Secura

A BUREAU VERITAS COMPANY

INDUSTRY 4.0: CHALLENGING CYBERSECURITY

Industry 4.0: Challenging Cybersecurity

The fourth industrial revolution, or Industry 4.0, is seen as the next step after the computer automated industrialization that happened during the last five decades. This new revolution is powered by buzzwords like IIoT (Industrial Internet of Things), integrated cyber-physical systems, big-data, A.I. (artificial intelligence) and digital twins. This is no different in the chemical sector. But no matter how a facility is made "smarter", all these technologies have two things in common: they are all data-driven and they require hyperconnectivity. These two properties represent the next big challenge for cybersecurity within these industrial environments.

Background

The demand for Industry 4.0 is clear. The drive within the chemical sector to improve is crucial. Moreover, the chemical industry also contributes to almost any other manufacturing supply chain so there is also lot of potential. Product improvements, increasing cost efficiency and business optimizations are some of the key drivers for this digital transformation. All the more reason to expect this trend will continue. But again, what about digital security?

Traditionally industrial control systems (ICS) or operational technology (OT) were strictly separated from the enterprise IT networks. The ICS Purdue reference model found its way too many facilities and describes a layered, well segmented network. One of the main reasons this is so important is the fact that many ICS components, like automation controllers, PLC's and SCADA systems were not designed with security in mind. They needed to be safe and reliable, security became an afterthought. Of course, there is more to cybersecurity than network segmentation. Standards like IEC 62443 define how a cybersecurity management system can be used to manage cybersecurity risks to acceptable levels. It could be debated if the current average security posture is already mature enough to withstand a cyber-attack like ransomware. Unfortunately, in practice we see many examples of the opposite being true.

On top of these challenges the Industry 4.0 initiative pushes forward to hyperconnectivity, which results in more exposure of OT networks, usage of more generic IT services and cloud connectivity, "bypassing" the traditional segmented references models. Again, this isn't necessarily a bad thing if cybersecurity wouldn't be an afterthought. Did we learn from the past or will we make the same mistakes again?

Table of Contents

Challenges Explained

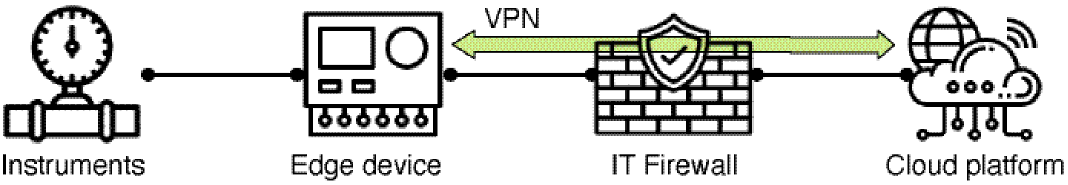
It is not always obvious that IIoT devices create new cybersecurity challenges as at first glance they often seem perfectly secure. Moreover, many IIoT vendors recognize the need of cybersecurity and deliver more secure and more capable devices. However, when poorly implemented or improperly maintained they can still introduce an unknown risk. These cyber risks could be generally divided into two types: the IIoT solution itself and the implementation of the solution.

Both use cases presented in this whitepaper are based on real scenarios encountered in the field. As the specific IIoT devices in question are not the main issue, they are not disclosed. The scenarios are derived from a chemical industrial plant based in the North of Europe. The facility itself is more than 12 years old, however in the last couple of years there have been several modifications and extensions where new sensors, PLC's and machinery of different manufacturers and suppliers have been installed. The IIoT solutions were part of these new additions.

