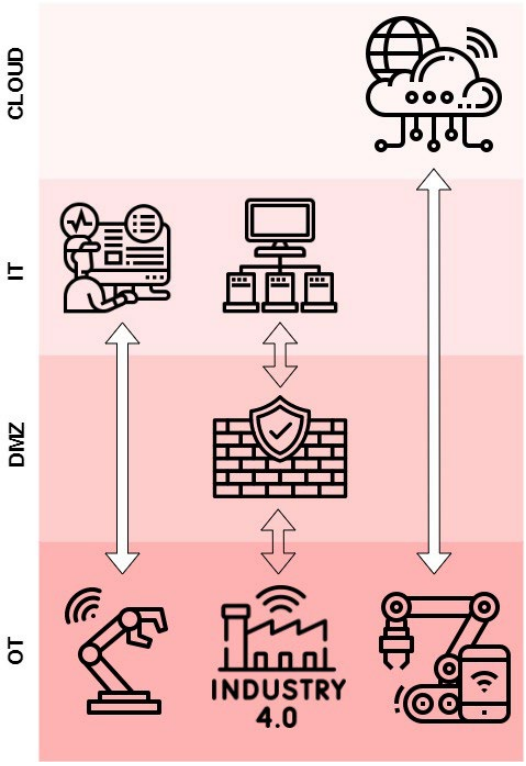
In general, systems that reside in Purdue levels 2 and 3 (Area Supervisory and Site Operations respectively) are based on generic IT components. Depending on the criticality of each system we can use more of less intrusive methods. Most often the question here is **to test how resilient the systems and network is against targeted attacks.** In these levels systems may also make use of OT specific protocols, like **Modbus, DNP3, IEC-101/104, CIP Ethernet/IP**, etc., to communicate to each other and to systems in the lower Purdue models. It is also not uncommon within OT environments that custom applications or solutions are installed on this level that might add an additional attack surface. **The ultimate question is whether it is possible for a hacker to move laterally over the network and to the deeper levels of the system**.

In the penetration test stage, we try to exploit vulnerabilities in the system configurations, installed (custom) applications, weak IT protocols like FTP, Telnet, HTTP and SNMP and the insecure industrial protocols. **The goal is to gain access to engineering workstations, SCADA databases or human machine interfaces** to investigate if we could influence the process.

Purdue Level 0 & 1

In level 1 (Basic control) and level 0 (Process) we will in general not use any intrusive methods unless it is specifically requested, for example when the system could also be operated manually or is not in active use due to a scheduled maintenance period. Often, **the question is if it is possible for an attacker to manipulate signals or measurements or carry out a cyber-physical attack**, especially when this level might also contain safety systems (SIS). It is also possible to research if these lower levels (that might be installed in unmanned remote locations) can provide access to higher levels of the OT network, and maybe even the IT environment.

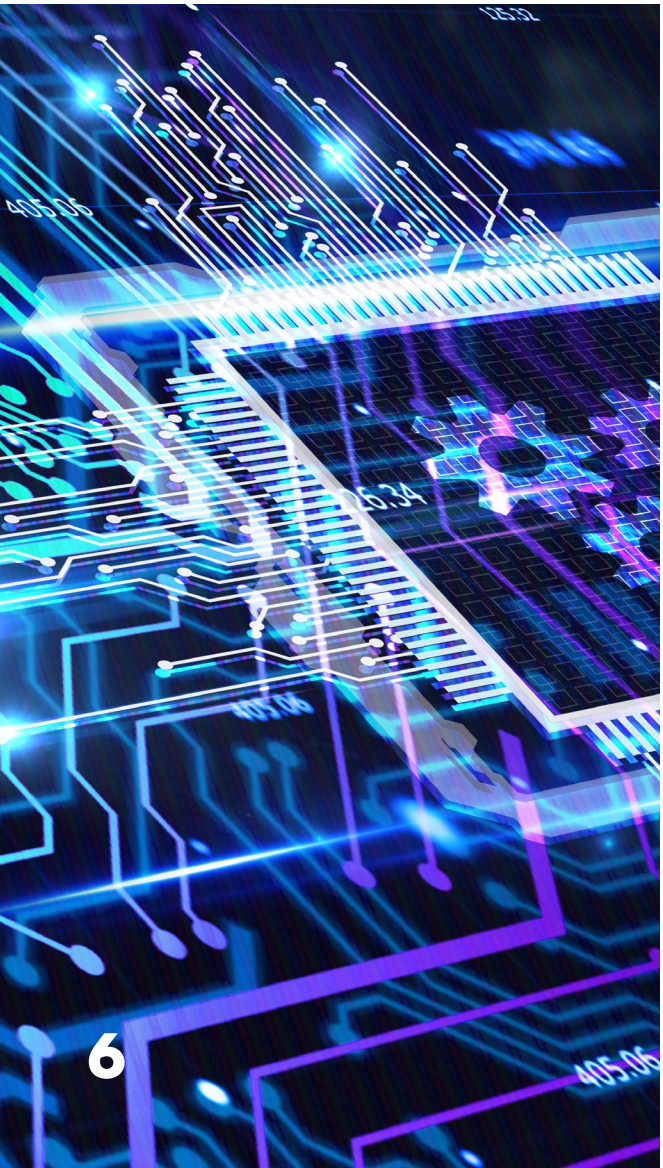
In these levels most of the communication is performed via OT specific protocols of which many are insecure. Some examples are, **Modbus-TCP, Fieldbus, Profibus, HART and many more**, including vendor proprietary protocols. On request we could, as part of the penetration test, investigate the possible vulnerabilities in these levels as well. We will try to **exploit vulnerabilities** in the used communication protocols, **potential vulnerabilities** in the controller's or device firmware or **abuse weaknesses** in the device configuration.



