Bridging the gap between Functional Safety and Cybersecurity.

Now, more than ever, Industry requires a new way of thinking and acting that recognizes the potential threats and effectively counters them. Cybersecurity is already an integral part of modern engineering and an indispensable part of industrial plant safety. In today's world of OT there can be no safety without security.

In the following, we have compiled and answered our most frequently asked questions.

HOW DO CYBERSECURITY THREATS AFFECT FUNCTIONAL SAFETY?

With technological progress, more and more industrial plants are adopting IP based solutions. This can increase their vulnerability to cyber events or incidents. We already have seen targeted attacks on Safety Instrumented Systems (SIS), such as with the TRITON attack, and we are likely to see more in the future. Thankfully in the TRITON case the attackers were not successful and the safety system responded appropriately. Safety standards such as IEC 61508 now require that cybersecurity risks are addressed as part of the overall safety assessment.

www.tuv.com/fscs

TÜVRheinland®
Precisely Right.

HOW CAN A BALANCE BETWEEN FUNCTIONAL SAFETY AND CYBERSECURITY BE ACHIEVED IN A COMPANY?

The results of our study about industrial security and the Cybersecurity Trends 2020 show that functional safety and cybersecurity are inseparably linked. In order to meet safety and cybersecurity requirements a risk based approach should be taken to ensure that limited budgets can be spent on the most important safety and cybersecurity areas. This requires OT managers to have a detailed understanding of business risks, safety risks and cybersecurity risks in order to prioritize budgets accordingly.

HOW MUCH SHOULD BE INVESTED IN CYBERSECURITY MEASURES?

This depends on the business risk, an assessment should be undertaken using an objective framework such as the NIST Cybersecurity Framework or IEC 62443. This will provide a very good overview of business risk issues and missing or inadequate cybersecurity controls. Any investment in cybersecurity measures need to be proportional to the risk. A program should be created that addresses the key issues first and then the remaining issues. It is unlikely this can be done in a single leap, and in the experience of TUV Rheinland an effective program can take 2 – 3 years, depending on the individual business and how mature the existing cybersecurity levels are. Risk assessments should be undertaken regularly to reflect the ever changing nature of cybersecurity threats.

WHAT ARE THE BIGGEST CHALLENGES IN THE FIELD OF INDUSTRIAL CYBERSECURITY?

For many organizations the biggest challenge, and one that has been underestimated by many until now, are the necessary organizational and cultural changes in the company that need to be addressed. New IP-enabled technologies can massively improve plant efficiencies but will often have associated risks that may not have been considered. In addition, due to the lack of skilled workers, it is difficult for companies to find trained personnel who understand industrial processes, operational technology and cybersecurity.

IS IT BETTER TO TRAIN IT STAFF OR EXPERTS FOR INDUSTRIAL PROCESSES AS OT-CYBERSECURITY SPECIALISTS?

It is possible to cross train IT staff to become OT cybersecurity experts over time if they have an appreciation of industrial processes, engineering and a passion for the subject. In practice the best OT cybersecurity team will consist of IT staff, OT process engineers, asset owners and OT cybersecurity experts. This approach enables the sharing and exchange of knowledge and experience which will make for a very good team. TÜV Rheinland Academie can offer coaching and further training for team members to help build up this capability.

WHAT IS THE BEST WAY TO COMBINE THE EXPERTISE OF A CHIEF INFORMATION SECURITY OFFICER / CHIEF SECURITY OFFICER FOR IT AND OT IN THE COMPANY TO MINIMIZE CURRENT RISKS AND ATTACKS?

It takes years of experience to achieve the necessary expertise in cybersecurity, IT and OT. Whilst experience and knowledge is being built up the use of third parties such as TUV Rheinland should be considered. TÜV Rheinland can contribute to the long-term training of employees in cybersecurity and associated technologies and challenges.

SHOULD THERE BE A SEPARATE OT-SPECIFIC CHIEF SECURITY OFFICER (CSO) IN A COMPANY?