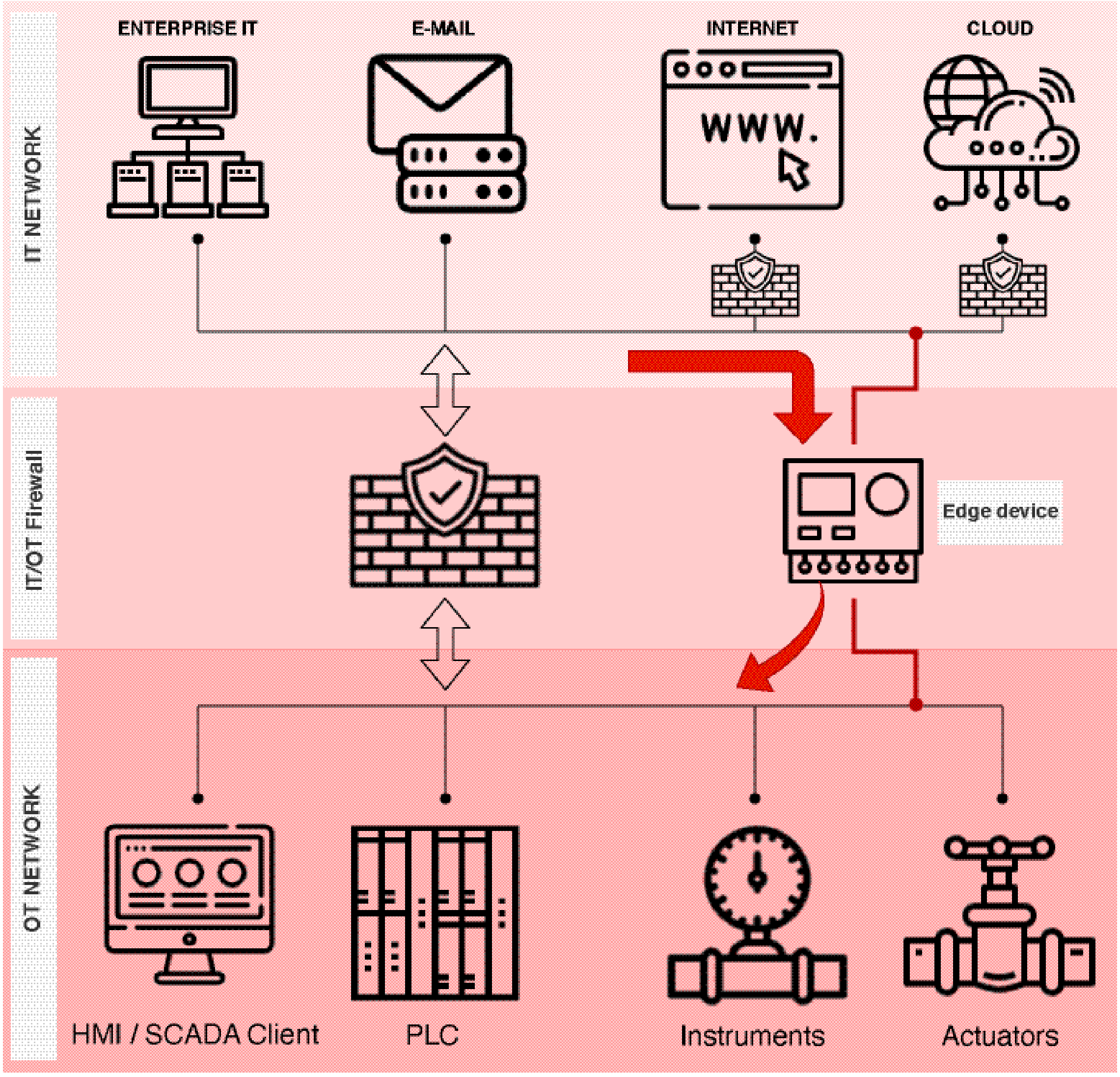
USE CASE 1: CLOUD DIAGNOSTICS

In the first example a solution is implemented to collect data from various OT instruments. A so called "edge device" collects the process and diagnostic data from the instruments and then sends it to a cloud application for analysis. Both the end-user and the vendor can make use of this cloud platform to perform condition-based maintenance or provide remote support.

