DEKRA

WHITE PAPER

Keeping Safety Integrity Systems Resistant to Cyber Attacks

Author: Clive de Salis, Principal Process Safety Specialist, and Dr. Arturo Trujillo, Global Director Process Safety Consulting

Technological advances that have given rise to functional safety, Safety Integrated Systems (SIS) and the Safety Integrity Level (SIL) mechanism have generally made high hazard industries less dangerous. However, technology can also be weaponized as the world has witnessed with the increasing frequency of cyber attacks. Since many organizations rely on SIS to maintain safe operations, it is reasonable to ask how vulnerable such systems are to hackers and the efforts of cyber criminals.

SIS Standards Offer Guidance on Cybersecurity, but Don't Guarantee Immunity to Attack

The Safety Instrumented System standards, the IEC61508 group that includes IEC61511 for the process industry, are the product of the same committee that writes the IEC62443, the cybersecurity group of standards for assessing systems and for protecting against cyber attack. These standards are now the European norms, EN 62443, as well. The standards require organizations to address cybersecurity threats to SIS and incorporate security measures into the defined SIS lifecycle for both new and existing SIS. The IEC62443 series of standards also details how to assess for and protect against cyber attacks.

The crucial point here is that the whole of the standards on Safety Instrumented Systems (both IEC61511 and the master standard IEC61508) are written on the assumption that the SIS is SEPARATE from the Basic Process Control System (BPCS). A BPCS is typically a distributed control system in a network of controllers. The SIS should never be combined with the BPCS unless there are very compelling reasons for doing so. Convenience, commonality of programming and maintenance, standardization and similar justifications are NOT compelling reasons. Nonetheless, manufacturers persist in including SIS controllers integrated into BPCS networks, marketing this feature as an advantage. A typical SIS controller may be a different color from the standard BPCS controller, but if the two are on the same network and data highway, the SIS is at increased risk of cyber attack, no matter how robust its protective barriers are purported to be. After all, cyber attackers are single-minded in their efforts to break through barriers, so as long as a controller is on the network it is remotely accessible to hackers.

What Does This Mean for SIL-Rated SIS?

To say that a Safety Instrumented System has a Safety Integrity Level rating sounds impressive, since the SIL-rated system is introduced to reduce risk. The SIL number comes into play when the gap between the probability of an unwanted event occurring and the corporate tolerability target is greater than a factor of 10.

An ordinary safety measure provides a risk reduction of between 1 and 10

> SIL 1 provides a risk reduction of more than 10 ^{1}
> SIL 2 provides a risk reduction of more than 10 ^{2}
> SIL 3 provides a risk reduction of more than 10 ^{3}

... and so on.

Yes, risk reduction is a good thing. But considered carefully, to have a SIL-rated system is not a success but an admission of failure: it means that without that one high integrity Safety Instrumented System organizations already fall short of what is an acceptable risk. For example, a SIL 2 system indicates that a process or facility is at least 100 times on the wrong side of tolerable if that system fails (and SIL 3 is even worse, as one can imagine). A SIL rating amounts to an admission that the other **Layers of Protection** (LOP) meant to ensure safety are insufficient. When thoroughly understood, therefore, the question of a SIL-rated system's vulnerability to cyber attack is a matter of considerable urgency.

A Practical Example

Imagine a SIL 3 system implemented to close the gap between the protections offered by a **pressure relief valve** combined with other LOPs and an organization's tolerability level. The SIL 3 system is put in place to achieve a better Probability of Failure on Demand average (PFDavg) than 0.0005 (i.e. 1/2000), which closes the gap. The PFD of a good pressure relief valve is normally on the order of just 1%. With all Layers of Protection present and functional, including the SIL-rated SIS, the system's probability of failure resulting in a death is 1 in a million-and that is good.

However, if the SIL-3-rated SIS is on the network and a cyber attack occurs which shuts down its functions, what is left is the relief valve and the other independent LOPs. It is as if the SIL-3 system did not exist, and the probability of an incident rises accordingly to beyond the corporate tolerability level. Should any of the other independent LOPs be impaired, the chances of an incident occurring increases even more. If all standard interface connected or virused Layers of Protection are compromised by the attack, and all that is left are the independent protections, then the probability of the unwanted event can drop from the intended 1 in a million to a highly likely event, such as a 1 in 10 likelihood of occurrence, or if the relief valve is truly independent then 1 in 100 likelihood.

Preventing Access to SIL-Rated SIS

One means of avoiding such a scenario is simple: if the SIL-rated SIS is not on the data highway at all then it can neither be reached remotely by unauthorized people, nor can it communicate remotely as a result of a virus infection. The latter situation can come to pass

