HEIGHTENED SECURITY RISKS REQUIRE ADAPTABLE OPERATIONS

The increasing pace of digitisation over the last few years has made cyber security a core topic for the storage industry.

Not a single day passes without news about yet another cyber attack. New software to protect against current threats is being released continuously, but issues related to cyber security often come from internal 'attacks'. Incorrect handling of IT-related issues often causes information asymmetries, for example regarding the current hardware or software status of individual plant sections, which increases the vulnerability of an entire industrial plant. Modern, smart maintenance solutions constitute a comprehensive approach for these issues.

Industrial plants are not just becoming more complex, they are also becoming more digital – Industry 4.0 and Internet of Things (IoT) are some of the most prominent examples of this trend. However, in addition to having the capability to operate with increased efficiency, modern plants are also more likely to suffer from unplanned shutdowns due to cyber attacks. These 'attacks' can come from the inside as well as the outside.

Critical infrastructures, which include the oil-processing industry, are one of the areas where potential damage can be especially severe. In its latest report 'Status of IT Security in Germany 2017' (Lage der IT-Sicherheit in Deutschland 2017) the German Federal Office for Information Security (BSI) pointed to the particularly high risk of unplanned shutdowns that critical infrastructures are exposed to.

In some cases, the direct damage can be accompanied by even more severe indirect damage, for example due to power shortages, shutdowns of telecommunication networks or difficulties in ensuring the provision of medical care.

HYBRIDISATION REQUIRES ADAPTABLE STRUCTURES

As modern plants become increasingly complex, particularly as a result of digitisation, detailed knowledge of a system's digital key characteristics is especially important to proactively identify disruptions.

Unfortunately, operators often do not have this knowledge, either because the facility is old or because it has been constructed by a subcontractor, who did not pass on the necessary knowledge to the operator. Additionally, a lack of interconnection between the current utilised monitoring tools often leads to relevant data flows being insufficiently represented, which can in turn lead to reduced oversight and an increase in operational errors.

The concept of cyber security therefore needs to be viewed from an internal perspective. Hybrid facilities in particular need to be monitored and controlled holistically in order to anticipate errors and prevent unplanned shutdowns.

For example, software changes in the wrong section of the plant due to incorrectly documented IP addresses or compatibility issues due to outdated key figures are just some possible sources of errors. In contrast, holistic cyber security also needs to be aware of such internal processes via seamless data collection. This includes basic information like hardware and software configurations, topology, and data flows, but also meta data, such as locations, plant reference, system networks, personal responsibilities as well as information about references, architecture, configuration drift, product data and known issues.

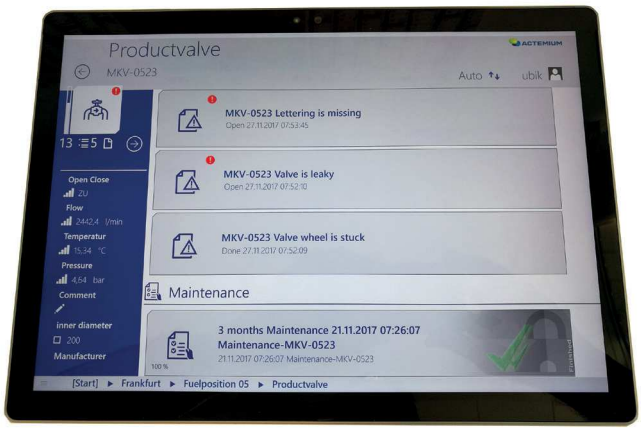
To achieve this, a modern maintenance model which intelligently combines the areas of analysis, automation, visualisation, and maintenance is required. At the same time, it needs to ensure that the demands of both international standards like IEC 62443 (industrial communication networks – network and system security) and national standards such as the German IT Security Act are fulfilled.

TRUST EXPERIENCED PARTNERS

Considering the multitude of requirements that must be met to ensure modern smart maintenance solutions are successful, operators need to be able to rely on trusted partners with the appropriate know-how.

In addition to having extensive experience in the areas of both information technology and operation technology, partners should also be able to present certifications, for example according to ISO/IEC 27005

(information security risk management). To ensure quality, it is prudent to collaborate with partners whose organisational and strategic measures are conducted in accordance with the PDCA cycle (plan, do, check, act). Example measures are – amongst others – structuring and design of the facility, monitoring, reporting, maintenance, analysis, assessment, and optimisation of the facilities. Of course, it is just as important to not just conduct the PDCA cycle once, but to regularly repeat it to facilitate a continuous process of improvement.



Smart maintenance: Actemium uses modern digital dashboards, which provide a comprehensive overview

MAINTENANCE BECOMES SMART MAINTENANCE

Systems integrators for automation and process engineering like Actemium – a subsidiary of the VINCI Energies Group – utilise holistic models, which take the special requirements of hybrid facilities into account.

The smart maintenance solutions used for that are designed to consolidate all necessary data from different systems – CAE, ERP, DCS, GIS or DMS. All the information is then made available to the operator on a mobile device. Should changes or adjustments become necessary during operations or if feedback data such as red lining, photos or other comments be relayed back to the operator, Actemium's solutions directly feed this data back into the basic systems. This ensures that the number of media interfaces used in the process is kept to a minimum and that all information is up to date at all times. That way, smart maintenance solutions are able to continuously keep all information about both operations and maintenance of the production facilities up-to-date and make the results of any ongoing processes available for review.

CONCLUSION

During daily operations cyber security can only be implemented successfully if the responsible decision-makers are able to holistically monitor the digital environment of their facilities. That way, unusual events can be addressed immediately and errors resulting from insufficient documentation can be eliminated.

Another key role is the attitude of the staff towards security issues. 'Cyber security is not an inconvenient add-on, but an essential part of our daily business', says Sabine Walitzi, project manager at Actemium Oil & Gas and Environmental Solutions. Unplanned shutdowns of facilities are not always caused by cyber attacks from the outside, sometimes their source is internal. This means that the issue of constantly changing threats can only be solved with an adjustable, constantly reviewed operational and maintenance model.

FOR MORE INFORMATION

This article was written by Klaus-Peter Fischer, business unit manager, Actemium Oil & Gas Environmental Solutions. www.actemium.de/en/
klaus-peter.fischer@actemium.de