The edge device was installed on the network with two separate network connections, a so called "dual-homed" system. It has one connection in the IT network to communicate to the cloud, and a second connection in the OT network to collect the information from the OT instruments. The cloud connection was also protected by a secure and encrypted VPN tunnel. Moreover, the edge device was configured to only send data from the OT network to the cloud, traffic to the OT network is not possible.



At first glance this seems to be a proper, secure, and well segmented solution. However, when the device is added to the overall network diagram it is obvious that it has the potential to create a bypass between the OT and IT networks. A detailed review and a network scan on the IT network exposed a running management service to configure the edge device. This was not known by the end-user and this connection was available for anyone in the IT network. It also became clear that the password required for access to the configuration was left in a default state which is easy to retrieve from vendor manuals. Moreover, the edge device was also running outdated firmware that contained publicly known security vulnerabilities. All these facts together provide a previously unknown attack vector on the edge device. This means that a hacker could potentially attack the edge device, log in using the default credentials, gain more privileges by abusing the known vulnerabilities in the old firmware and break-out to the OT network. This attack path is visualized in this network diagram.

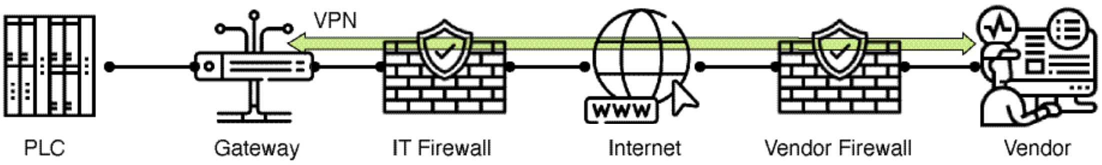


Please note that this attack path was not available via the cloud as that part was still secured by the VPN. However, because the edge device was not installed in a protected network zone, like a firewall protected IT/OT DMZ, this setup provided a potential bypass to jump from the IT to the OT environment. This issue was discovered by performing a threat model assessment in combination with a vulnerability assessment. These approaches are described in more detail in the solutions section.

USE CASE 2: REMOTE ACCESS GATEWAY

The second example is about a remote access gateway. This is a communication device that provides remote access and diagnostic data to a third-party vendor. In this case, it was part of the service contract that came with some heavy machinery installed in the factory. The vendor uses the remote access for remote maintenance and troubleshooting in case of any operational issues. The benefits for the end user are obvious: less downtime and a reduction of maintenance costs.

The remote access gateway was also configured and installed by the vendor in co-operation with the site maintenance team. The gateway creates a secure network connection to the vendor using a VPN tunnel with the strongest available encryption technologies.