This depends on the business in question. Many organizations are moving to a converged approach where IT and OT cybersecurity teams work closely together with a single CSO being responsible. The problem is that such CSO expertise is difficult to find so having separate functions may be a better medium term arrangement.

WHAT ARE THE KEY FACTORS IN PROTECTING OT ENVIRONMENTS AGAINST RANSOMWARE?

Ransomware is malicious software that will encrypt computer systems. Often delivered via a phishing email the threat actor will demand payment to decrypt this data. Often, even if money is paid, the decryption process may fail. As IT and OT systems are often linked there can be a direct impact on a production facility following a ransomware incident resulting in loss of production and system downtime.

Patching, good backups and a segmented network are good measures to help prevent ransomware, as well as good user education, email filtering and management. OT assets must be documented and fully understood as well as how they connect to IT systems. Use of properly configured firewalls can be helpful. Ultimately the answer to a successful ransomware incident is to restore systems from backup. This must include OT systems and the backup must be secured from inadver-

tently being encrypted by the same ransomware. Finally a good, well-rehearsed incident response and recovery plan will ensure that should you be a victim of ransomware you have the people, process and technologies in place to deal with it.

HOW CAN THE RISK WITH EXTERNAL SERVICE PROVIDERS / THIRD PARTIES BE MINIMIZED?

With third parties it is important to define liability and ensure this is supported by the appropriate contracts. Cybersecurity must be considered from the beginning of a supplier relationship, and certainly before the contract is signed. After this regular audits by third parties are of utmost importance in order to check that the cybersecurity measures are being maintained during the whole contract period.

The TISAX audit program in the automotive industry shows how such cybersecurity assurance programs work. It is an evaluation and exchange mechanism for information security and enables the mutual acceptance of cybersecurity evaluation results between participants. If you process sensitive information from your customers or want to evaluate the information security of your own suppliers, TISAX is a very good example of how this can be achieved.

HOW ARE BUSINESS RISK CONCERNS AND OT-CYBERSECURITY RISKS RELATED?

OT systems should be integrated into the business's **G**overnance, **R**isk and **C**ompliance (GRC) strategy so that cybersecurity measures are considered along with other key business risks. We have created a new solution call CARM (Continuous Adaptive Risk Monitoring) that provides a GRC overlay for OT operations. Please contact us for further information.

HOW IMPORTANT AN ISSUE IS OT DATA LOSS DURING AN EVENT OR INCIDENT? WHAT ARE THE CONSEQUENCES OF A LOSS OF PRODUCTION?

Protecting production system's availability is normally the major concern for OT cybersecurity experts working in this field, along with protecting people and the environment. The financial consequences of a production outage are usually immense and can damage a company in the long term. The loss of OT data should not be ignored. For example OT process information, function block diagrams or company secrets can be lost or stolen resulting in reputational damage or the loss of major contracts. Both of these are important issues and cybersecurity controls and processes need to be put in place to deal with an inevitable event or incident.

AT WHAT POINT DOES THE TRANSITION FROM IT TO OT TAKE PLACE WITHIN A COMPLEX INDUSTRIAL ENVIRONMENT?

The transition point between IT and OT depends on the structure of the business or OT system in question. The Purdue reference model provides a good way of explaining this. Often the IT/OT transition takes place from level 3 or 4 of the model. Level 4 systems usually deal with day-to-day business operations and are decoupled from the process levels. Level 3 contains the Operations Management, which is separated from Level 2, the supervisory control. As time goes on and the world of OT develops the use of the original Purdue model may be challenged, but for now it provides a useful „ideal" logical structure.

DO YOU HAVE MORE QUESTIONS? CONTACT ONE OF OUR EXPERTS FOR FUNCTIONAL SAFETY AND CYBERSECURITY.

ONLINE CONTACT

TÜV Rheinland i-sec GmbH
Am Grauen Stein
51105 Cologne, Germany
cybersecurity@tuv.com

www.tuv.com/fscs

TÜVRheinland®
Precisely Right.

® TÜV, TUEV and TUV are registered trademarks. Their use must be approved beforehand.
DE20_I07_2000498_en