Proceedings of the 33rd European Safety and Reliability Conference (ESREL 2023)
Edited by Mário P. Brito, Terje Aven, Piero Baraldi, Marko Čepin and Enrico Zio
©2023 ESREL2023 Organizers. *Published by* Research Publishing, Singapore.
doi: 10.3850/978-981-18-8071-1_P138-cd

Requirements Analysis Tool to Identify CERT and IDS Services for the Energy Industry

Asiye Öztürk

Clavis Institute for Information Security of the Niederrhein University of Applied Sciences and University of Wuppertal, Germany, Asiye.Oeztuerk@hs-niederrhein.de

The Intrusion Detection System- Weighted Sum Model (IDS-WSM) is a sub-module of the CERT- Requirements Metamodel (CR2M). The CR2M is a modular and incremental requirements analysis tool for energy industry stakeholders. The CRM2 addresses the specific needs and requirements analysis of distribution system operators to design targeted integrative security processes. It uses its methodology to identify the specific requirements of distribution system operators for an OT CERT solution and intrusion detection system (IDS) services. On the basis of technical and organization-specific characteristics, strategic decision-makers are provided with different solution approaches as a basis for decision support. The IDS-WSM includes a dedicated utility analysis, which can be used to examine and select possible IDS solutions on the basis of an evaluation matrix. The IDS-WSM represents the result of empirical and industrial research, which can be used as a decision support tool for the purpose of fulfilling legal requirements regarding the IT security law 2.0 for the use of systems for attack detection. In the following paper, the results of the use of the decision support tool are presented. The IDS-WSM tool was tested at a DSO by four experts from different divisions. The goal was to select the most suitable tool for the company according to the individual user's expertise.

Keywords: Critical Infrastructure, Energy Industry, Information Security, Intrusion, Detection

1. Introduction

With the increase in digitalization and automation in the energy industry, numerous technical supply processes and procedures are being successively modified. The technical field of action can be characterized by the term “system” or “network”. This predominantly includes electrical engineering, information technology and automated functions and components that are used in the central network control centers and in the decentralized network interconnection points, transformer stations and substations. For distribution system operators (DSOs), these technical units are used as part of network operation and management. Due to the depth of digitization and automation in the value chains of the DSOs, the dependency on information and communications technology (ICT) is increasing at the same time, and with it the fragility. It can therefore be postulated that the maintenance of fault-free security of supply in the energy industry is largely dependent on resilient ICT. To increase the resilience of the IT systems of critical infrastructures, including those of DSOs, the German government enacted the first IT Security Act (IT-SA) in July 2015. As an article law, it draws on existing legislation, including the Federal Office for Information Security Act (BSI Act) and the Energy Industry Act (EIA), to define binding requirements for ensuring and maintaining the information security of critical infrastructures. The legal declarations for DSOs are described in § 8a of the Federal Office for Information Security Act (BSI Act) and § 11 para. 1a of the Energy Industry Act (EIA). Federal Network Agency (2015) In detail, DSOs must recognize the following primary requirements:

- Implementation and certification of an Information Security Management System (ISMS) based on the international series of standards ISO/IEC 27001, ISO/IEC 27002 and ISO/IEC 27019,
- Creation of a homogenized network structure plan

- Establishment of a point of contact and a contact person as a single point of contact (SPOC) for the written reporting of information security incidents or IT incidents to the Federal Office for Information Security and the Federal Network Agency.

Other requirements include the holistic approaches defined in ISO/IEC 27001 and ISO/IEC 27019. The focus of this consideration is on Controls A.16.1.1 to A.16.1.7 in the areas of incident response management and disaster recovery management as well as evidence preservation. ISO/IEC (2017)
The DSO is required to establish the technical and organizational measures used for detection, correction and response measures to maintain the operational capability of IT systems. In principle, differentiated internal and external technical and organizational early detection systems and instances must be used to identify existing vulnerabilities or system anomalies at an early stage and eliminate them before they are misused. External monitoring systems and instances include Computer Emergency Response Team units (CERT units) that make notifications of potential vulnerabilities. In addition, systems deployed in the network, such as Security Information Event Management, Intrusion Detection/Prevention Systems, anti-spam and anti-virus software, and log and event review software. Koza (2022)

The IT-SA 2.0 in 2021 defined the use of intrusion detection systems as a further core requirement for operators of critical infrastructures. Bgbl (2021) However, this modification presents a complex challenge for many DSOs. As a rule, the design, support, maintenance and administration of process networks, including Supervisory Control and Data Acquisition systems, are outsourced to external service providers or system manufacturers. In addition, a large number of IP-capable field components such as programmable logic controller components are used, most of which are still maintained remotely by the manufacturers via VPN interfaces. This creates a certain complexity and heterogeneity in the operational technology (OT) landscape of the DSOs. However, this process outsourcing can be linked to the personnel and technical deficits of the DSOs.
For example, not all DSOs have enough employees with a sound knowledge of information technology in the OT area to be able to adequately meet the requirements of IT-SA 2.0 with regard to the integration and operation of intrusion detection systems (IDS). The article is structured as follows:

After a short introduction, chapter 2 presents the different attack detection methods. Chapter 3 deals with the actual research project between academia and industry that this thesis is based on. In chapter 4 and 5 the artifact of this thesis is presented first conceptually then operationally. The Weighted Sum Model. The thesis concludes with a brief consolidation and outlook.

