Enable innovations by enhancing safety and cybersecurity in OT

The success of BATZ in Industry 4.0 depends heavily on a high level of safety and cybersecurity in Operational Technology (OT). By working with experts from TÜV Rheinland, this international automotive tier one manufacturer was able to quickly identify key risks and enhance its cybersecurity program.

SUPPLYING PARTS TO MAJOR OEMS WORLDWIDE

The BATZ Group is part of the Mondragon Corporation and has 16 facilities around the world with a turnover of €230M. Mondragon Corporation is a corporation of worker cooperatives headquartered in Spain. The corporation employs nearly 75,000 people globally across four domains – finance, industry, retail and knowledge.

The BATZ plant in Igorre, Spain, is an automotive tier one manufacturer, that supplies parts to many major OEMs worldwide. Products include pedal assemblies, vehicle jacks, gear shifters and handbrakes.

NEW EQUIPMENT CONNECTED TO THE INTERNET

BATZ operates in a competitive market and needs to innovate and make best use of cost-saving production methods. As the plant receives additional investment new equipment will be purchased that increasingly needs to be connected to the internet. The company understands the need to provide a secure environment in which to safely develop new and innovative products. The concept of Industry 4.0 and its associated innovations is important to BATZ as they wish to make best use of new technologies.

THE TASK WAS DEMANDING:

BATZ was concerned about cybersecurity risks impacting their ability to win and retain customers. The manufacturing technology platform had been designed and maintained by a third party.

BATZ engaged TÜV Rheinland to perform an OT and IT cybersecurity risk assessment at their plant near Bilbao, Spain. TÜV Rheinland worked onsite at the plant with the team followed by several weeks of analysis offsite to compile a comprehensive report.

www.tuv.com/informationsecurity

BATZ

TÜVRheinland®
Precisely Right.

During the time onsite the experts conducted an intensive workshop with employees from the BATZ team. This included IT and OT security teams, plant engineering, academic researchers and support staff.

IDENTIFYING RISKS, PRIORITIZED REMEDATION

The assessment by TÜV Rheinland was based on the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (NIST Cybersecurity Framework). This assessment provided a common taxonomy and mechanism for BATZ to do the following:

- Describe their current cybersecurity posture
- Describe their target state for cybersecurity
- Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process
- Assess progress toward the target state
- Communicate among internal and external stakeholders about cybersecurity risk

ACTION PLAN FOR MITIGATION UNACCEPTABLE RISKS

By working with TUV Rheinland, BATZ were able to quickly identify key risks. These were categorized, triaged and sorted to ensure that the top risks could be addressed first. TÜV Rheinland developed a plan to address these risks over a timeframe of 12 to 18 months. This will help mitigate risks and enhancing BATZ's cybersecurity program in general.

PROPORTIONATE, MEASURED APPROACH

The team at BATZ should be commended for taking a proactive approach to managing their industrial cybersecurity risk. TUV Rheinland took a proportionate, measured approach to this engagement, enabling BATZ to quickly identify a way forward.

THE RESULTS

- The company can use its budgets in a more focused way to reduce their key risks.
- The organisation can transition to a converged security model so that logical and physical risks can be the responsibility of one team.
- Key customers can be assured that the systems used in the facility have been risk assessed and appropriate controls will be implemented.

The project was a great example of delivering real value for the customer in a cost-effective and efficient way.

Any questions? We are happy to assist you with all questions regarding safety and cybersecurity in Operational Technology. In the area of information security and cybersecurity, we have been advising and implementing cybersecurity in all sizes of companies for 20 years.
When will we talk about your challenges?

TÜV Rheinland Group
Digital Transformation & Cybersecurity
otsecurity@tuv.com

www.tuv.com/en/ot

BATZ

TÜVRheinland®
Precisely Right.