BLOG/BILLINGHAM, UNITED KINGDOM | APRIL 2021

# Does my SIS really need to be Cyber Secure?

Blog by Rafal Selega

Rafal Selega, Senior Functional Safety Consultant, ABB

In the good old days, most Industrial Automation and Control System (IACS) networks were air-gapped and separated from business networks and the Internet. This meant that they 'operated independently' from non-process plant operational systems.

Today, the significant benefits offered by greater business insight and remote network access, combined with the adoption of hardware and software from traditional IT (e.g. TCP/ IP networking, Windows-based) and even cloud-based platforms to meet client requirements, have led many process industry companies to integrate their control systems and enterprise IT systems. With this 'intelligent approach', however, key aspects of Industry 4.0 are opening process safety systems to new risks.

**Opening the door to hackers**

Imagine what could happen if any operating company had vulnerabilities in its plants that exposed its risk-reduction measures, such as the safety instrumented systems (SIS), to malicious hackers. Potential destruction of the plant and/or worker injuries or fatalities could be a real possibility. Even if the IACS is non-programmable, or is physically separated from other networks, threats to security must still be taken seriously. Maintenance activities, software upgrades or unauthorised access all have the potential to enable attacks. Worryingly, statistics indicate 60% of attackers in such cases are insiders, often disgruntled or dismissed employees.

**Awareness of safety risks is obligatory**

SIS engineers and operators must be aware of the safety challenges that come with new IACS technology. The International Electrotechnical Commission (IEC), Instrumentation, Systems and Automation Society (ISA) and Health and Safety Executive (HSE) organisations have all acknowledged the importance of cyber security and have provided the required standards and guidelines.

The functional safety standards IEC 61508 / IEC 61511 have requirements to address cyber security in Safety Instrumented Systems (SIS). So from a functional safety (FS) point of view, having cyber secure SIS is now a must, not an option. This is because in today's world, neither FS nor information technology are independent of one another.

**How to make your SIS cyber secure**

The most effective and efficient means to achieve cyber security is to adopt a lifecycle approach which is fully integrated with process safety work processes. There is no turning back on Industry 4.0 as it becomes increasingly adopted and encompassing. We cannot air gap the SIS or ban the use of smart devices which all simplify and benefit our processes; however, we must be aware of the highly critical nature of IACS cyber security and how seriously it should be taken.

**So what must be done?**
It therefore follows that process industries should immediately be implementing an 'integrated' control and cyber security lifecycle management approach to ensure consistency, repeatability, robustness and systematic capability across the conceptual, design, engineering, installation, operation and maintenance of control and safety systems.

Clearly, organisations in all process industries need to ensure that the cyber security of their safety system is given the exact same level of rigour and detail as the FS requirements detailed in the IEC safety standards. Because, quite simply, the SIL of any safety function is today determined by how cyber secure the SIS really is.

For further information please email me at rafal.selega@pl.abb.com or see Functional safety lifecycle services