CYBER and IEC61511: DEFENCE IN DEPTH

Clive de Salis, Principal Process safety Engineer, DEKRA, Phi House, Southampton Science Park, Southampton, Hampshire, United Kingdom SO16 7NS

This paper talks about why defence in depth i.e. more than just one safeguard) and how diversity of types of safeguards, are both essential if the protection of people and the environment are to be achieved. In doing so, this presentation concentrates on misunderstandings and mistakes encountered when doing actual Cyber-protection projects on process plants.

The world of process plant control and safety has a few differences to what the main-stream media ("MSM") understand as the world of office work. I deal with process safety. There are several standards and guidance documents all trying to achieve the same end. The two main standards are the ISO standards and the IEC standards.

IEC62443 is now the European Norm,.but...from the perspective of publicity, people have been bombarded with the problem of protecting computers, an I.T. network and data highways. However, the truth is that the number of words in a standard is NOT proportional to how important the statement is.

For EN62443 we have written a huge amount of words, for obvious reasons, on how to protect your computer systems …. BUT … not very many words on what is equally important in every respect! The HSE guidance OG0086 is representative of what safety inspectors want to ask about. OG0086 talks about diversity of safeguards and defence in depth, so this is about how to use independence from Cyber attack within your barriers and safeguards.

We need BOTH barriers that are genuinely INDEPENDENT and barriers to protect the data highway to get defence in depth. Protecting the data highway alone is not enough.

For barriers some need to be high integrity so the ONLY part of IEC61511 that allows SIL assessment to be designed and calibrated for Cyber attack specifically has been used. The analysis showed that SIL assessment against Cyber attack can only be qualitative because, currently, no precise numbers are available.

Keywords:Cyber, IEC61511, IEC61508, defence in depth, diversity, independent barriers.

CYBER and IEC61511: DEFENCE IN DEPTH

By Clive de Salis, DEKRA Process Safety

A Brave New World of Interconnectivity

In today's world, interconnectivity, digitalization, automatic control systems and other technological advances are buzzwords that permeate both work and play. These phrases do actually have meaning, and they are not just buzzwords. Indeed, we use the same tools on a daily basis to "optimize" their private lives. The tools have also been adapted to optimize industrial processes of every type. Today almost all process plants have industrial control systems (ICS) embedded in the various levels of the company's digitalization, from field devices (instruments, actuators, relays, etc.) to the highest level of corporate servers. For convenience and cost, too often there is commercial pressure to use the same tools that allow remote access to the control systems suppliers for them to be able to undertake maintenance and enact changes. The same is true of allowing remote access to others in the user's business who work remotely to the actual process plant. The very obvious problem with that approach is the opening up of any process plant control to remote cyber attack that has no physical risk at all to the attacker because they are miles and miles away.

ICS is the acronym you see in a lot of cyber attack prevention standards, and so is the acronym IACS (Industrial Automation and Control Systems) as that now often appears in government documents such as OG0086 in the UK.

These types of control systems remotely monitor and control worksites, acquiring and transmitting data without requiring personnel to travel long distances. The devices that make up an ICS can open and close valves, collect data from sensor systems and monitor the local environment. Within a single plant, an ICS can centrally control the various phases of production, gather and share data for quick access, and find and remedy faults while reducing their overall impact. Efficiency is not the only advantage to an automated system. Worker health and safety can also sometimes benefit from these systems' ability to detect danger quickly and reliably.

However, no system is invulnerable. In an industrial context, a technology malfunction can lead to financial losses, asset damage, environmental consequences and even injury to humans or ultimately loss of life. The scale of the consequences can be massive and can also be the result of criminal activity that targets vulnerabilities in these automated, centralized cyber-systems.

In the USA, last year, a water treatment and processing plant was cyber attacked and some valves opened leading to excess of sodium hydroxide, known in the USA as "lye", into the water. In excess this is a serious poison, but it was pure luck that an operator spotted that this excess was happening and manually closed off the supply.

The same commercial pressures apply at two levels to making the high-integrity SIL rated controllers to be the same controllers as those doing ordinary BPCS functions (Basic process Control Systems). BPCS is the acronym you see in the high integrity safety instrumented system standards IEC 61511 and IEC 61508. These standards they are used worldwide. Indeed, both standards are now European Norms which means that throughout western Europe the same standard is printed as EN 61511, and hence in the UK, for example, it is published as BS EN 61511, in which BS is the publisher (British Standards).

From a manufacturers' perspective the mass production of the same PLC as both a safety system PLC and as a BPCS PLC is cheaper leaving the only difference, if any, as the software. This makes the safety instrumented system ("SIS") something produced in greater quantity and cheaper to mass-produce.

