Secura
A BUREAU VERITAS COMPANY

Cyber Resilience Testing for Industrial Control Systems (FAT/SAT)

As the operator or owner of Industrial Control Systems (ICSs), you are responsible for verifying the cybersecurity requirements of these systems. For a new ICS this verification should be part of the Factory Acceptance Test (FAT) and Site Acceptance Test (SAT). Secura can help you with independent verification.

Secura has worked in information security and privacy for more than 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. We offer a range of security testing services varying in depth and scope.

Your challenges

Ransomware, malware: our security experts see all kinds of security threats emerging in OT, spread by malicious actors taking advantage of weak OT security posture. Not implementing security measures from the start can be costly or even dangerous.

How we can help you

Our service "ICS Cyber FAT/SAT" raises the cyber resilience for your industrial control systems. This fact sheet explains this service in depth. We perform an independent review to verify that your new ICS meets cybersecurity requirements, and you have security best-practices in place.

How our cybersecurity services fit in the project life cycle

The life cycle of a new ICS starts with a project specification created by the owner or operator. Naturally, this specification describes the main functions of the new installation, but usually also contains some cyber security requirements. These can either be based on compliance with company security policies, industrial standards (IEC 62443) or applicable laws and regulations.

Next is the design & engineering phase. Here, cybersecurity again plays a vital role. To ensure security requirements are embedded in the project, and are not an afterthought, you can perform risk assessments, threat modeling and design reviews.

After this stage, the system is ready to be implemented. This is where the FAT and SAT come into play. Secura's ICS Cyber FAT/SAT focuses specifically on the verification steps common during the regular FAT/SAT phase of each project.

Later in the life cycle, during the operation & maintenance phase, cybersecurity becomes an ongoing activity. This ensures continuous attention to security processes and the security posture of the OT assets. It also makes sure all digital risks remain acceptable. OT Risk assessments, OT site assessments and OT Security Maturity assessments are important tools to determine these risks.

Secura provides all services mentioned above, specifically tailored to the OT environment and ICS systems, covering the entire project life cycle.

