

“Zones and Conduits” in automation networks: Security protects Safety

Safety is the top priority

Ostfildern, July 2026 – **The Machinery Regulation makes it mandatory: Industrial Security is designed to protect safety-related functions from manipulation – in other words, Security is a prerequisite for functioning Safety. But how do you provide holistic protection for an automation network? Standards such as IEC 62443-3-2 and the forthcoming EN 50742 set out a clear direction: separating systems into zones, monitoring connections – a principle that runs through the current recommendations from industry bodies and experts. Pilz is convinced: the strict separation of Safety and so-called standard automation is the key to effective Machinery Safety – underpinned by the defence-in-depth principle and implemented through the zones and conduits approach.**

A house can be built to be sturdy and safe: with solid walls, fire-resistant materials, reliable electrics and working alarms. This structural safety is a prime example of Machinery Safety, where design measures, sensor technology and protective mechanisms are intended to prevent unintended hazards. However, such a house only remains safe if it's not subjected to deliberate interference.

Manipulated heating controls, sabotaged electrical circuits or deactivated alarm systems can transform a building designed with safety in mind into a risk. In the world of machinery, the best safety-related design becomes ineffective if safety-related components are tampered with or disabled without authorisation.

In this context, Security plays the external protection role: sturdy doors, secure access points, monitored connections and barriers against unauthorised interventions. So Security does not protect against accidents themselves, but instead stops protective mechanisms from being disabled – by individuals who gain access via an unauthorised operating mode selection or action, for example. This is the only way Safety remains reliably effective – Security for Safety.

From regulatory requirement to proposed solution

For the very first time, the Machinery Regulation (EU) 2023/1230 makes Security a mandatory requirement for functioning Safety on plant and machinery: safety functions must not be compromised due to manipulation, whether intentional or otherwise. This is precisely where the emerging standard EN 50742 comes in; it will help to clarify the essential Security requirements of the Machinery Regulation. The standard defines technical details for protection against corruption and sets out clear requirements for hardware, software and data that may affect safety-related functions. The standard covers the entire lifecycle – from development through to operation and decommissioning. The existing IEC 62443 series of standards, which sets out a systematic approach to cybersecurity for industrial automation and control systems, also plays a key role. It provides a structured framework for risk analysis, “defence-in-depth” and the principle of segmentation (“zones and conduits”), and is explicitly recognised in EN 50742 as an alternative or complementary approach to safeguarding Security. Together, these standards form the normative core of Security for Safety: they require the digital integrity of a machine to be recognised as a prerequisite for its functional safety and protected accordingly.

Why “Zones and Conduits” make machinery safer

Returning to the image of the house: the boiler room represents a zone, while the connection to the smart home gateway represents the associated conduit. If this connection is manipulated, the entire system can be affected – even if the room is perfectly secure.

Therefore, it is not only crucial to safeguard the individual zones, but also the security of the routes that connect them. This is precisely where the “Zones and Conduits” principle comes into play. Zones are clearly separated from one another, and the transitions between them are designed to be monitored. Just as in a house, where doors and assigned keys determine who can go where, internal protection (Safety) and external protection from manipulation (Security) are structurally intertwined inside an industrial plant.

The result is a protection concept based on the defence-in-depth principle: Safety is not achieved through a single barrier, but through multiple layers of protection arranged one after the other. If one layer is overcome, the next one stands firm. Zones form these tiered spaces, while conduits are the monitored passageways between them. This way, a single vulnerability cannot compromise the entire system – particularly when it's a matter of Safety and therefore protecting people.

Pilz consistently pursues this approach as “Security for Safety”, Safety being the primary protection goal of Security. The focus is on protecting Safety, which in turn protects people. That's why Pilz separates Safety from the general machine control, i.e. the standard automation, and thereby reduces the exposure of safety-related functions. The more clearly these “assets” are separated functionally,

the fewer additional safety measures are needed to provide reliable protection.