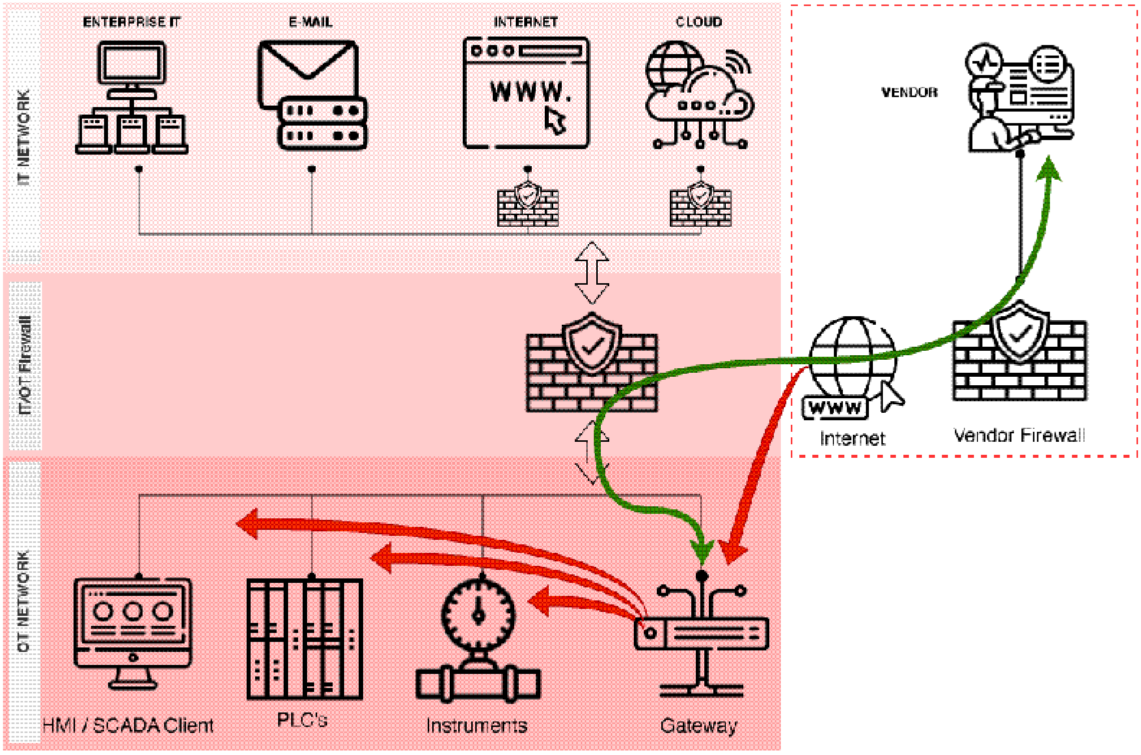


Again, this setup appears very secure on the surface. While the VPN tunnel itself is secure and protected, the way it was set up introduced multiple security issues.

The first issue was concerning the remote exposure. As the gateway needs bidirectional connectivity from and to the vendor network it was required to allow this traffic in the firewall. However, due to unknown reasons, the firewall was not restricted to only allow VPN traffic from that specific vendor, but it allowed all types of traffic and from anywhere on the Internet. Most likely this can be explained by the fact that there was not much focus on cybersecurity during the installation and commissioning of the heavy machinery, where the gateway was just a small part of the delivery. Another frequent reason for misconfiguration is that the solution is not working properly during commissioning and the firewall rules are relaxed as part of the troubleshooting. Afterwards, these settings remain. It is not uncommon that IIoT devices find themselves connected directly to the internet and eventually can be found with e.g., Shodan[1], a specific search engine for connected devices. There are even specific subsections dedicated to OT equipment and protocols.

The second issue was the configuration of the gateway. As this was part of the vendor's scope, this vendor was also responsible for the security maintenance and the configuration of this device. As all traffic to the gateway was encrypted by the VPN the end-user had no idea what the vendor could do on this device. After investigation it became clear that it was possible for the vendor to update the configuration and provide itself much more privileges then necessary.

Finally, the gateway feature was to provide remote access to specific components of the machinery in question. However, due to the poor implementation of this device, the gateway could also directly or indirectly access a lot more equipment. Moreover, due to the lack of segmentation of multiple network connections it was theoretically possible to connect to almost the entire OT network.



In this specific case no harm was done by the vendor as they had the best intensions, but this setup created a real attack path from the vendor network to the end-user network. These supply chain attacks are often ignored but could have the potential to provide easy access into an otherwise well-protected network. These issues were discovered by performing a design review based on the installation documents, network diagrams and system information as explained in the solutions section.

Solution

The best solution is to incorporate cybersecurity during the design phase of new projects, especially when IIoT or other remote connectivity is involved. This is not only applicable for new facilities but also for expansions or modifications to exiting sites. Of course, that is easier said than done. The OT network is not always suited to incorporate all technical requirements and at the same time the technical expertise might be lacking. Moreover, as most of these solutions are business or operations driven, they might overlook the cybersecurity implications during the project phase altogether. Finally, many different IIoT implementations that provide all kinds of connectivity may already exist in a facility in the maintenance phase or are sometimes even unknown to the end-user. In the next sections some possible approaches are described that provide a solution for these issues.