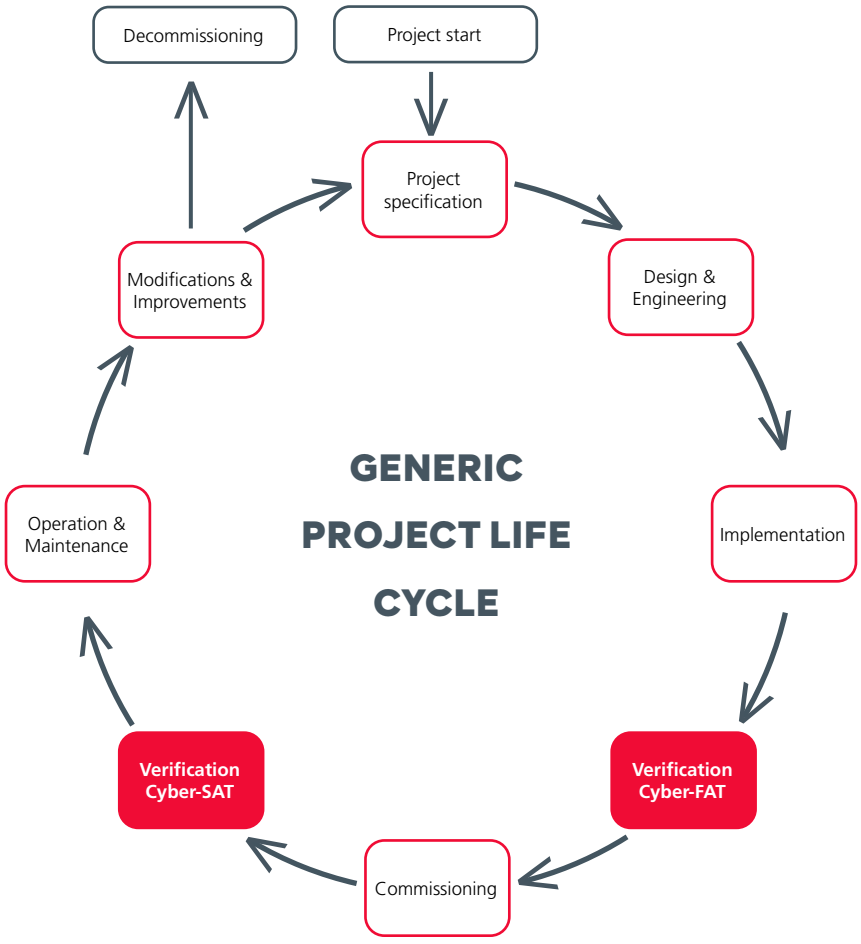


Figure 1.Generic project life cycle

Why choose Cyber FAT/SAT?

Between the design & engineering phase and the operation & maintenance phase, there are other important phases, like implementation and commissioning. Especially between these phases, a factory- and site acceptance test is performed to verify that all design requirements are met.

A FAT occurs at the vendor's premises before the completed systems are shipped to site. A FAT involves extensive testing of all components to verify compliance with the design and project specifications, and to check if the system meets all functionality and performance requirements. The tests are facilitated by the vendor or system integrator and executed by the asset owner.

A site acceptance test (SAT) is similar, but takes place at the customers site and only after the complete commissioning/installation of the system. It ensures the system is installed in a proper, reliable, and safe operating state.

While cyber security requirements are often part of the design specifications, they are regularly neglected during a conventional FAT or SAT. For the owner or operator, it is often too difficult to verify the complex nature of all these cybersecurity controls. And the vendor, integrator or EPC contractor can't be expected to independently check their own design. Secura's Cyber FAT/SAT bridges this gap: we deliver support as an independent security provider.

The Cyber FAT/SAT (CFAT/CSAT) is an extension of the conventional FAT/SAT with a focus on cyber security. It can be planned in parallel or after the regular FAT/SAT. The goals are similar, but focus on digital security.

This is what we do:

- Make sure the systems are installed and configured according to the design specifications and contractual agreements;
- Verify the correct configuration and hardening of the OT assets;
- Rigorously test if the cyber security controls work effectively;
- Detect and remediate security issues before the system is shipped to site or commissioned.

Secura can perform these validation checks using two approaches or a combination of both. Namely: by performing a design & security review and/or penetration testing (VA/PT). Both options will be detailed in the sections below.

How a design & security review works

With a design and security review, Secura can verify that the implemented design and configuration are in accordance with the project specifications. And if required, we also review against industry standards like IEC 62443.

The network architecture and its security configuration are reviewed against the Purdue model reference architecture, but also against industry best practices like micro-segmentation and a zero-trust design. Secura also reviews the network and firewall configuration, to ensure that these segmentation boundaries are effective.

For individual ICS assets, such as engineering workstations (EWS), human machine interfaces (HMI), network components and industrial controllers (e.g. DCS, PLCs, RTUs), we review the security posture and verify that they are configured according to the specifications, best practices and industry standards. These checks include, but are not limited to: system hardening, security patches, anti-virus, backups, and authentication & authorization controls.

