A-183

Cybersecurity: From Theory to Practice

J. Möller
Siemens AG, Digital Industries, Mannheim, Germany

Increasing digitalisation and networking pose major challenges for critical infrastructure companies in terms of the security of their systems and data. In order to effectively counter these threats, the European Union has developed the NIS 2 Directive, which is specifically tailored to the requirements of KRITIS companies.

The presentation will focus on the important and current topic of cybersecurity in the oil and gas industry. In view of the increasing digitalisation and networking in the industry, the security of information systems is of the utmost importance.

The first part of the presentation deals with the **legal requirements**, e.g. through NIS2 and the IT Security Act (KRITIS). These laws and regulations form the framework for the security measures that companies in the oil and gas industry must take.

The second part deals with the differences between **safety and security.** Although these terms are often used interchangeably, in practice they have different meanings and implications, especially in relation to cybersecurity.

The third and final part of the presentation highlights the technical cybersecurity **fields of action** (e.g. segmentation, OT/IT separation, DMZ1, attack detection systems) in the oil and gas industry (KRITIS). Practical measures and strategies that companies can implement to protect their systems and data will be presented.

This presentation is aimed at companies in the oil and gas industry that want to expand their knowledge of cybersecurity and better protect their systems.