Similarly, from the user's perspective spares holding becomes easier as it becomes the same PLC or parts that is held in stock somewhere and quickly replaced if it breaks down.

The trouble is that little of that is properly true when you start to get into the details.

A significant accident in Argentina happened when the BPCS PLCs and the Safety System PLCs were all made and supplied by the same manufacturer. When the cyber hackers got in they were going through the network and discovered that some PLCs had different barriers installed in the software preventing access. To the cyber-hackers this was like a big signpost telling them to attack because all the important and dangerous stuff must be behind these barriers – and so they did attack the Safety instrumented Systems as well.

We MUST understand, and realise, that the whole raison d'être, the whole reason and existence for cyber hackers is to defeat whatever you install. So, you can install more and more barriers and obstacles, but hackers are there to find a way to defeat whatever you put in.

The same scenario produced the situation in a control system in the UK when one weekend a controller used for SIL[1] 2 safety loops developed a fault. The maintenance engineer that weekend went into the stores and found another PLC that was also certified to SIL[1] 2, but of a different manufacturer. To shorten a longer story, he replaced the faulty PLC with the new one by another manufacturer. He was then shocked a week later when the government safety inspector asked how he had changed the proof test interval for the new model? His answer was "pardon?" followed by "Changed what?"

It is true that even if you make any of the mistakes above possible, then you still have to proof-test the new system from end to end once you have completed putting it in place. You must prove that the system is working correctly and keeping everyone safe. In simplistic language we have an annual MOT on a car as part of our car tax system. In an MOT they are NOT interested in how fast the car goes – they are very interested to show that the car can STOP safely and quickly. A proof test, like an MOT, is there to show the safety works.

Finally, we come in this risk category to the question of SOUP.

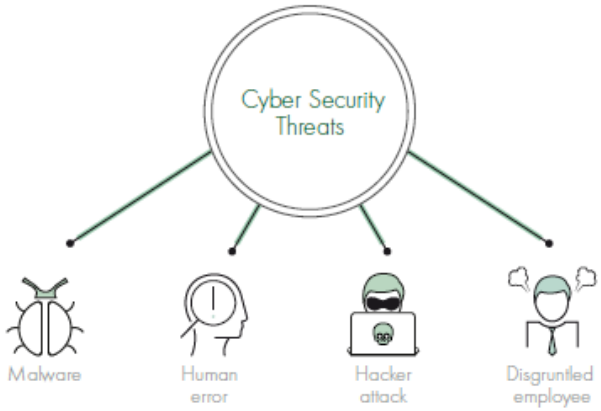
SOUP means "Software of Unknown Pedigree". In any safety system you must know that it will act in the same way every single time, there can be no variation on that. The moment you allow remote access, any adjustments to the configuration can have unintended consequences. Therefore, the act of allowing remote updates and maintenance is simultaneously opening the door to SOUP as the new reality.

We all know of cases where on own laptop, or on our PC, we have received an update of the Windows software and something stopped working properly, and sometimes would not even open. This experience is increasingly common on mobile phones, so it is not connected to the size of the device, it is instead derived from a noticeable lack of proper testing before it was issued as an update and installed. Even Windows can therefore be categorised as SOUP by those who try to use it as an operating system for either SIS or BPCS systems.

Facing the Downside of Digitalization

The scope of the damage that can be done when organizations fail to establish robust, resistant cyber protections is far greater than what may befall an individual technology user. When a plant fails or struggles financially, when the air or water is polluted, or employees' health and safety is compromised the effects are far reaching. Precisely because the stakes are so high, industry leaders must understand that cyber threats are just as potent as the safety risks they have confronted traditionally, and now can indeed hijack the conventional safety measures they have put in place. In this cyber-age, it is possible to disable alarms, manipulate controls, or tamper with the signals upon which workers rely for safety without needing any direct physical access.

Human error, the culprit behind many industrial accidents, continues to play a role in cyber-related disasters. Employees or contractors may inadvertently plug an infected machine into the system, connect to an unsecured network, download the wrong program or install malware. What is new, is the increased potential for remote attacks. A disgruntled employee who knows the system may be motivated by revenge. Hackers may break in to the network, often for "kudos", but now sometimes for publicity, financial gain or political advantage. Those seeking a competitive edge may steal secrets or cripple production. Other cyber-criminals may be intent on disrupting critical infrastructure from nuclear plants to water supplies to electrical grids. Whether small scale or large, simple or sophisticated, the risks created by advancing technology demand the attention of industry leaders.