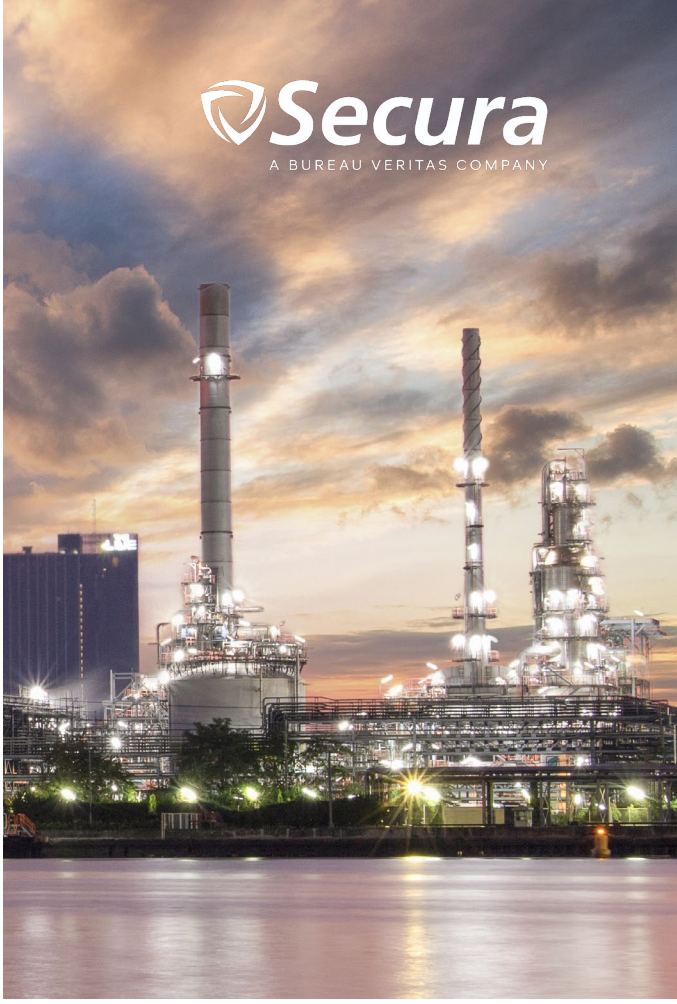
The FAT would be the most ideal time to perform the design & security reviews. This would allow more time to fix any potential security issues before the equipment is shipped to site. If the review can be done during the FAT, the SAT scope could be limited. In that case, you would only have to retest previous findings and test equipment and interfaces that were not part of the FAT setup.

How vulnerability assessments and penetration testing (VA/PT) help build resilience

A Vulnerability Assessment and Penetration Test (VA/PT) for OT systems requires a specialized approach. With a vulnerability assessment, the aim is to find as many vulnerabilities as possible by scanning and manually reviewing systems, network devices and application configurations. In contrast, a penetration test is performed from an attacker's perspective. Its aim is to exploit these vulnerabilities to illustrate what the consequences of these security issues would mean to the digital resilience of the environment. The outcome of both assessments can be used to solve potential security issues before the system is put in production.

A major benefit of performing these tests as part of the FAT and/or SAT is the ability to do more rigorous testing. It is commonly known that many ICS systems are less resilient against vulnerability scans, and therefore it is more difficult to perform these kinds of tests when the system is in production. So, these FAT and SAT phases are the ideal time to perform an in-depth VA/PT assessment. It is also the perfect opportunity to verify if the defensive and monitoring controls were effectively implemented.

You can find more information about our Industrial VA/PT service on our website: **www.secura.com/markets/industrial**



Scoping VA/PT during the FAT/SAT

It depends on the existing FAT and SAT plans how to scope this assessment. Usually, it is impossible to setup and test the entire OT system during a FAT. Field instruments, heavy machinery, third-party packages, existing systems, and connections to the corporate network are usually not part of the FAT. The same applies to potential IoT connections, vendor cloud applications, secure remote access, or other forms of connectivity between systems connected to the IT network or internet. Therefore, the focus during the FAT is often on vulnerability scans and penetration tests of the applicable assets residing in Purdue level 1, 2 and 3. During the SAT, this can be extended to all external interfaces and include assets in level 0, the IT/OT DMZ, and the business IT network. Finally, any issue that cannot immediately be solved as part of the FAT can be retested during the SAT.

