5 Concepts of IEC 62443

The standard IEC 62443 is based on several underlying concepts. Some of these are described in the first which was published in 2009. The following clauses summarize the actual concepts which will be described in the next edition of the part IEC 62443-1-1 [4].

5.1 Defense in depth

Rather than to rely on a single measure, it is commonly accepted that the protection of an automated industrial facility requires the implementation of complementary cybersecurity measures, each of them providing a layer of defense. If an attacker were able to overcome the first layer, the attacker would then have to overcome the second layer, and then the next layer, and so on before being able to reach the final target. This strategy is commonly called "defense in depth". The standard IEC 62443 addresses all parts of the strategy involving all involved actors.

The first defense layers result from the practice of OSM by the asset owner and are addressed in IEC 62443-2-1 [6]. Examples of such measures are security awareness, education, and training of personnel, physical entry controls of rooms, definition and continuous review of roles, privileges and responsibilities of the users of the automation solution, and the implementation of a business continuity plan in case of incident. The asset owner also has the responsibility to ensure the roll-out of security patches under consideration of the operational conditions of the industrial facility, see IEC 62443-2-3 [8] on the patch management process.

Further layers of the defense in depth strategy are created by the SLM. Examples are the segmentation of the network in zones, protection with firewalls, access control with identification and authentication mechanisms, and restriction of the actions of the users to the minimum needed for their function. This is the responsibility of the integration service provider and is covered by IEC 62443-3-2 [11] and 3-3 [12]. The policies and procedures of the integration service provider should avoid generating new vulnerabilities. For example, temporary accounts used during the design and implementation phases should be deleted, the newest security patch and virus pattern should be installed before starting operation, and the password complexity should match the required protection in accordance with the password policy of the asset owner. IEC 62443-2-4 [9] is the relevant document for these issues.

The inner layers are provided by deploying inherent security capabilities of components and systems used in the automation solution. They are developed by the product supplier and are addressed by the parts IEC 62443-3-3 [12] and 4-2 [14]. Typical security functions include protection against malware by virus scanners or whitelisting technologies, signed software download, and hardening or time delay mechanisms to protect against password

guessing. Security vulnerabilities can be caused weak implementations in the products. A stringent development process as addressed by the part IEC 62443-4-1 [13] should be implemented to reduce the probability of occurrence of such vulnerabilities.

As a summary, all actors must contribute to realize an efficient defense in depth strategy:

- The product supplier must develop components and systems with powerful inherent security capabilities to support the deployment of cybersecurity measures in automation solutions. The development process must ensure to reduce the risk to generate vulnerabilities during development activities.
- The integration service provider must use the capabilities of the components and systems to design and deploy SLM in automation solutions and act according to policies and procedures with the objective to reduce the risk of introducing new vulnerabilities.
- The asset owner must establish and practice OSM to reduce the risk of misuse of the during operation. This includes the continuous cybersecurity risk analysis as well as an incident response planning.

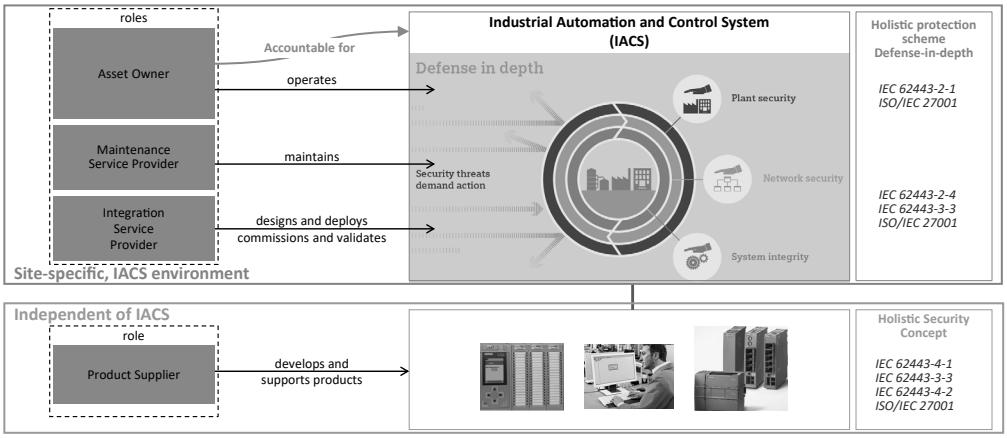

Figure 5.1 Defense in depth involves all actors.

