4 Concepts of IEC 62443

Several basic concepts underlie the standard IEC 62443. Some of these are described in the first edition of the part IEC 62443-1-1 [4] which was published in 2009. The next edition is under development. The following clauses summarize the concepts described in the working document.

4.1 Defense in depth

Rather than rely on a single measure, it is commonly accepted that the protection of a plant in operation is optimized by implementing several complementary countermeasures, each of them providing a layer of defense. If an attacker were able to overcome the first layer, the attacker would then have to vanquish the second layer, and then the next layer, and so on before being able to reach the ultimate target. This strategy is commonly called "defense in depth". The standard IEC 62443 addresses all parts of the strategy involving all stakeholders.

The first defense layers have to be realized by the asset owner and are addressed in IEC 62443-2-1 [6]. An important barrier to realizing these defense layers results from the organizational measures given by security policies and procedures of the asset owner. These includes security awareness, education, and training of personnel, regulating 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 within the limits given by production needs; see IEC 62443-2-3 [7] on the patch management process.

Further layers of the defense in depth strategy are created in the design of the automation solution. Examples of the countermeasures are segmentation of the network in zones, protection with firewalls, access control with authenticators, and restriction of the actions of the users to the minimum needed. This is the responsibility of the system integrator and is covered by IEC 62443-3-2 [10] and 3-3 [11]. The policies and procedures of the system integrator should avoid the introduction of new vulnerabilities. For example, temporary accounts used during the design and set-up 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 level in accordance with the password policy of the asset owner. IEC 62443-2-4 [8] is the relevant document for these issues.

The inner defense layers are realized by functional 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 [11] and 4-2 [13]. Typical security functions include protection against malware by virus scanners or whitelisting technologies, signed software download, and hardening or time delays to protect against password guessing. Security vulnerabilities can be caused by faults (or bugs) in the components. A stringent development

process as addressed by the part IEC 62443-4-1 [12] should be implemented to reduce the probability of occurrence of such vulnerabilities.

As a summary, all stakeholders have to contribute to realize an efficient defense in depth strategy:

The product supplier has to develop components and systems with powerful integrated security capabilities to support the deployment of secured automation solutions. The process has to ensure the reduction of the risk of vulnerabilities generated during product development.

The system integrator has to use the capabilities of the components and systems to design and deploy secured automation solutions and to act according to policies and procedures which reduce the risk of introducing new vulnerabilities.

The asset owner has to establish and act according to operational policies and procedures which reduce the risk of security violation due to misuse of the system during operation. This includes in particular the continuous risk assessment of cyber threats as well as the incident response planning.

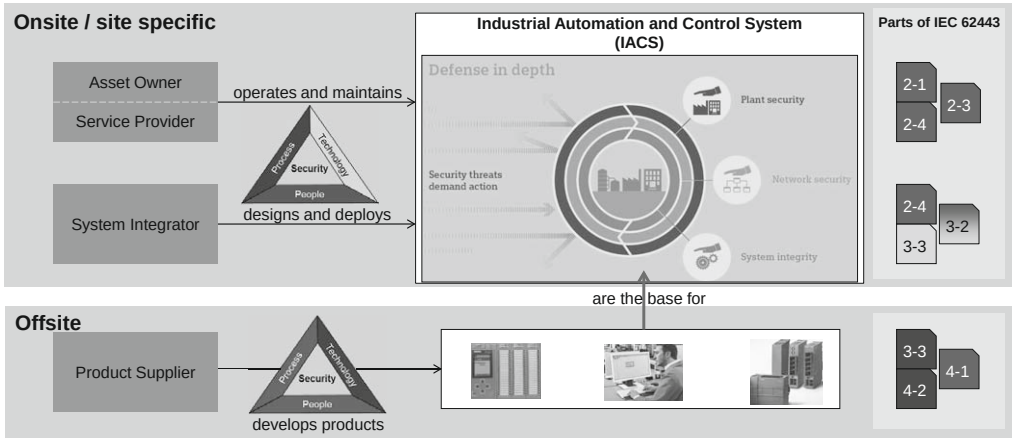

Figure 4 Defense in depth involves all stakeholders.

The following example in the area of "User Management and Access Control (UMAC)" illustrates that each stakeholder has to contribute to a defense in depth concept in particular by avoiding creating new weaknesses. For example, many products on the market still have hard-coded passwords. If someone can successfully extract and analyze the firmware of such products, he will easily find such hard-coded passwords. Many tools for this purpose can be obtained at no cost 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. This weakness encompasses all possibilities for misusing the product by a potential attacker. The product supplier can avoid these weaknesses by programming according to stringent secure coding rules. Configuring the products by changing the factory settings – in particular, changing the default passwords – is the responsibility of the system integrator. For the design and deployment of the automation solution developers commonly set temporary accounts which are protected by simple passwords. 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 operational phase. One can imagine what can happen if these accounts are misused. System integrators should follow policies and procedures which ask for actively closing these potential weaknesses. Finally, the asset owner, in its responsibility as operator of the automation solution, has to assign the names of personnel to their respective roles. The asset owner has to regularly maintain the list of active accounts of authorized personnel. As the operating 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 of essential importance to de-activate that administrator's account. If that person intended to harm the company and their account were still active, it would be very difficult to defend against a possible attack. Another duty of the asset owner is to make sure that passwords are treated confidentially and that they are regularly renewed. This should be documented in the policies and procedures, and their proactive implementation by the assigned personnel should be controlled.

All the measures described in the example are equally important to achieve a given protection regarding access control. A single non-implemented measure can weaken the protection chain and thereby define the strength of the whole chain. A holistic protection solution requires taking care to implement all measures since potential attackers frequently search for the weakest link to define their attack vector.

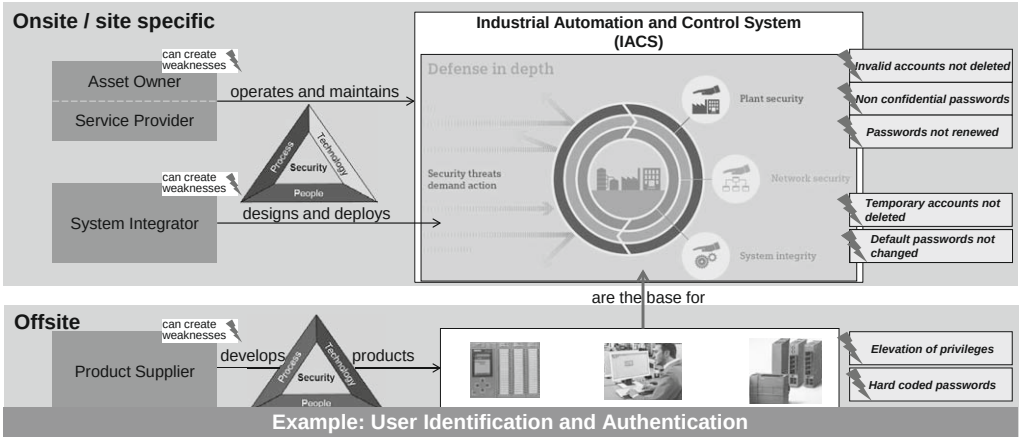

Figure 5 Each stakeholder can create weaknesses; the weakest link defines the strength of the chain.

4.2 Risk assessment according to VDI/VDE 2182

IEC 62443 is fundamentally based on a risk based approach to analyze threat scenarios and their impact on the system under consideration. The scope of such risk assessments is different for each stakeholder. The product supplier focuses on its products in their intended use; the scope of the system integrator is the automation solution; and the asset owner evaluates the impact of a misuse or a failure of its production on its business.