[1] SIL = Safety Integrity Level, in which SIL 2 is a risk reduction of more than 10^2 (i.e. 100) up to SIL 3 of 10^3 or more (I.e. 1000).

Against this backdrop, safety authorities pose two main questions to their industrial clients and partners. First, if a cyber-attack is underway, what security measures are preventing it? Secondly, when (not if) a cyber-attack succeeds, what is the ultimate risk to people (and/or the environment)?

Both of these questions are crucial, but it is important to highlight the essential difference between them: one is concerned with attack prevention and the other identifies the ultimate unwanted risks to people and/or the environment.

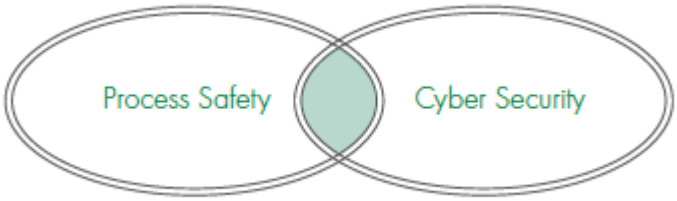
Hackers Make Headlines

In 2018, hackers made the biggest headlines with attacks on financial and political institutions, but infrastructure also fell victim. In addition to the high-profile assault on Britain's National Health Service in April 2018, a cyber-attack accessed US power grids over the summer. No damage was reported, but the perpetrators were able to gain vital information that could be used to inflict greater harm in the future.

So far, the results of most published cases of cyber-attacks aimed at industry have been limited to economic damage. In 2017, the petya virus was behind a 3% drop in one large company's quarterly sales figures and resulted in a loss of £110 million for another company. However, it is easy to imagine far worse outcomes. Terrorists could target plants that utilize hazardous substances as part of an attack on the civilian population, causing explosions, contaminating the air or water supplies and taking human life. These are not risks worth running. They require a systematic analysis and a proportionate response.

Cyber Protection with Process Safety Tools

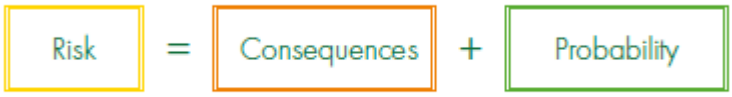
As frightening as these scenarios may be, it is important to realize that industry can leverage many of the tools it already employs as part of process safety management in the fight against cyber threats. Both process safety and cyber-security aim to prevent or mitigate events involving a loss of control of hazardous materials and energy sources. Recognizing and exploiting this overlap is key when building robust cyber defences.



The risk-based approach at the heart of the process safety lifecycle extends successfully to cyber-security in an industrial process context. Risk measurement frameworks traditionally used in process safety work equally well for cyber-security when applied correctly and thoughtfully. At the same time, each discipline has a distinct lifecycle requiring continuous management, and each affects multiple and overlapping aspects of industrial processes.

A Formula for Calculating Risks

The general principle used in process safety for assessing risk is applicable universally, wherever hazardous situations arise. Essentially, the level of risk is a product of the consequences produced by the hazard multiplied by the probability of those consequences coming to pass.



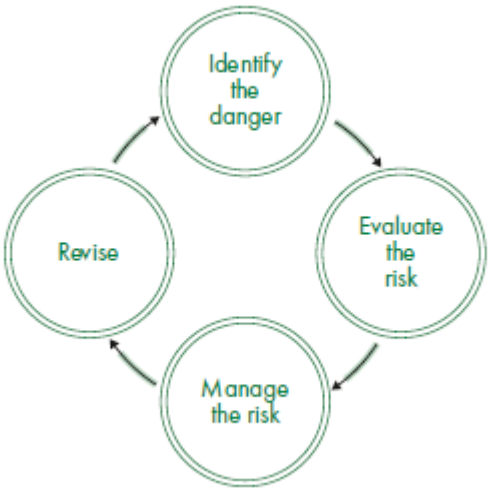
What is new is that a Cyber attack is now the cause of ICS / IACS failures.

In a cyber context, perhaps the hazard is that sensors used to indicate dangerous levels of certain substances become disabled as a result of hacking, technical malfunctions or user error. The consequences might include damage to machinery or other equipment or even injury to personnel. A worst-case scenario could involve an explosion that injures or kills people and releases toxins into the environment. So Cyber attack can be the cause and the consequence can be extremely serious. The likelihood is different when faced with a Cyber attack to what has traditionally been considered but the principles can often be the same.