DESIGN REVIEW AND THREAT MODELING

During a design review all the available and relevant design documents are reviewed and discussed with the technical owner, solution architect and/or the vendor. It is important to notice that this approach is possible for both new facilities (CAPEX) as well as existing facilities (OPEX). Especially for the latter it is valuable to combine this review with a site assessment, which is explained in the next section. The benefit of a design review is that the security design can be independently verified against the company security policies, industrial standards and organizational and/or industry-specific best practices. Discovered design flaws, policy violations or deviations from these best practices could then be mitigated.

For threat modeling the same design information is used, however this assessment follows a different approach and uses a hacker's mindset. It is a structured methodology to map the threats of all possible attack paths on the subject in scope. During an interactive session a diagram is created that provides a complete overview of the attack surface and if any additional mitigations might be required.

Both the design reviews and threat model assessments[2] can be performed on existing environments but also, based on design documents, on new systems or system expansions. The second use case described above was discovered during a design review assessment. Finally, it is also worth noting that threat modeling will also provide very useful information for subsequent technical assessments, such as a penetration test, which is described in one of the next sections.

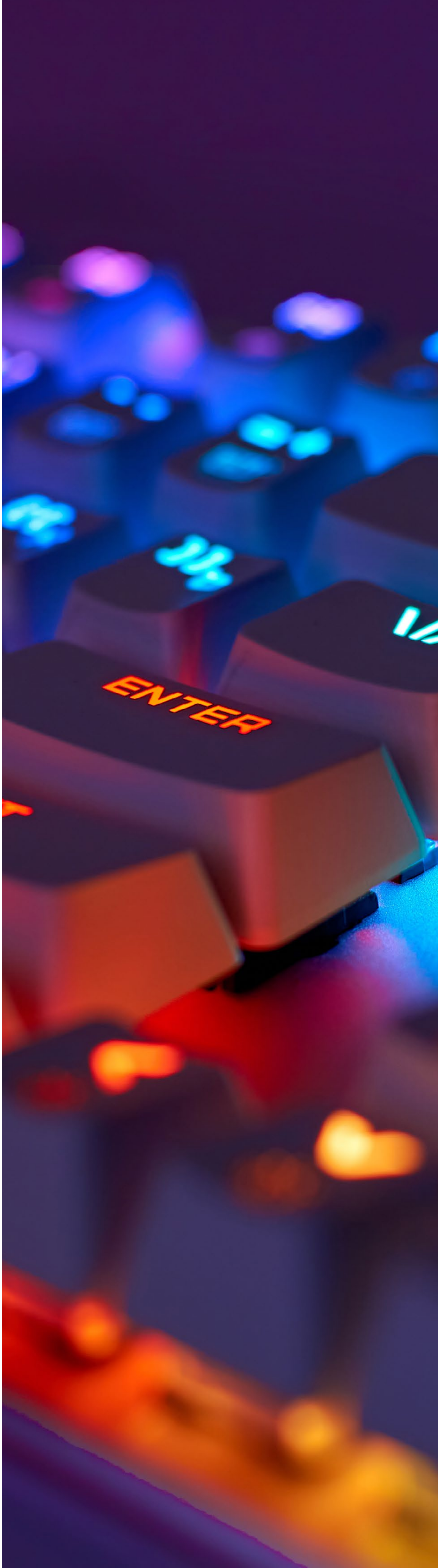
SITE SECURITY ASSESSMENT

A site assessment[3] follows a more practical and bottom-up approach to identify technical site-level risks. The design and architecture reviews are combined with a site visit and a system walkthrough. The assessment will include all the important aspects of the functional requirements as specified in IEC 62443.

