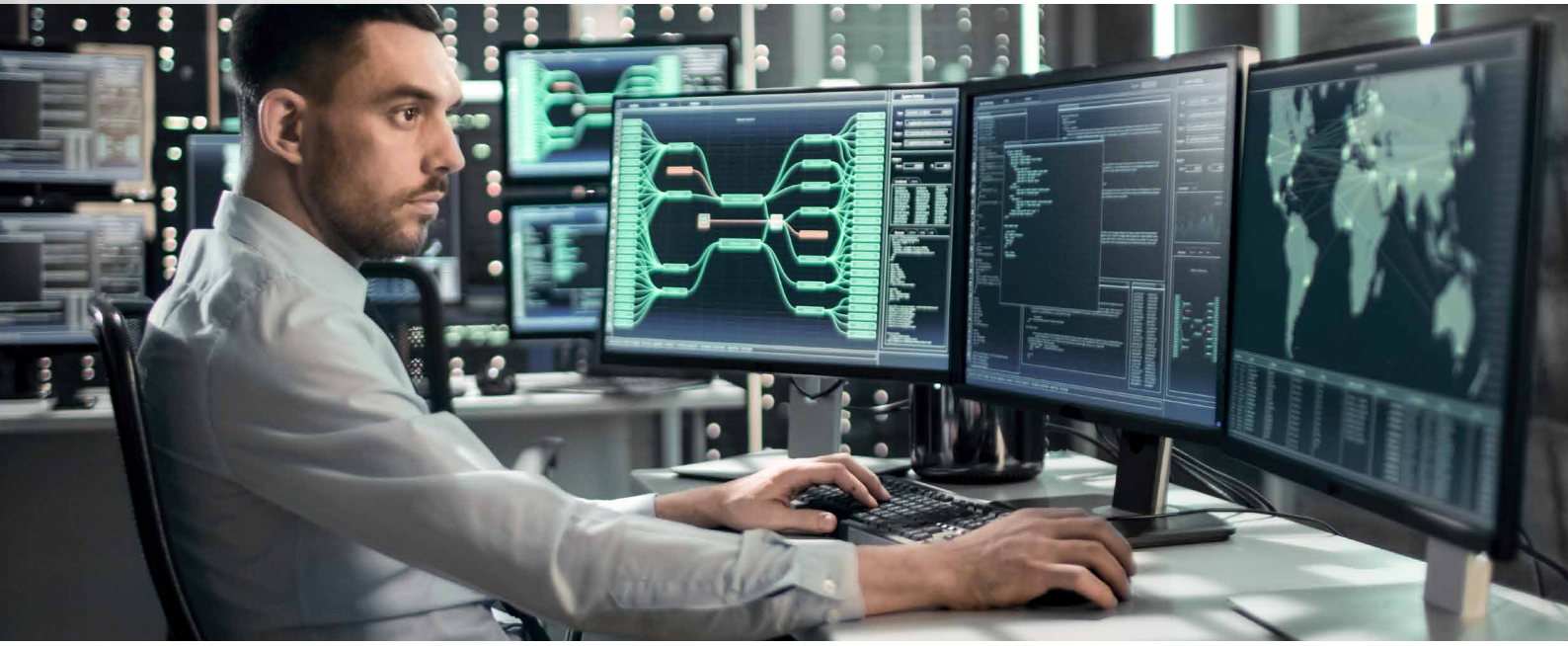


WHITE PAPER

# Cybersecurity and Process Safety: An Integrative Approach to Risk Management

## A Brave New World of Interconnectivity

For many of us, interconnectivity, digitalization, automatic control systems and other technological advances permeate both our work and play. What we may overlook is that the same tools we use on a daily basis to "optimize" our private lives have also been adapted to optimize industrial processes of every stripe. 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 ...) to the highest level of corporate servers.

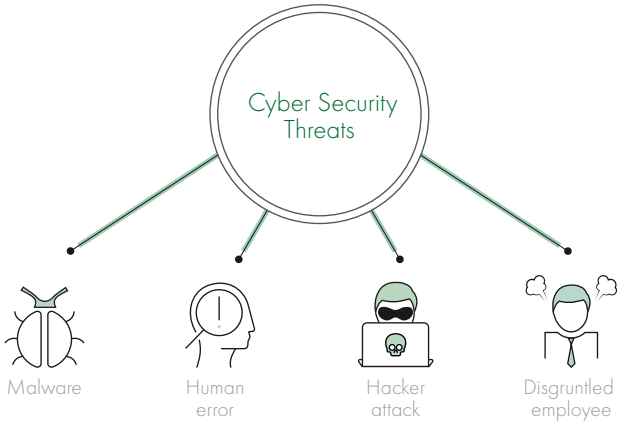
These systems can be used to remotely monitor and control worksites, acquiring and transmitting data without requiring personnel to travel long distances. The devices that make up an ICS can open and close valves and breakers, collect data from sensor systems and monitor the local environment. Within 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 also benefit from these systems' ability to detect danger quickly and reliably.

However, no system is invulnerable. We have all experienced breakdowns in the technology we use in our personal lives. In an industrial context, a technology malfunction can lead to financial losses, asset damage, environmental consequences and even injury to humans or 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 cybersystems.

## 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 a single 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. 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 can indeed hijack the conventional safety measures they have put in place. Alarms can be centrally disabled, controls can be manipulated, the signals workers rely on to ensure safety are vulnerable to tampering in the cyber age.

