Cyber Dangers of Hazard Materials

In any given state or country, there are thousands of manufacturing plants and facilities which hold and use hazardous materials as part of their production processes. Failures in the production, storage or transportation systems of these plants may result in severe damage to public health and the environment. In most cases, these systems are operated, automated and controlled by computerized systems, or ICS (Industrial Control Systems), so a cyber event can potentially cause a failure or disruption in the computerized system and lead to a catastrophic hazardous materials event.

Examples of hazardous events that may occur due to a cyber incident:

- Emissions of gases that endanger the public
- Explosions of hazardous substances
- Excursions of hazardous materials to the environment.
- Hazardous industrial effluent to water sources or drainage systems

Recently, the Israeli Ministry of Environmental Protection presented a first of its kind cyber protection guide, to any plant or facility that stores or uses hazardous materials in its plant. The guide is based on the principles of defense theory by the INCD, which relies heavily on the American standards of NIST CSF regarding the security of computerized control systems, while adapting it to the world of industry and hazardous materials.

Level 0, Yet Again

In several of its control mechanisms for cyber readiness, the guide explicitly refers to Level 0 monitoring as a key element to manage, detect and eventually overcome cyber incidents that may affect the control systems. Among these control measures, one may find level 0 monitoring in these categories:

- Unidirectional connectivity
- Advanced Access Control
- Sealed Access Control
- Prevention of malicious malware (IDS anomaly detection)

This guide proves yet again, that more and more regulatory agencies acknowledge and refer to Level 0 as an integral part of their cyber perception and methodologies. Level 0 allows safe remote monitoring, safe access control and out-of-band authentication that Industrial Control Systems are operating as intended. Without Level 0 monitoring, one is only as strong as its network is, while networks were proven time and time again to be vulnerable. if you want to be safe, start with Level 0.

References of level 0 in the guide:

Clause	Required control	Details	Recommendations / Comments	Level	Checks	Number of controls in this section
	Advanced access control 4.7 The list of users with access authorizations to computerized systems and control systems for hazardous substances must be reviewed at least quarterly and updated if changes have occurred in the personnel and in authorized officers in the business. 4.8 A user's connection to a system must be blocked after 5 failed connection attempts, by disabling any possibility of connecting for a defined timeframe or until released by the system administrator.	4.11 We recommend at least 8 characters, at a complexity of 3 out of 4 (capital letters, lower-case letters, numbers and special characters). 4.12 For example: a laptop without connection to the Internet that never leaves the business's premises and is used solely to program the controller;	4.10 This can be implemented using a unidirectional connection system to electrical signals directly from the sensors and actuators (level 0) using a configuration that is completely severed from the enterprise network and is not affected by it. 4.13 A		4.7 Present an updated list. 4.8 Perform a test on a random station. 4.9 Demonstrate the mode of remote connection. 4.10 Perform a test using a computer that is connected	
4	**Maximum access control** 4.21 Computers that came from outside of the company or that left the premises must not be allowed to access computerized and automated systems managing hazardous substances. 4.22 Remote connection to the operating system must not be allowed, apart from viewing only (to view status) through a secure unidirectional connection. 4.23 Conditions for blocking the use of accounts must be defined and enforced according to the business's operating hours and according to the work schedules of the various types of employees.	4.21 Such as by technicians' laptops, SCADA applications for smart phones on the employees' devices. Examples of entry blocking conditions: weekends, nights.	4.22 This can be implemented using a unidirectional connection system to electrical signals directly from the sensors and actuators (level 0) using a configuration that is completely severed from the enterprise network and is not affected by it.	4	4.20 Check the documentation. 4.21 Present the unidirectional solution. 4.22 Present the mode of use.	3
11	**Unidirectional connection** 11.4 Computerized systems and control systems for hazardous substances must be restricted to exporting data to a cloud via unidirectional connection, using an approved solution for unidirectional transmission of information.		11.4 This can be implemented using a unidirectional connection system to electrical signals directly from the sensors and actuators (level 0) using a configuration that is completely severed from the company network and is not affected by it.	4	11.4 Present the unidirectional solution.	1