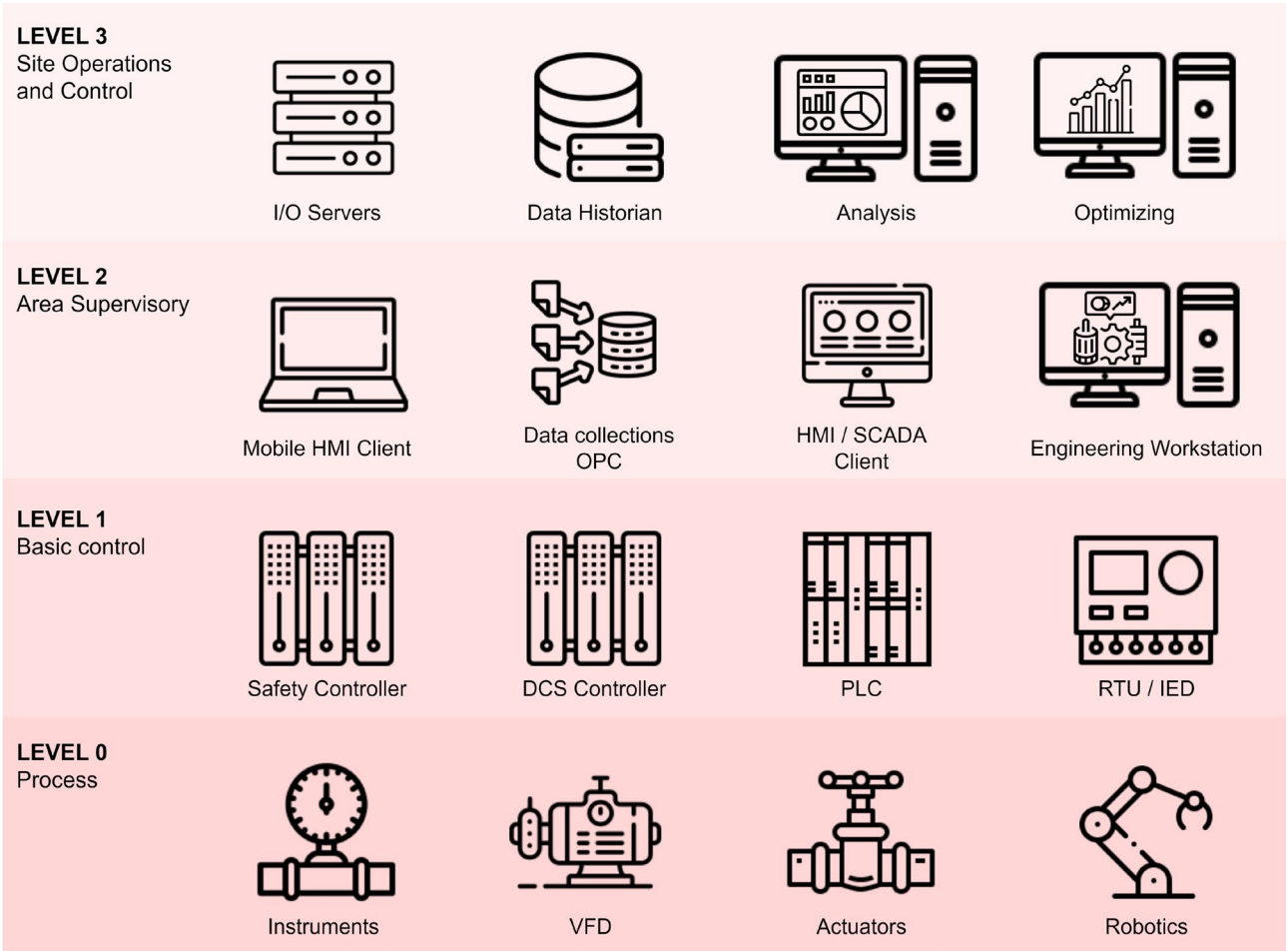


Figure 2. Focus during FAT is generally on Purdue level 1, 2 and 3. During the SAT, this can be extended to level 0

