DEKRA

Datasheet

Is Your Plant Safe from Cyber Attack?

Digitalisation, automatic control systems and other technological innovations are commonly utilised to optimise industrial process plants. These Industrial Control Systems (ICS) can be used to optimise efficiency and production.

However, these same systems that have been designed to optimise processes are just as vulnerable as any other digital system. A cyber-attack can result in environmental consequences as well as injuries or even fatalities and not just financial losses. The scale of the consequences can be substantial and is often as a result of criminal activity that targets vulnerabilities in these automated systems. The scope of the damage that can be done when organisations fail to establish robust cyber protections can be considerable. When a plant fails or struggles financially, when the air or water is polluted, or employees' health and safety is compromised, the effects can be far reaching.

Given the risks and subsequent consequences, organisations must understand that cyber threats are just as significant as the ‚traditional' safety risks, and cyber-attacks can hijack the conventional safety measures they have put in place. Alarms can be disabled, controls can be manipulated, and the signals that workers rely upon to ensure safety, are all vulnerable to manipulation via cyber-attack.

Importance of Cyber Security and Protection
Historically, the main-stream media has focused on protecting computers, I.T. networks and data highway, however, with ICS' being just as vulnerable to cyber-attack, the consequences can be far more devastating than the breach of personal data that is typically reported. Organisations therefore need barriers that are completely autonomous, along with barriers to protect the data highway.

When considering the possibility and consequences of cyber-attack to a plant, then looking at how to put things out of reach must form a major part of any Cyber Risk Assessment work; questions to consider include:

- Have you identified the areas vulnerable to cyber-attack?
- Have you identified what Major Accidents might be caused by a cyber-attack?
- Do you have clearly defined safeguards that require controls (cyber-security) to prevent remote access?
- Where are your independent barriers?
- Can you confidently answer HSE questions?

If you cannot answer the above questions positively, the cyber security of your plant should be of the utmost priority, given the potentially devastating outcomes of an attack.

DEKRA Cybersafe PS
The main points to consider when assessing cyber-attack risk include:

- The need to establish MAH (Major Accident Hazards) that could be caused by a cyber attack;
- The obligation to highlight all valid safeguards and barriers that prevent such devastation;
- The requirement to create a schedule of all the cyber-critical independent safeguards;
- The need to produce a schedule of all MAH for which there are no independent safeguards and for which you must rely upon computer protection systems alone.

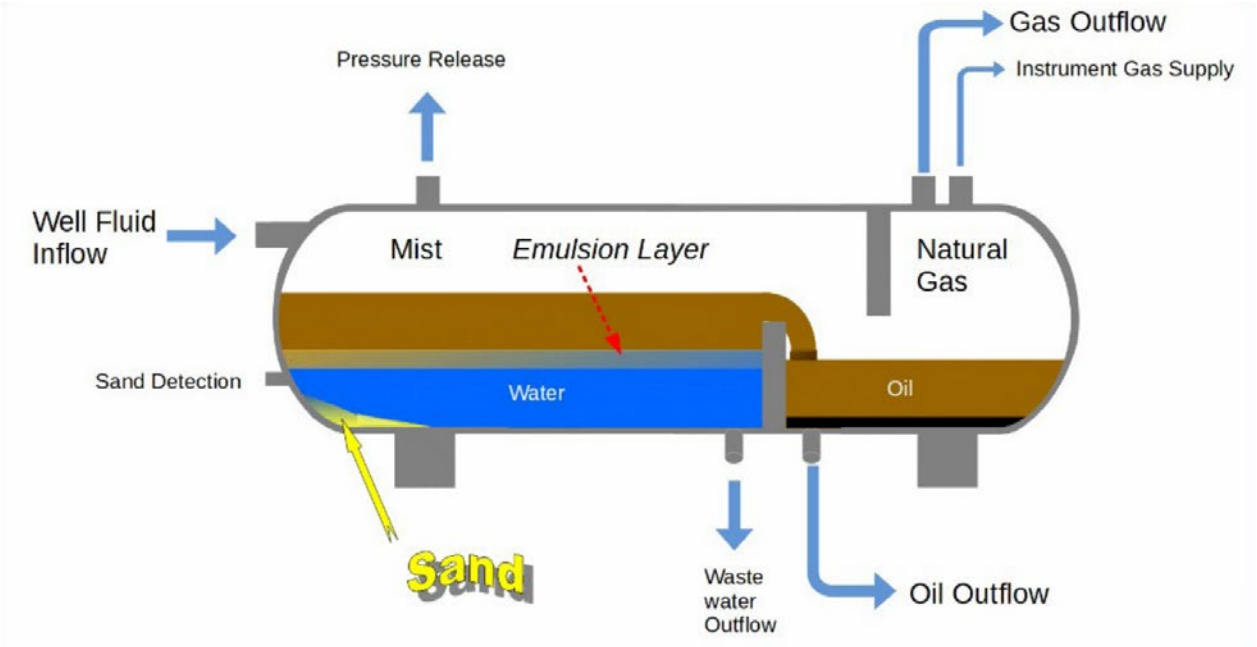
The DEKRA Cyber SafePS solution has been designed to identify the cyber security risks to the plant; highlight the different types of safeguards, from the vulnerable, to the acceptably secure and robust; enable potential consequences to be identified; enable organisations to determine effective solutions. Our Cyber SafePS assessment identifies all barriers against cyber-attack that are genuinely independent and guides clients through protection for people; the environment; assets.

Understanding the Concept
Almost every offshore platform has an oil, gas and water separator; sand and sea-water residue is separated out and disposed of, leaving the gas and oil to go forward to the process plant.

In this example, the possible Major Accident Hazards are:

- Cyber-attack could close valves and stop waste liquid being taken out; liquid fills the vessel, blocks it and suddenly all oil and gas to the plant stops.
- Cyber-attack closes the valve before the pressure relief valve used for pressure release; on high pressure, the vessel could rupture and explode.
- The flushing out of the sand is stopped by cyber-attack; this allows sand to stay in the with the oil.

Every Major Accident Hazard has barriers and safeguards that prevent it from happening so that everyone is kept safe. In the example, simply making the valve beneath the pressure relief valve a manual valve that cannot be operated from the control system highway will prevent Cyber-attack,



similarly to firewalls and software systems that stop Cyber-attack. The example demonstrates that safeguards can be simple; it is possible that pipe and vessel pressures can now be additional protections. Plants must however ensure there is diversity of barriers so that no MAH relies on just one barrier; diversity of safeguards = not just ONE barrier.

DEKRA Cyber SafePS system performs the analysis for you, highlights the level of diversity and defence in depth you have in your process plant and shows what must be identified as cybercritical barriers and safeguards. The solution also automatically shows what cyber-critical barriers need to have high integrity (SIL rating), as well as giving you the simple network diagram the standards require.

The DEKRA approach ensures the right balance between independent barriers and computer and data highway protection and our experts assess the risks to produce a Cyber Assessment Report; which includes a number of schedules that ensure all cyberCritical safeguards are identified and ensures clients have the “defence in depth” and “diversity” in protections required by the HSE.

DEKRA Organisational & Process Safety **Contact**

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 understand and evaluate their risks, and we work together to develop pragmatic solutions. Our value-adding and practical approach integrate specialist process safety management, engineering, and testing. We seek to educate and grow client competence in order to provide 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 48,000 employees in 60 countries and five continents. 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**

Would you like more information?

Contact