Comparison Of Functional And Information Security Requirements For Critical Facilities

Livshitz Ilya
ITMO University, IT-Security faculty, Russia

+7 (921) 934-48-46
Livshitz.il@yandex.ru

1. Introduction

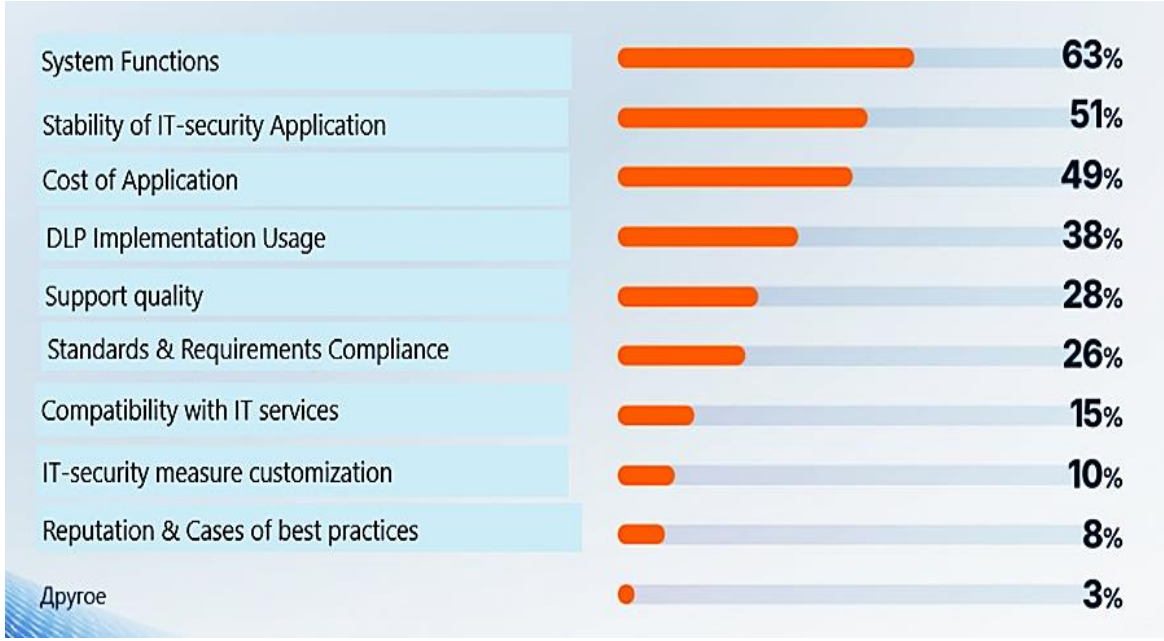
- **IEC standards (and their equivalents in the GOST R system) of the 61508** series are known, which use the concepts of failure flow (dangerous and non-dangerous), safety architecture, and risk assessments. For each assessment object, the safety integrity level (SIL) is calculated, which has 4 precise discrete values and is characterized by a measurable indicator that measures the reduction of risks to an acceptable (specified) level.
- **IEC standards (and their equivalents in the GOST R system) of the 62443** series are also known, which use the concept of functional requirements (FR). There are a total of 7 FRs, and each FR has 4 security levels (SLs).
- These two standards systems do not provide complete clarity on the methods for assessing the cybersecurity level of CII objects, as they were historically developed for different aspects: risk assessment and cybersecurity management (IEC 61508) and the listing of recommended cybersecurity measures (antivirus software, firewalls, intrusion prevention systems, etc.) in IEC 62443.

2. Statement of the task

The role of standards in assessing the level of security of ICS components for CII is small.