The first phase of this assessment is similar to the design review, where all existing documentation is analyzed and discussed with the facility owner, technical representatives and/or the vendor. However, additional depth is required to review all the main IEC 62443 functional requirements.

During the site visit the actual system status is compared to the current understanding of the OT network. Moreover, the configuration of specific devices is reviewed to gain more insight into potential security issues. For example, the firewall configuration, network routing and VLANS, installed software and running services are reviewed to investigate the exposure of the OT network. Also, user authentication and authorization, security controls, backup strategy and security monitoring are assessed to determine the OT cyber resilience.

Finally, various samples of network traffic are passively collected on strategic point on the OT network. These captures make use a copy of already existing network traffic and will not interfere with, possibly fragile, OT equipment. The traffic is then analyzed and the findings are correlated with all the previous information. Optionally, it is also possible to perform specifically tailored selective scans to retrieve additional information in the least intrusive way. The results could lead to the discovery of unknown hosts, open ports, weak protocols, unexpected network connectivity or other unknown security issues. For example, the first use case presented earlier was discovered during a site assessment.



VULNERABILITY AND PENETRATION TESTING

A vulnerability assessment and penetration test, commonly abbreviated as VAPT[4], is going one step further and is a more detailed and technical assessment. The goal is to search for unknown vulnerabilities and to test if these can be exploited. This will also illustrate what the consequences of a certain cybersecurity issue could be, and what that would mean to the organization.

These VAPT tests provides detailed insight into the current cyber resilience and what kind of improvements might be required. However, these assessments are more intrusive, and it is well known that older, legacy OT systems cannot handle this. A critical system could even stop operating while being scanned for vulnerabilities. Therefore, it generally not recommended to execute these tests in a live OT environment.

At the same time some techniques do exist, like passive scanning, that can still be used safely. Alternative, by carefully selecting the rights scope or make use of spare devices intrusive penetration test can still be performed without any impact on the production process. Of course, this requires a very specific approach, tailored to OT systems and the systems in scope. Another good opportunity is to make VAPT test part of the installation, test, and commissioning processes, like the factory acceptance test (FAT) and site acceptance test (SAT). This could be applicable for new systems or system expansions.

The results of the assessment can be used to take steps to close security gaps and reduce the risk in your organization. In relation to the first use case, a penetration test could investigate if the assumed attack path is actually feasible for an attacker. The results might determine the final security mitigation solution.

Conclusion and the Way Forward

It is expected that the Industry 4.0 and IIoT trend will continue the next years for all sectors, including the Chemical sector. This will be primarily driven by the business and operational benefits. This is a fine so long as cyber-security is not an afterthought. It's important to include security design and operational costs directly into the business case of these smart initiatives and verify their impact on OT cybersecurity posture. Internal and external security design review could assist in this stage. For existing solutions and systems there are multiple approaches to review and verify the current security state, providing the opportunity to pro-actively solve potential issues before they create any business impact. The end goal remains to achieve safe, reliable, and cost-effective production and to manage cyber risk to an acceptable level to support those goals.

References

1. https://shodan.io
2. https://www.secura.com/services/operational-technology/threat-modeling
3. https://www.secura.com/services/operational-technology/site-assessment
4. https://www.secura.com/services/information-technology/vapt

About Secura

Secura has worked in information security and privacy for over two decades. This is why we uniquely understand the challenges that you face like no one else and would be delighted to help you address your information security matters efficiently and thoroughly. We work in the areas of people, processes and technology. For our customers we offer a range of security testing services varying in depth and scope.

Secura has the mission to support organizations with up-to-date knowledge to work towards a bright and safe future.

Keep updated with the latest insights on digital security and subscribe to our periodical newsletter.

Follow us on:

Contact us today at info@secura.com or visit secura.com for more information.

SUBSCRIBE

TO OUR NEWSLETTER

Secura

A BUREAU VERITAS COMPANY

BUREAU VERITAS 1828

BUREAU
VERITAS

Shaping a World of Trust