The following examples in the area of "User Management and Access Control (UMAC)" illustrates that each actor must contribute to a defense in depth concept and avoid creating weaknesses due to activities in its area of responsibility. If hard-coded passwords are part of the firmware of products they can successfully be extracted by analyzing the firmware of such products. Many tools for this purpose can be obtained for free on the internet. Another typical weakness found in products is the possibility to circumvent user account management settings by elevating privileges and registering as an administrator which leads to many possibilities for misusing the product by a potential attacker. The product supplier (role PS) can avoid these weaknesses with stringent secure coding rules.

Deploying and configuring the products is the responsibility of the integration service provider (role SI) and requires changing the default passwords. Developers commonly set temporary accounts, protected by simple passwords for the development of automation solutions. It is understandable that developers do not want to enter complex passwords at each login.

An often-discovered weakness is that these poorly protected temporary accounts were not deactivated after commissioning and are still active during the operation phase. One can imagine what can happen if these accounts are misused. Integration service providers should follow policies and procedures which request to actively close these potential weaknesses.

Finally, the asset owner (role AO), in its responsibility as operator of the automation solution, must assign the names of users according to their respective roles. The asset owner must regularly maintain the list of active accounts of authorized personnel. As the operation phase often lasts many years, the responsibility of the asset owner to maintain the level of protection is very high. For example, if an administrator leaves the company it is essential to de-activate his account. If that person would intend to harm the company and the account were still active, it would be very difficult to defend this threat. Another duty of the asset owner is to ensure that passwords are treated confidentially and that they are regularly renewed. This should be documented in the policies and procedures, and their practice by the assigned personnel should be controlled.

All the measures described above are equally important to achieve a required protection regarding access control. A single non-implemented measure can weaken the protection chain and thereby will define the strength of the whole chain. A holistic protection scheme requires taking care to implement all measures since potential attackers search for the weakest link.

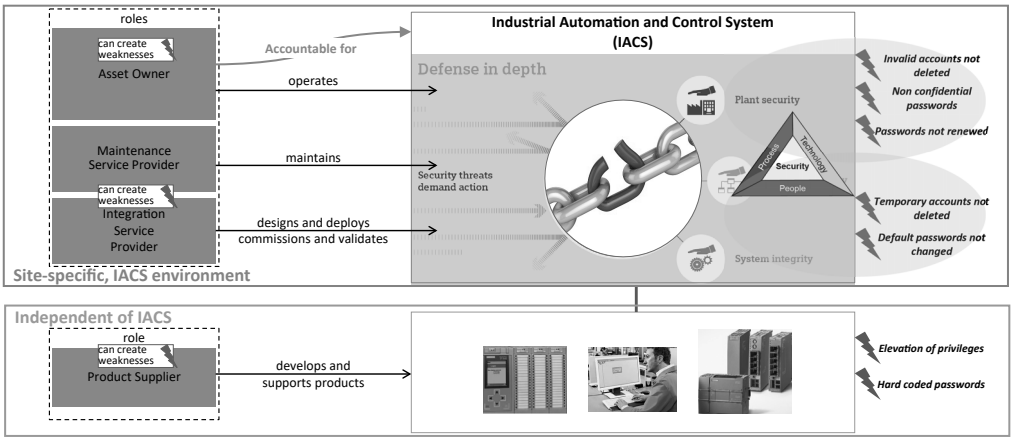

Figure 5.2 Each actor can create weaknesses; the weakest link defines the strength of the chain.

5.2 The standard IEC 62443 in product and IACS lifecycles

Although some products are specifically developed for a given project, the aim of the product supplier is generally to provide components and systems which meet the security requirements of their intended target markets and ensure a reasonable level of confidence that they are free from vulnerabilities. The product lifecycles are therefore independent from IACS lifecycles i.e. lifecycles of site-specific automation projects for industrial facilities.