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 for financial gain or political advantage. Those seeking a competitive edge may steal secrets or cripple production. Other cybercriminals 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 posed by advancing technology demands the attention of industry leaders.




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

DEKRA can help extensively with both of these questions, 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.

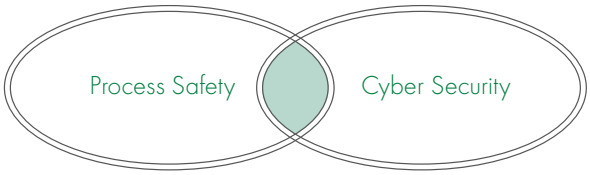
## Hackers Make Headlines

During 2018, hackers have made the biggest headlines with attacks on financial and political institutions, but infrastructure has also fallen victim. In addition to the high-profile assault on Britain's National Health Service in April, a cyberattack 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 cyberattacks 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. Corporate spies could exploit network weaknesses to steal secrets, sabotage production and inflict lasting damage on competitors. 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 **cybersecurity** 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 defenses.




The risk-based approach at the heart of the process safety lifecycle can be applied successfully to cybersecurity in an industrial process context. Risk measurement frameworks traditionally used in process safety work equally well for cybersecurity. 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

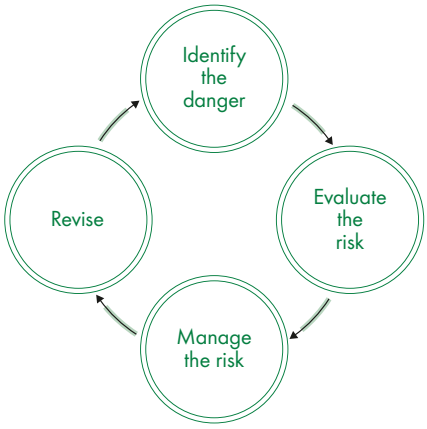
The general principle used in process safety for assessing risk can be applied universally, wherever hazardous situations arise. Essentially, the level of risk is a product of the consequences produced by the hazard multiplied by the probability of those consequences coming to pass.

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. The consequences would of course vary depending on the specifics of the plant in question, as would the third element, probability. This refers to the likelihood of an incident occurring. In process safety, this is a real number from 0 to 1. If an event is nearly certain, the probability assigned is near 1; if it is practically almost impossible, nearly 0.

The example above demonstrates the complexity of industrial hazards and underscores the importance of cooperation between EHS, IT and operations teams when confronting cyberthreats. There are no longer well-defined lines of demarcation among these divisions - the success of one in combatting 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. DEKRA actively integrates cybersecurity assessments when implementing these process safety tools, analyzing the ultimate risk to people when a cyberattack succeeds.

The same goes for the second phase, risk assessment. Here, too, instruments such as SIL and LOPA have been developed by process safety specialists to evaluate risk, and these can be adapted for use in a cyber context to ensure proper independence as required by the standard. In order to assess the resistance of a cyber network to attack, its weaknesses and points of access need to be investigated. Process safety tools can aid in these endeavors.

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.

## HAZOP With a Cyber Twist Becomes a Cybersecurity Assessment

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. DEKRA uses the familiar HAZOP approach and style to create a cybersecurity assessment of the process. This assessment evaluates not just the causes of, but also the safeguards against particular hazards. It pays particular attention to the independence of safeguards in terms of their vulnerability to cyberattacks, as well as identifying the ultimate risk to people.

First our cybersecurity assessment looks 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.

Our cybersecurity assessment also 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 cyberattack situation, the displays operators rely on may be 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 be inaccurate as well. Alarm systems are therefore very vulnerable to cyberattack.

If both causes and safeguards are vulnerable to cyberattack, and there are no safety measures available that are resistant to such attacks, then our DEKRA cybersecurity assessment turns to the consequences. Potential damage to people and the environment. Anyone can opt to include the assessment of the risk of a Cyber-attack on production, assets and reputation. Depending on the severity of the consequences, a corresponding Security Level (SL) can be determined using both of the IEC standards which are European Norms: EN 62443 and EN 61511.

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

## Moving Forward: Integrated Process Safety Management

Industrial control systems, like social media and on-line banking, are a fact of life in a digital age. The challenge is how to reap the benefits while minimizing the risks. We have seen how industry can expand proven process safety methodologies to strengthen resistance to cyberattacks. Indeed, cyber risks can be easily integrated into process hazard analyses (PHAs) in a way that prevents the unnecessary duplication of effort or expense. It is a matter of intelligently adapting existing PS tools and recognizing the interdependency of IT, EHS and operational concerns.
An experienced interdisciplinary team can effectively manage conventional process safety while simultaneously identifying and analyzing scenarios whose causes and safeguards are vulnerable to cyberattack - the framework already exists. Enlisting the help of third party process safety experts such as the team at DEKRA can ease integration of a cyber dimension into organizations' safety management systems. Among the many uncertainties digitalization brings one thing is certain: industry cannot afford to neglect cybersecurity issues.

### DEKRA Consulting

DEKRA Consulting combines evidence-based science, cutting-edge technology, and internationally renowned expertise to create innovative safety solutions for today and tomorrow. We aim to lead safety transformation at the workplace and business practices, within operations and processes as well as in the dynamic and rapidly changing digital era.

### Would you like to get more information?

Contact Us



DEKRA