The example above demonstrates the complexity of industrial hazards and underscores the importance of cooperation between EHS, IT and operations teams when confronting cyber-threats. There are no longer well-defined lines of demarcation among these divisions; the success of one in combating hazards is dependent on the others.

Interconnectivity Means Interdependence

The process safety lifecycle is typically conceptualized as four continuously repeating phases.



The simplicity of the graphic belies the complexity of the task, however. For instance, identifying hazards has to go beyond the superficial in order to be effective, and this requires experience and expertise. Current process safety management utilizes tools such as HAZID, HAZOP, CHAZOP and FMEA to facilitate this step, and these tools demand the input of professionals with an intimate knowledge of the processes in question. When processes are automated or digitalized, not only must health and safety officials and operations supervisors have a place at the table, but cyber experts as well.

The same goes for the second phase, risk assessment. Here, too, process safety specialists have developed instruments such as SIL and LOPA[2] to evaluate risk. When adapted for use in a cyber-context, these tools ensure proper independence of safety measures, as required by safety standards. In order to assess the resistance of a cyber network to attack, it is vital to investigate its weaknesses and points of access. Process safety tools can aid in these endeavours.

Managing risks means reducing their impact and frequency. Again, cooperation across disciplines is essential for effective risk management as industrial processes become increasingly intertwined with cybernetworks. Solutions designed by interdisciplinary teams drawn from EHS, operations and IT will undoubtedly prove more robust in the face of new technological hazards than single-discipline approaches.

The final phase, revision or review, can include audits, training programs, accident investigation and other forms of consolidation. It propels the lifecycle onward as new information comes to light regarding either internal blind spots or external developments and advances. With the rapid changes taking place in technology, this is an especially important step for a robust, resistant cybersecurity system.

Risk Assessment with a Cyber Twist

One of the most popular Process Hazard Assessment (PHA) tools used to identify dangers (phase 1 of the process safety lifecycle) is the Hazard and Operability (HAZOP) study. This is a process that is understood but increasingly government safety regulators are making clear that HAZOP is not the right tool for Cyber-attack risk assessment. However, simultaneously, governments are wanting to see Defence in Depth and diversity of safeguards.

A cyber-security assessment starts by looking at the cause of a given scenario, or the factors contributing to a deviation from normal processes. For instance, if a hazard arises from a technological failure affecting a reactor's automated temperature control loop, then the cause of this hazard is considered vulnerable to cyberattack. Conversely, if human error leads to an incorrect catalyst charge to the reactor, the cause is not vulnerable to cyber manipulation.

Therefore, the first step in any anti-Cyber attack risk assessment is to identify what are all of the Major Accident Hazards (MAH) for any process plant. For every MAH there are safeguards and barriers preventing the MAH from happening. If you compare the list of barriers and safeguards to each MAH you can find the safeguards and barriers that must resist Cyber-attack.

Having got a list of all the safeguards and barriers that prevent any specific MAH it is then realistic to ask if any of them cannot be made more independent so that they cannot be Cyber-attacked. This is turning a list of safeguards and barriers into "Defence in depth" and checking for genuine diversity between the defences. If the defences are lacking in diversity then whatever technique the Cyber-Hacker used to get through one defence will also get through the next one, and so on. Therefore, defence in depth on its own is not enough. The defences must also be diverse.

Diversity – Where new politically correctness badly distorts good engineering!

We said above: "…. governments are wanting to see Defence in Depth and diversity of safeguards."

"Diversity" is a real word, meaning, "The condition of being diverse; difference, unlikeness." *(The shorter Oxford English Dictionary, Volume 1, A-Markworthy, page 585).*

In the UK the early edition of OG0086, the government Health & Safety Executive guidance on cyber-security acknowledged the importance of diversity and defence in depth. If a cyber-attacker uses one technique to get through a barrier then it is really, really

[2] LOPA = Layer of Protection Analysis as shown in IEC61511 Part 3 Annex (and now also shown in IEC61508 Part 5).

important that the same technique does not get through all the other barriers. Therefore, it is not just "defence in depth", i.e. multiple barriers, that matters but what is also essential for safety is the other essential characteristic, i.e., that each of the barriers are "different" and "unlike each other" - That means all the barriers need to be diverse.

Unfortunately, in the new version of the UK government's guidance from the HSE, OG0086 says:

Diversity - No special requirements.

As the HSE pointed out to the writer, that is because within the civil service in the UK, i.e. in government, "diversity" is the term now used for male/female/trans, Black, White, Asian, LGBT, etc, etc. If the civil service really wishes diversity to have a new meaning then it is essential that an adjective is put in front of the word to make that clear. There is not an alternative word that engineers can use. This paper is written for engineers and for real people: Frankly a safeguard is a safeguard, and no engineer can make any sense of ever describing any safeguard as BAME / Male/Female/ LGBT etc – it is just nonsense.

