AMERICAN PETROLEUM INSTITUTE

IADC

Cyber Risk Management for Industrial Control Systems (ICS) in the Offshore and Onshore Oil & Natural Gas Industry

The **American Petroleum Institute (API)** is the only national trade association that represents all aspects of America's oil and natural gas industry. Our more than 625 corporate members, from the largest major oil company to the smallest of independents, come from all segments of the industry. They are producers, refiners, suppliers, marketers, pipeline operators and marine transporters, as well as service and supply companies that support all segments of the industry.

The **International Association of Drilling Contractors (IADC)** represents members that own most of the world's land and offshore drilling units that drill the vast majority of the wells producing the planet's oil and gas. IADC's membership also includes oil-and-gas producers and manufacturers and suppliers of oilfield equipment and services.

Managing cyber risks for industrial control systems (ICS) is a priority for API and IADC member companies active in both the offshore and onshore oil and natural gas industry. The digital automation of industrial control systems (ICS), the real-time data monitoring of offshore and onshore infrastructure and the commercial sensitivity of intellectual property require that companies protect these assets from being compromised.

Cyber Risk Management, or **Cybersecurity**, is "the process of protecting information by preventing, detecting, and responding to attacks."[1] API and IADC member companies' cyber risk management and cybersecurity programs encompass protections against malicious or non-malicious threats, with emphasis on maintaining the operational integrity of digital systems and assets from disruption, including in order to prevent a health, safety or environment (HSE) incident.

API and IADC member companies use a risk management approach for cybersecurity. Most, if not all, of the largest API and IADC member companies **manage cybersecurity risk at an enterprise level** with oversight from Boards of Directors and Senior Executives. API and IADC member companies deploy company-wide cybersecurity programs and systems intended to prevent or mitigate the risk of cybersecurity incidents.

These programs include conformance to **internal policies and external standards** through a range of specific initiatives and controls. Many API and IADC member companies:

- Orient their overall cybersecurity programs around the ***NIST Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity*** and their ICS security programs around the ***ISA/IEC 62443 Series of Standards on Industrial Automation and Control Systems (IACS) Security***.
- Use the ***IADC Guidelines for Assessing and Managing Cybersecurity Risks to Drilling Assets***, which provides guidance for conducting risk assessment and applying key external standards and controls to drilling assets.
- Use ***API RP 75 Development of a Safety and Environmental Management Program for Offshore Operations and Facilities***, which prompts for the management of all potential risks (which may include cyber) that could compromise safety and environmental performance for offshore operations.

[1] NIST. ***Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity***. p. 37.

energy API
AMERICAN PETROLEUM INSTITUTE

IADC

Typical Cyber Risk Management Controls

Cyber risk management at any individual API or IADC member company is tailored to that company's assets and potential risks and must also be flexible to respond to ever-changing external threats and internal deployment of digital assets. Companies assess their industrial control systems (ICS) to identify and manage cyber risk throughout the lifecycle of ICS, which includes software and hardware as well as specific capabilities such as communications protocols. Although one size does not fit all, the following key high-level controls are typical features for managing cyber risks for ICS of many offshore and onshore oil and natural gas industry companies:

- **Inventory of Digital Controls of Critical Systems.** Companies document their assets that require protection in order to assess the potential vulnerabilities and/or threats to vessel, process and marine systems.
- **Training and Security Awareness.** Companies continuously develop and improve training and security awareness programs to increase and improve the cyber hygiene both on offshore and onshore installations.
- **Assessment of Vulnerability Management in Software Development.** Companies assess software developers' management of potential vulnerabilities in the software development lifecycle in order to take confidence in "off the shelf" software security and reliability.
- **Patching and Anti-Virus Protection for Industrial Control Systems (ICS).** Companies conduct patching and anti-virus protection of digital controls for critical systems when appropriate based on risk, with restrictions in access to these process control environments, such as requiring that vendors conduct patching and anti-virus installation/updates and validate patches prior to installation.
- **Segregation of ICS.** Companies segregate ICSs from the business IT network and the Internet, using perimeter defense control such as a firewall as well as an intermediate network (sometimes called a de-militarized zone (DMZ)) so that communications can only flow out of the ICS to the business network and not vice versa.
- **Hardening ICS networks.** As additional protection, companies set-up the ICS as a specialized network, to eliminate unneeded protocols (like unprotected email or internet connection) and to allow for white-listing to preclude unwanted code from running on the supervisory and control networks.
- **Secure Remote Access to ICS.** Companies manage access to the ICS remotely through secure channels. Many implement the additional control of ICS system hardening during procurement with features such as enabling authentication requirements, disabling insecure protocols, etc., during Factory Acceptance Testing (FAT) or commissioning. Additional measures may include actively monitoring remote access sessions and recording each session in video format.
- **Restricted Access to Programmable Logic Controllers (PLC).** Companies restrict personnel access to PLCs, e.g., by making PLCs accessible only in industrial cabinets available to authorized personnel, implementing single point of authority on vessel controls access and securing entire rooms with limited access, such as control rooms or power equipment. Port locks (USB & RJ45) may also be installed as physical security at each device and PLC.
- **Restrictions and Monitoring for access to Equipment and Systems.** End users see the value in remote technical support and therefore enforce restrictions and monitoring for access. Examples may include (a) control by single point of accountability in company personnel; (b) proper change management and permit to work required for vendors to begin work; (c) restricted access to port that is made available only to that vendor when access is needed; (d) restricting personnel access to using portable memory devices, including engineering laptops, USB devices and portable external hard drives; (e) scanning of USB devices off network prior to installing them within the ICS by a vendor; and (f) monitoring of network traffic once a connection is established by a vendor for authorized work.
- **Intrusion Detection on ICS.** Companies implement capabilities to monitor and detect intrusions to the ICS.
- **Periodic Onsite Cybersecurity-related Drills.** As in responding to other risks, companies conduct drills to improve their ability to respond and recover from potential cybersecurity incidents.