Reason for increasing the IT-security budget



Criteria for selecting countermeasures

2. Statement of the task. Collision

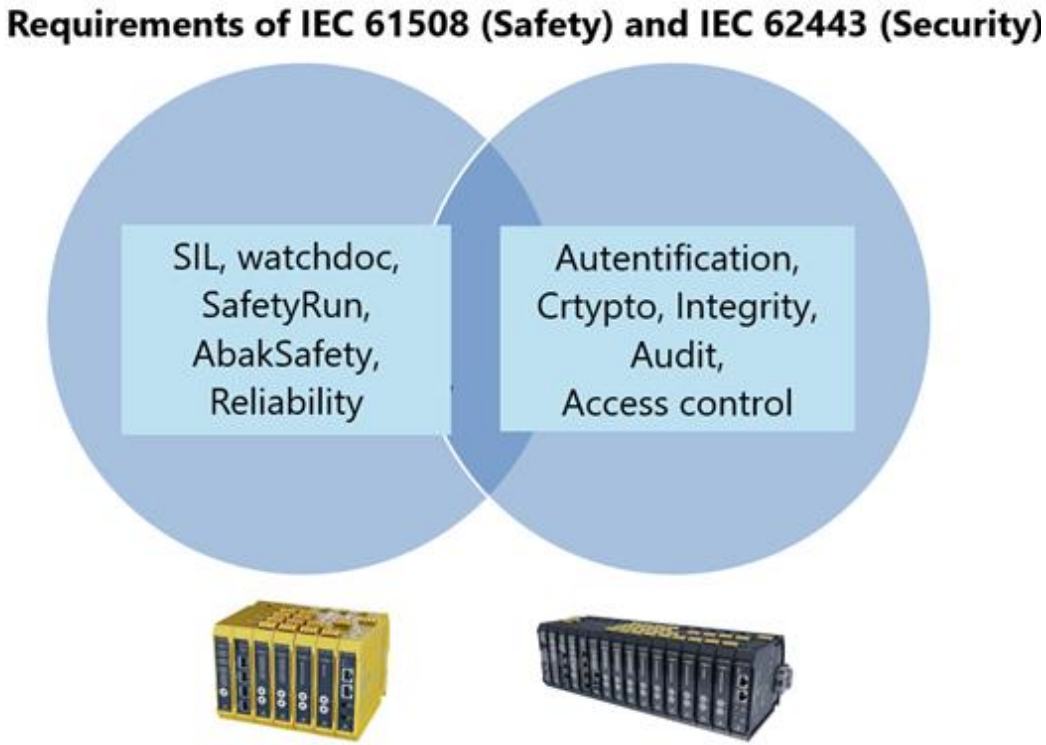
Such a collision is an important objective criterion that gives grounds to make the following judgment – customers of ICS components **“shift”** the concern for the selection and assessment of compliance with the requirements of standards to manufacturers, often without understanding the specifics of the SIL calculation methods, for example, dangerous or safety failure or specified architecture (ex-ample of IEC 61508).

Consequently, the **level of expertise is transferred** to the manufacturer, who performs all stages of the life cycle (design, development, testing, etc.) and provides certification in independent laboratories for the appropriate level of HAZOP (for example, SIL 2 for ABB PLCs and SIL 3 for R500S PLCs).

3. Applicability of "imposed" protection measures

Example of a thoughtful analysis of the **interface** of the IEC 61508 and 62443 standards under consideration/

The practical solutions proposed in the field of ICS and the methods used to create them **do not provide** a unified method for assessing compliance with the requirements of the Federal and Information Security Laws.



4. Comparison of the requirements of IEC series 61508 and 62443

When determining the functional safety requirements, it is possible to solve both the "**forward**" problem, which involves determining the final SIL of the entire system based on the known initial data of the components (e.g., MTBF, λd, λs, etc), and the "**reverse**" problem, which involves determining the reliability requirements of all components based on the specified SIL.

It is extremely important to note that the methodology underlying IEC 61508 series aims to achieve a safe state as a **level of acceptable risk**, rather than an **abstract formal compliance** with regulatory requirements. Moreover, IEC 61508-7 clearly establishes the developer's responsibility to perform the designed system through the most severe conditions, such as:

- p. B.6.9 **Worst-case testing**;
- p. B.6.10 **Fault injection tests**;
- p. C.2.10.1 In-service testing requires **690,000 operational passes** (per year);
- p. C.5.21 Critical load testing (**stress testing**).

4. Comparison of the requirements of IEC series 61508 and 62443

Accordingly, the IEC 62443 series standards are designed to ensure the security of ICS. The proposed methodological framework requires first taking into account the risks, then preparing an **economic justification**, and only then recommending the selection of protection measures:

- p. A.2.2.3 The expected cost of technical countermeasures **must be confirmed** in the economic justification;
- p. A.3.2.2.3.1 Risk management includes the processes of identifying, reducing, and **residual risks**;
- p. A.3.4.2.2 Building a **risk management system** and documenting information on countermeasures and residual risks;
- A 3.4.3.5 The **system is tested in all possible states** to ensure that each safety condition is met and the residual risk is known.