We do need barriers with different characteristics to provide a robust & resilient cyber defence.

Every group of safeguards MUST use diversity by the proper, original meaning of the word (and there is no obvious word to use in its place once the political class pushes to redefine what they even mean by the word and to give a totally new meaning that never even existed before). If the defences are lacking in diversity then whatever technique the Cyber-Hacker used to get through one defence will also get through all of the other defences, and so this matters for safety.

Completed assessment leads to knowing what to do

A cyber-security assessment considers the different safeguards in place to ensure normal functioning, evaluating each of them separately. A safeguard is any mechanism intended to prevent accidents or to limit damages should an incident occur. An automated high-pressure alarm is a type of safeguard that is vulnerable to attack by cyber criminals whilst a pressure relief valve or rupture disc is not. In a cyber-attack situation, operators may find themselves relying on display data that has been manipulated to hide the actual attack. Alarms require operator action, and not only could the alarm itself be false, but the status of the process plant could equally be inaccurately reported as well. Alarm systems are, therefore, very vulnerable to cyber-attack.

If both causes and safeguards are vulnerable to cyber-attack, and there are no safety measures available that are resistant to such attacks, then the cyber-security assessment turns to the consequences: potential damage to people and the environment. Assessments can include the risk of a cyber-attack on production, assets and reputation.

IEC61511 requires security assessment to include cyber

I am one of a number who write not only the Cyber standards in the IEC62443 group, but also the safety instrumented system standards in the IEC61511 and IEC61508 groups.

When making the current edition of IEC61511 we included the requirement for a security assessment as part of the SIL assessment in part 1 clause 8.2.4. Since it is in Part 1 the requirement is normative, i.e. mandatory. As you read in part 1 it becomes clear that the SIL assessment for security includes security against cyber attack (for example see clause 12.4.2).

The problem for us is that we have not specified a technique to be used for such cyber-attack risks and, at present (and for the immediate future), there is insufficient data to do any quantitative cyber-attack assessment. Any cyber-attack SIL assessment has to be qualitative at the moment. However, I personally have used IEC61511 Part 3 Annex I to specifically design and calibrate a SIL assessment system for a process plant under cyber attack. Therefore, the IEC61511 standards still do give the tools to enable a qualitative SIL assessment to be done.

At this point, the cyber-security assessment has reached its objective: identification of potential major hazards and operational problems, in this case those that can be provoked by a cyber-attack. The report lists all the available safeguards and their vulnerability to attack. The generation and design of appropriate solutions takes place in subsequent phases of the process safety lifecycle.

It is also at this point that some errors in understanding also appear.

The Cyber standards talk about Zones and assigning your equipment into such zones. This is important BUT the zones are not the safeguards at all. The zones are important for understanding what is at risk. By putting together your process control network into zones then its purpose is to help you see that if a Cyber-Hacker gets into a zone at one point then they could access everything else in that same zone. Therefore, identifying the zones correctly does matter, but they are not safeguards that prevent an attack at all, they are a useful tool for you to see the attack potential holistically.

Which standard should I use? In truth, it is not as important as you might think, and both the ISO set of standards and the IEC set of standards could be used without much difficulty. Both the ISO 27000 set and the IEC62443 set are in the early stages of development. They are not incompatible with each other at all. To a layman, IEC62443 set is better for process control protection of any process plant, and the ISO 27000 set is better at protecting your offices, but in reality there is a clear overlap between the two and neither set is perfect at all.

What matters is to:

1. identify all the Cyber critical safeguards
2. Ensure diversity between safeguards and defence in depth for all Major Accident Hazards.
3. Ensure Critical Cyber Safeguards are sufficiently independent that they cannot be Cyber attacked.
4. Tag all Cyber critical safeguards so that they neither get altered by mistake nor the system around them getting altered by mistake.

5. SIL rate them to ensure the integrity is proportionate for their use.
6. Maintain them and proof test them regularly and keep records of the testing results.

Clive de Salis

August 2021

CLIVE DE SALIS

Clive de Salis is the Vice Chair of the I.Chem.E's Safety & Loss Prevention group in the UK as well as being an International Professional Process safety Engineer. Clive is also the author of the I.Chem.E's book on SIL systems. That book is directly referenced in IEC61511 now.

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, 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.

Phone number: +44 7502 414564

Email address: clive.desalis@dekra.com