CYBER SECURITY INCIDENTS & THEIR HSE IMPACT ON TANK TERMINALS

Tank terminal operations are more and more dependent on systems to operate the facility in a safe manner due to the increased complexity of OT infrastructure. The infrastructure frequently consists of integrated legacy and non-legacy infrastructure including the application of new technology like Industrial Internet of Things (IIoT), which raises the risk that a cyber security incident occurs.

Hudson Cybertec, an independent security solutions provider with full focus on the OT domain, often encounters situations where organisations underestimate their cyber security resilience. Standards like the 2700X standards developed primarily for the IT domain, are applied to the OT domain with little or no consideration for its specific environment. Reliance on existing security measures for safety instrumented systems (SIS), the usage of outdated policies and procedures all give a false sense of security.

CYBER SECURITY RISKS

Cyber security risks for tank terminals are present in all forms. Threats can originate from inside and outside the organisation and are continuously evolving. This means that a storage operator's OT-domain cyber security needs to evolve as well. Tank terminal operations must be prepared by being aware of the latest threats and staff need to know what to do in case of an attack. It is recommended that cyber security is well integrated in the operation of a tank terminal. Only if this is the case can you ensure that cyber risks, including disruption in operations (loading/unloading), financial gain (stock manipulation) or industrial espionage (access to confidential data), are managed appropriately.

Health, Safety & Environment (HSE)

Tank terminals are built so that HSE risks are minimised. However, recent incidents show that even SIS is vulnerable to attack. After a successful breach, existing infrastructure is manipulated so that the breach is not detected. Based on the point of entry, the malicious hacker has direct access to the OT domain or uses various systems in the IT domain to reach the OT domain.

Once access is obtained, the malicious hacker ensures that changes are not detected, by modifying firmware, applications or dataflows without the operator and control systems being aware. This results in the loss of control or loss of view of primary processes.

For example, multiple control valves that are installed in order to ensure a safe operation can be controlled and manipulated such that the control systems or safety systems do not take appropriate action in case of an anomaly. Alarm notifications can be manipulated or suppressed, so that either no alarm is given or that an alarm is changed to reflect a situation with less priority.

If cyber security was not considered during the design of a tank terminal, or an organisation relies on security measures that are not up-to-date, it can leave the tank terminal vulnerable to cyber-attacks. In case of a successful hack or breach, existing HSE measures may prove inadequate. When a breach or manipulation of information is finally detected, it is safe to assume that the installation has been comprised for some time. Therefore, operators should take control of cyber security within the organisation in order to increase the resilience level of the organisation.

TAKING CONTROL OF CYBER SECURITY

Tank terminals should be prepared, both on an organisational and technical level, for the latest threats and they should perform cyber security checks regularly. The international Industrial Automation & Control Systems (IACS) cyber security standard IEC 62443 provides the basis to incorporate cyber security within an organisation.

Decisions on how to implement cyber security within a tank terminal can only be made if operators know where they stand with regard to the cyber security of the organisation. As a first step to take control of your cyber security, Hudson Cybertec often performs a baseline measurement in the form of a cyber security assessment, as a starting point to improve cyber security at a tank terminal.

The results of the cyber security assessment show where there are weaknesses at both an organisational and technical level. Based upon the results of the assessment, a plan of action can be formatted in order to remediate any found weaknesses. A cyber security management system can be used to ensure that cyber security is applied in a controlled manner throughout the organisation.

ONGOING PROCESS

Cyber security is an ongoing process and needs to be integrated within an organization as part of operations. This will minimise the potential of successful attack and the potential impact. Since a cyber security incident can have an impact on primary processes and can make HSE measures inadequate, ideally it should be given the same attention as HSE.

As part of the ongoing process, a regular independent review of an OT-domain against the IEC 62443 standard combined with the current threat landscape, should become part of normal tank terminal operations. This ensures cyber security policy and measures taken to mitigate the risk are up-to-date to handle current threats.

FOR MORE INFORMATION

This article was written by Ilya Tillekens, senior security consultant, Hudson Cybertec.
www.hudsoncybertec.com