Connectivity

Finally, all these components are connected via network devices such as **switches, routers, firewalls,** and even wireless access points. On top of that it is also common that a lot of protocol and media converters are used in OT environments, like **RS-232/ RS-485 to Ethernet or Copper to Optical Fiber convertors.** All these intelligent devices generate additional attack surface. Network configuration and segmentation are key and therefore a good focus area for our VA/PT service. In general, these devices are resilient for these types of scans and will be included in the scope of regular vulnerability scans and tests.

During the penetration test we try to abuse weaknesses in the configuration of these devices or exploit potential vulnerabilities in the firmware to gain access to the infrastructure layer. **If succeeded it becomes easier to attack other parts of the network, manipulate network traffic to influence the process or eavesdrop on unencrypted communication.**



IIOT

A specific category are Industrial Internet of Things (IIoT) systems. More and more devices are becoming "smart" and sometimes this connectivity is even required from a vendor. Often only for remote "read-only" diagnostics but this is not always the case. Of course, IIoT is not necessarily a bad thing when it is properly and securely used for process optimizations. However, we need to keep in mind that these devices or services do not always follow the clear demarcation rules as previously described. **It's not uncommon that the added connectivity stays under the radar and creates a blind spot.** It's possible that local industrial equipment directly communicates to the cloud environment from a systems vendor or service provider using a cellular network. Other possibilities are the use of LoRa or Bluetooth connectivity bypassing all traditional layers of security.

As part of the penetration test, Secura is also able to test these devices, their communication protocols, webservices or companion apps. Moreover, we try to **leverage these connections to get access to the OT level.**

Different techniques used for OT systems

PASSIVE SCANNING

One of the techniques Secura can use in OT environments is passive vulnerability scanning. In contrary to normal (active) vulnerability scanning there is no (intrusive) traffic injected into the network to make sure even the most fragile systems are not affected. **Passive scanning is a "read-only" technique that makes use of a copy of already existing network traffic.** This traffic is analyzed and could expose vulnerabilities like weak protocols, poor configuration or outdated firmware.

The downside of this method is it is **less accurate and will not provide full coverage** (only devices in use at the time of testing will generate traffic to be analyzed). It will therefore require a bit more manual investigation to confirm the findings.

SELECTIVE SCANNING

On top of passive scanning Secura can, in collaboration with the customer, use specific and less intrusive active scanning techniques. These queries will be tailored to a single host or a selected part of the network. Parameters will be configured in such a way to prevent any overwhelming amount of traffic. **This technique is more accurate than passive scanning but it's time consuming.** Still, some devices like legacy PLCs should never be scanned when they are in production. It might however still be possible to perform these scans during a maintenance period or manual supervision, or if available, in a separate test environment containing the same types of devices.

The team

Secura has a **specific penetration testing team for the industrial market** which is formed by specialists with varying experience levels and specializations. Testers are certified to a minimum (IT) standard (eWTP) and often hold other certifications like **eCPPT, OSCP, GPEN** and many others. Moreover, they also have the experience to work in OT environments. Finally, the team also consists of certified experts in OT cybersecurity (**GICSP, IEC62443**). Therefore, all levels of VAPT services covering IT, OT, IIoT and anything in between can be covered.

Why Secura?

Secura believes it is important that OT security is addressed to the highest level achievable, considering the impact a cybersecurity attack may have on health, safety and the environment. We support organizations across various industries in their journey to improve their OT security. Secura is experienced in delivering security and visibility for some of the world's most complex OT networks including Europe's largest manufacturing facility and other various key players in critical infrastructure. We guide organizations in **understanding risks, gaps and vulnerabilities in industrial control systems** by using a layered approach considering the **NIS and NIST compliance frameworks** for critical infrastructure. The value of Secura comes forth in **approaching OT security from well-known and internationally recognized ICS standards** required by the regulations of various countries or distinct areas in the world.

Not only does Secura understand what is required by world's most known and accepted ICS standards, but our **team of experts also possesses the necessary engineering understanding to identify and interpret the impact of vulnerabilities** in distinct OT environments consisting out of Stand-Alone, Distributed and/or Supervisory Control and Data Acquisition systems. Secura **identifies threats and risks** to OT systems by continuously investing in the training and education of its dedicated consultants.

Secura requires that its consultants have the right **cybersecurity and engineering knowledge** including but not limited to control loops, plant organization (as per ISA-88), architecture, data flows, connectivity and commonly used diagrams such as process flow diagrams and piping and instrumentation diagrams to identify specific cyber risks related to PLCs, PACs, RTUs and Safety Instrumented Systems (SIS). The cybersecurity and engineering understanding of our consultants bring them at the forefront of OT security in the world translating to understanding the concerns of our clients and providing state-of-the-art solutions based on well-recognized standards for each distinct area of the world.

Secura
A BUREAU VERITAS COMPANY

Interested?

Contact us today:

Follow us:

+31 88 888 31 00
info@secura.com
secura.com

BUREAU VERITAS 1828

Shaping a World of Trust