The benefits of this approach are evident throughout the entire lifecycle of a machine. If safety functions and standard functions are separate, there is no need to recertify or adapt the safety functions in parallel if the standard functions are updated. This reduces maintenance and servicing work significantly. Classic safety controllers also require considerably fewer safety-critical updates than standard controllers, so this separation eliminates the need for many unnecessary interventions. Separation also offers technological advantages: a standalone safety system such as the safe small controller PNOZmulti 2 can be freely combined with control systems from different manufacturers, whereas integrated systems are often tied to specific technologies. At the same time, separate safety solutions raise the bar for attackers, because separate systems must be compromised individually, which makes manipulation much more difficult. What's more, a standard system can be online when required, while the actual safety functions remain isolated, thereby drastically reducing the attack surface.

This separation of Safety and Security automation – each with perfectly coordinated security levels – also increases efficiency by making it easier to plan safety, maintenance and expansion measures. So changes to the standard program do not require any intervention in the safety-related section, significantly reducing the amount of programming and adaptation work required.

Simultaneously, this separation has a positive impact on software and support costs, as separate systems often incur lower licence and service fees.

Protection through separation – competence through training

The clear separation of safety and standard automation not only ensures technical robustness, but also reduces operator errors and lowers training requirements. As safety-related functions run on dedicated hardware and are clearly separated in organisational terms, they remain protected even if changes are made to the standard program. As a result, errors in day-to-day operations do not compromise Safety, and responsibilities can be assigned more clearly.

Pilz offers a comprehensive training and service programme to help companies implement this architecture. These include the training courses “Fundamentals of Industrial Security” and “CESA – Certified Expert for Security in Automation”, as well as Industrial Security Services. These explain how to develop robust Security for Safety concepts from the individual blocks, but also go much further: they demonstrate how to manage security risks systematically and develop holistic safety concepts, how to incorporate the requirements of IEC 62443, how to structure the architecture of a safe machine network and how to assess and continuously improve the effectiveness of the measures that are taken.

One key advantage of this approach: operators at the end user's do not need to be deeply immersed in issues of security because the protection of the safety functions is already guaranteed by the architectural design. For this reason the training courses are primarily aimed at those who make security decisions or design systems – whilst operators can continue to work safely without the need for additional training in Industrial Security. The result is a practical division of roles, which simplifies plant operation while at the same time sustainably increasing the level of protection.

Increased safety through a clear structure – and the right expertise

An effective “Security for Safety” strategy is not achieved through individual measures, but through a well-thought-out architecture, clear lines of responsibility and targeted skills development. This is exactly where Pilz comes in. With its strict focus on defence-in-depth and a clear separation between safety and standard automation, Pilz lays the foundations for resilient machinery – supplemented by practical training and consultancy to ensure that companies can follow this path with confidence. The result is a level of safety that not only meets the requirements of the standards but also delivers tangible added value in day-to-day operations: simpler, more robust and effective long-term.

(Characters: 9,640)

Pilz – The Spirit of Safety

Pilz is a global supplier of products, systems and services for automation technology. As a pioneer of safe automation, Pilz creates safety for human, machine and environment. Founded in 1948, today the family business with its head office in Ostfildern is represented worldwide with 2500 employees in 42 subsidiaries and branches.

The technology leader offers complete automation solutions for Safety and Industrial Security on the machine. These include sensor, control and drive technology – as well as systems for industrial communication, diagnostics and visualisation. An international range of services with consulting, engineering and training completes the portfolio. Pilz solutions are used in many industries beyond mechanical engineering, such as intralogistics, packaging, railway technology, or the robotics sector for example.

www.pilz.com

Pilz on social networks:

On our social media channels we provide background information about the company as well as the people at Pilz and report on the latest news from automation technology.



www.pilz.com/facebook



www.pilz.com/xing



www.pilz.com/youtube



www.pilz.com/linkedin

Press contact:

Martin Kurth

Corporate and Technical
Press
Tel.: +49 711 3409-158
m.kurth@pilz.de

Sabine Karrer

Technical and Corporate
Press
Tel.: +49 711 3409-7009
s.skaletz-karrer@pilz.de

Jenny Skarman

Technical Press
Tel.: +49 711 3409-1067
j.skarman@pilz.de

Eva Gellner-Röbke

Technical Press
Tel.: +49 711 3409-7147
e.roessle@pilz.de