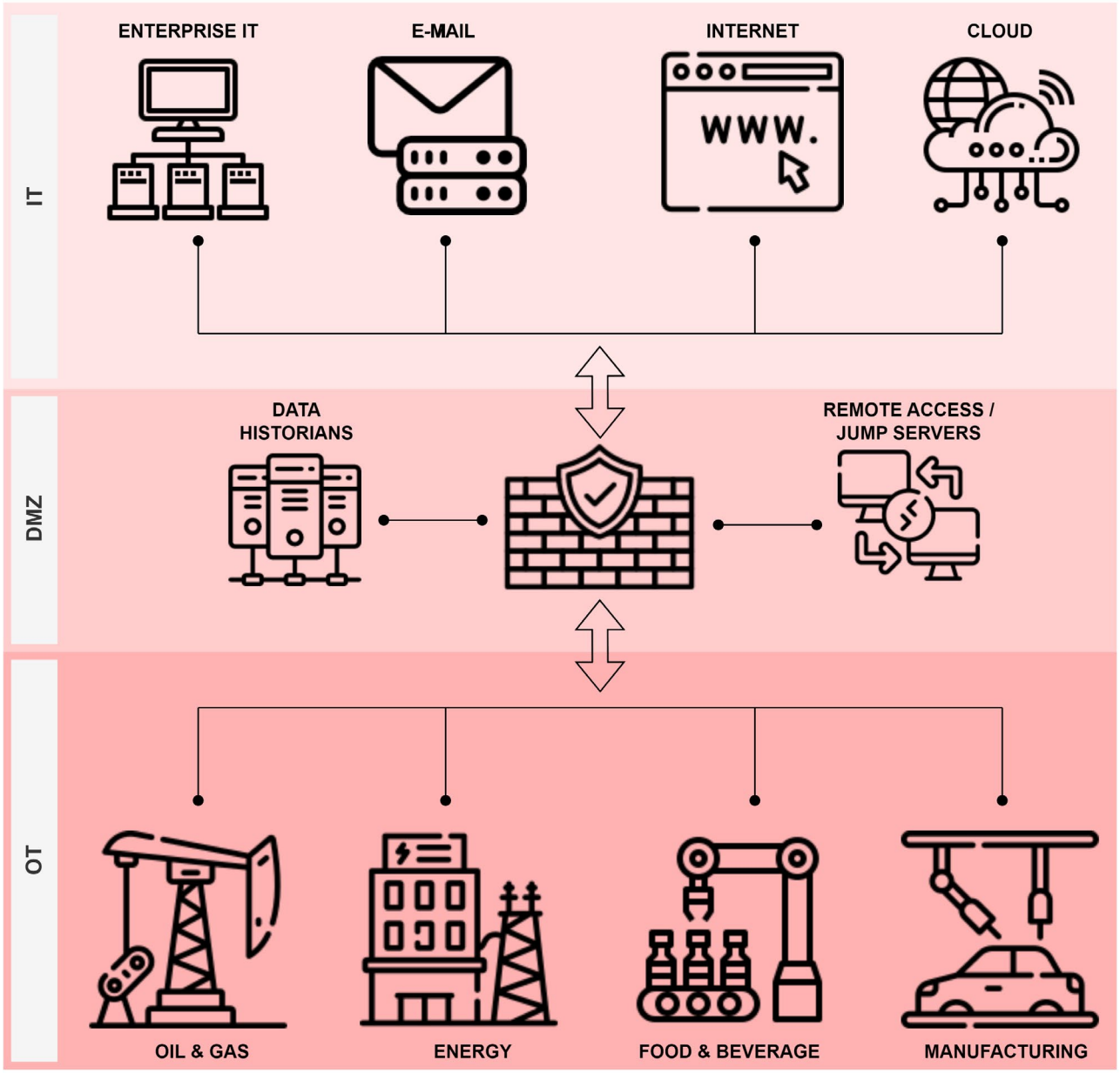


Figure 3. Testing of external interfaces during SAT, like IT/OT DMZ and Internet Connectivity

Outcome of the Cyber FAT/SAT

Secura will match the existing FAT/SAT process if possible. We add our findings to the punch list. Based on priority, these issues could be solved by the vendor and retested during the FAT/SAT, while Secura could support by providing recommendations.