5. Comparison of IEC series 62443 and IEC series 61508

Comparison criteria	The system of requirements IEC series 62443	The system of requirements IEC series 61508
Destination area	Information security	Functional safety
Defines	7 FR and 4 SL	4 discrete SIL
Key advantages	— defines requirements for architecture, vulnerability management, monitoring, and incident response; — allows to build layered protection and manage risks.	— methods for analyzing and calculating the probability of dangerous (non- dangerous) failures have been introduced; — requirements for the system architecture have been defined; — requirements for the life cycle, verification, and validation have been introduced.
Advantages for joint use	— **Risk assessment** (qualitative and/or quantitative); — Consideration of external factors (infrastructure limitations); — Creation of a layered protection from trusted components; — Management of the system life cycle phases; — **Modeling of dangerous situations** (requirements of the worst-case conditions); — **Independent certification in accredited laboratories**; — **Formation of economic assessments of the impact on business continuity**.	

6. Conceptual formula for the final assessment of the safety

$$CII_{Int} = W_{funct} \cdot \left(\frac{\sum_{i=1}^{n} w_i^{SIL} \cdot X_i^{SIL} \cdot \alpha_i}{X_{SIL}} \right) + W_{cyber} \cdot \left(\frac{\sum_{j=1}^{m} w_j^{SL} \cdot X_j^{SL} \cdot \beta_j}{X_{SL}} \right)$$

CII_{int} – the security index of the CII, taking into account 2 components (SIL and SL);
W_{func} – the weighting factor for whole functional component (SIL) for CII;
W_{cyber} – the weighting factor for whole cybersecurity component (SL) for CII;
w_i^{SIL} – the weighting factor of the *i*-functional countermeasure at a given SIL;
w_j^{SL} – the weighting factor of the *j*-cybersecurity countermeasure at a given SL;
X_i^{SIL} – the RRF (in accordance IEC 61508) of the *i*-functional countermeasure at a given SIL;
X_j^{SL} – the RRF (in accordance IEC 62443) of the *j*-cybersecurity countermeasure at a given SL;
i (1, n) – the *i*-functional countermeasure at a given SIL;
j (1, m) – the *j*-cybersecurity countermeasure at a given SL.
X_{SIL} – the risk reduction factor (RRF in accordance IEC 61508), is derived from SIL: $RRF_{SIL1} = 10^2$ – $RRF_{SIL4} = 10^5$
X_{SL} – the risk reduction factor (RRF in accordance IEC 62443), is derived from SL: $RRF_{SL1} = 10^1$ – $RRF_{SL4} = 10^4$
α_i — the effectiveness coefficient for implementing the *i*-countermeasure (according to IEC 61508);
β_j — the effectiveness coefficient for implementing the *j*-countermeasure (requirements from IEC 62443).

6. Conceptual formula for the final assessment of the safety

Let us consider a compact numerical calculation of the generalized **CII_{int}** based on the specified input data.
The results are presented below:

$$\mathrm{CII_{Int}} = 0{,}4 \cdot \left(\frac{10^4 \cdot 0{,}4 \cdot 0{,}9 + 10^4 \cdot 0{,}6 \cdot 0{,}95}{10^4}\right) + \ 0{,}6 \cdot \left(\frac{10^2 \cdot 0{,}3 \cdot 0{,}85 + 10^2 \cdot 0{,}3 \cdot 0{,}9 + 10^2 \cdot 0{,}4 \cdot 0{,}95}{10^2}\right) = 0{,}372 + 0{,}543 = 0{,}915$$

Accordingly, using the proposed conceptual formula, we find that the **CII_{int} is equal to 0,915**, which does not fully correspond to the level of complete compliance with all IEC standards of the 61508 and 62443 series, but is at a fairly high level.

7. Conclusion

The presented publication analyzes the requirements established in the IEC 61508 and 62443 standards and applied to the numerical evaluation of the components of ICS for CII.

The main result of the work is the unification of the requirements of two different approaches: functional and information security – and the objective comparison of these requirements with the capabilities of the “overlay” protection measures proposed to ensure the security of CII in the Russian Federation.

Developers and experts in the processes of design, development, testing, and audit of critical infrastructure facilities can apply the obtained results.

Comparison Of Functional And Information Security Requirements For Critical Facilities

Thank you!

Livshitz Ilya
ITMO University, IT-Security faculty, Russia

+7 (921) 934-48-46
Livshitz.il@yandex.ru