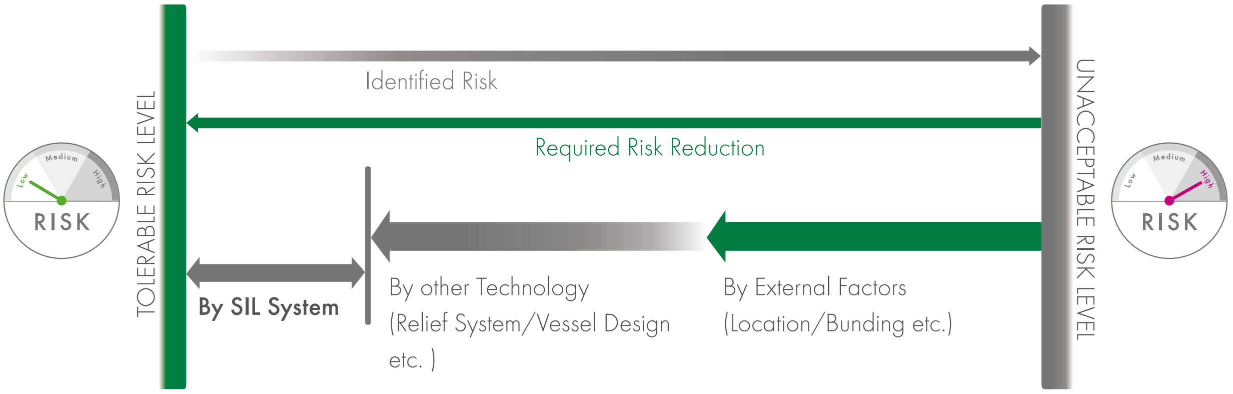

Figure 1 IEC 61508: Hazard & Risk Analysis

even if the SIS is not on a network, because a corrupted device like a memory stick could be unwittingly put into the SIS by a maintenance engineer, for example. Cases like this have occurred wherein a virus instructs a computer to contact another point on the network that then allows the cyber attacker to gain access unnoticed because the communication was initiated by the controller and not an external cyber attacker?

If a virus has attacked the SIS, then proof testing should identify if the SIS still works or has failed. Proof testing is mandatory for SIS, so the only questions have to do with its frequency and scope. A virus that allows the SIS to continue functioning properly but simultaneously requires the controller to set up communications cannot be detected by the proof test, but if the SIS is not on any data highway then it cannot set up communications.

The Value of Expert Cybersecurity Risk Assessments

Considering the ways in which SIS may be vulnerable, it is clear that risk assessments are required. The fundamental question that such an assessment must ask is not "how or why" a cyber attack happens, but instead, "When a cyber attack succeeds then what is the risk to personnel and the environment?" This question enables organizations to understand how important each safety system is and determine if additional proof testing is valuable. It also reveals how integral SIS systems are to safe operations and enables decision makers to decide whether the SIS should be on the network based on the seriousness of the consequences should it fail.

A risk assessment that looks at all the Layers of Protection and identifies those that are independent and NOT open to cyber attack is essential. If the outcome of a cyber attack is a serious risk to people or the environment then additional, properly independent Layers of Protection are needed. For the most serious risks of attack, SIS independence is valuable and important, but the additional Layers of Protection need to be independent as well.

An analysis that identifies the risk to people and the environment is the very analysis that enables businesses to manage and prioritize spending. If the analysis shows that there is little risk to people on one part of the network, then the organization can concentrate instead on the section of the network that poses a higher risk. It is unfortunately too often the case that organizations see cyber defense as a colossal, undifferentiated expense and spend vast sums of money indiscriminately. A risk assessment that explores what happens to people and the environment when - not if - a cyber attack succeeds empowers organizations to plan sensible countermeasures and manage and prioritize spending, resources and efforts. An informed, efficient risk analysis ultimately leads to responsible investment over time and better outcomes at every stage of SIS implementation and improvement.

Safety Solutions That Think Forward

360°CYBER SECURITY

Our cyber security experts develop and deliver consulting solutions that reflect the needs of our rapidly changing industries as they adapt to evolving information technologies and confront the challenges of cybersecurity. **Cyber security** has become a universal necessity, essential for organizations of all sizes and sectors, especially with the ever-increasing use of industrial automation and the Internet of Things. Our consultants offer comprehensive and customized solutions to secure your data, network and products as well as your IT infrastructures and processes. We have compiled a comprehensive portfolio that allows you to address all your cyber security concerns under one roof.

CLIVE DE SALIS

Clive de Salis is Principal Process Safety Specialist and consultant in process design safety, critical instrumentation and hazards. He writes both the IEC62443 series of standards on Cyber security and the IEC61508 series, which includes IEC61511 on SIL, rated systems. His main areas of expertise are process risk assessment, including HAZOP, with extensive experience in the design and installation of safety systems and determination of safety integrity levels. His recent experience includes expert witness selected by barristers and solicitors for dust explosions.

DR. ARTURO TRUJILLO

Dr. Arturo Trujillo is Global Director of Process Safety Consulting. His main areas of expertise are diverse types of process hazard analysis (HAZOP, What-if, HAZID), consequence analysis and quantitative risk analysis. He has facilitated more than 200 HAZOPs over the last 25 years, especially in the oil & gas, energy, chemicals and pharmaceutical industries.

DEKRA Organisational & Process Safety

DEKRA Organisational and Process Safety are a behavioural change and process safety consultancy company. Working in collaboration with our clients, our approach is to assess the process safety and influence the safety culture with the aim of ‘making a difference´.

In terms of behavioural change, we deliver the skills, methods, and motivation to change leadership attitudes, behaviours and decision-making among employees; supporting our clients in creating a culture of care and measurable sustainable improvement of safety outcomes is our goal.

The breadth and depth of expertise in process safety makes us globally recognised specialists and trusted advisors. We help our clients to understand and evaluate their risks, and work together to develop pragmatic solutions. Our value-adding and practical approach integrates specialist process safety management, engineering and testing. We seek to educate and grow client competence to vide sustainable performance improvement; partnering with our clients we combine technical expertise with a passion for life preservation, harm reduction and asset protection.

We are a service unit of DEKRA SE, a global leader in safety since 1925 with over 45,000 employees in 60 countries and 5 continent. As a part of the world’s leading expert organisation DEKRA, we are the global partner for a safe world.

We have offices throughout North America, Europe, and Asia.
For more information, visit www.dekra-uk.co.uk/en/dekra-organisational-and-process-safety/
To contact us: dekra-ops.uk@dekra.com
To contact us: +44 (0) 23 8076 0722

Would you like to get more information?

Contact Us

DEKRA