2. Attack Detection Methods

An IDS supports event detection, evaluation, escalation and documentation of events. It is an attack detection system.
IDS usually consist of network sensors, which monitor the network traffic at a specific point and host sensors that monitor applications or the operating system. Furthermore of database components, management station and evaluation station (analysing events and reporting) Federal Office for Information Security (n. d.)

Basically, there are three ways in which an IDS can detect attacks.

1. detection of attack patterns,
2. anomaly detection
3. correlation of event data.

2.1 Detection of Attack Patterns

Signature-based IDS, attack detection is performed according to defined attack patterns. The IDS sends an alert as soon as a pattern is detected. Some IDSs also offer the option of adapting these attack signatures or formulating new ones.

2.2 Anomaly Detection

Anomaly analysis is the process of detecting deviations from the normal state of a system and reporting them accordingly.
In addition to protocol analysis, anomaly detection offers detection based on statistical data, artificial intelligence as well as honeypots.

2.3. Correlation of Event Data

When multiple, not simultaneous events or events from different sensors are detected by the evaluation logic, the correlation is described. This may be associated with anomaly detection or signature analysis.

In industry, correlation is made more difficult because, on the one hand, unsuitable database systems are used to back up events and, on the other hand, standards are lacking, so many manufacturers do not offer this functionality.

3. Research

In a university and industrial research cooperation, the technical conception and, in a later course, the operationalization of an OT CERT as an SSC primarily for the DSO and secondarily for other players in the energy industry are therefore currently being strived for. In order to solve the problems arising from the practical relevance, two parallel research strands are defined. The first research strand deals with the conceptual design of the OT CERT unit from the perspective of the service provider, i.e. the OT CERT. The dedicated research areas for this are the design-oriented processes for the technical connection of the DSO, the portfolio setup, the elaboration of a scalable and hierarchical overall concept for the OT CERT operation, the onboarding process, and the instantiation of the processes for vulnerability analysis (descriptive, diagnostic, predictive and prescriptive analytics). The second research strand focuses on the specific needs and requirements analysis of the DSO to design targeted integrative security processes of IDS. Specifically, the following descriptive research question is defined here: “How can DSOs specific requirements for an IDS solution be captured using an appropriate and universal requirements analysis tool?” The answer to this question is essential because many DSOs have already been required by IT-SA 2.0 to deploy IDS from May 2023, taking into account the timeliness of the detection patterns used. Koza and Öztürk (2022)

Due to the necessity of the mandatory declaration of the IT-SA 2.0, this paper addresses the second research question and tries to identify the most important key issues and criteria through the conceptualization of a weighted sum model (WSM), which can be used as a decision-making basis for the evaluation and categorization of the existing IDS solutions in order to be able to determine a sustainable and DSO-specific solution from the existing IDS portfolios.

Guiding principles for this work are:

- Which holistic criteria play an important role in the selection process?
- What requirements do individual operators have of the products (technical, organizational, general)?
- Which of the products on the market are suitable?
- How is the product integration carried out? (Consulting |Integration |Training |Support during integration and afterwards | Project management)

4. Weighted Sum Model

The WSM model contains a total of three modules, whereby only the first two modules (Module 1 and Module 2) are used for assessment. Koza and Öztürk (2022)

The first module, “global requirements (G),” is defined for recording and capturing global technical and organizational requirements and contains a total of three subcategories:

G: Global requirements with a total of $\sum$ 58 requirements.

Table 1. Module 1

G-ID	Description
G1	Compliance and contract management requirement
G2	Requirement for knowledge management
G3	Technical requirements for functions and interface programming

The first module of the WSM covers the integration of the main global requirements. Within the first module, the general requirements are defined, which are addressed as overarching requirements for all IDS solutions, regardless of type and technical depth. These requirements thus represent the common technical, organizational, and legal intersection that must be met by IDS solution providers regardless of the dedicated IDS solution.

By separating the higher-level and specific criteria, the global requirements can be defined more efficiently and, as a result, can be better evaluated. Koza and Öztürk (2022)

The second module "Service requirements (D)" is used to record and capture the individual technical requirements for the dedicated IDS solutions and contains a total of seven subcategories:

D: Service requirements with a total of ∑ 59 requirements Koza and Öztürk (2022)

Table 2. Module 2

D-ID	Description
D1	Requirement for UI/UX
D2	Requirement on support processes
D3	Technical requirement for alerting
D4	Requirement for detection
D5	Requirements for sensor technology
D6	Requirements for Role-Based-Access- Control
D7	Technical requirements for migration and onboarding

The second module is used to record the relevant service-related criteria, which are set and evaluated individually for the service providers, particularly within the technical consideration. The second level contains a total of 7 main requirements, which in turn are specified by 59 individual criteria. Within this module, the IDS-specific main topics such as requirements for sensor technology, detection, Role-Based Access Control, requirements for correlation, multi-client capability and migration onboarding are determined and individual criteria are defined in order to be able to individually record the specific weighting of the requirements.

The third module "Results Area" is used to visualize and compare the evaluated solutions and products and contains a total of two subcategories:

Table 3. Module 3

R-ID	Description
R1	Results area
R2	Overview
R3	Placement chart

The third module presents or compares the analysed and evaluated solutions, which are quantified on the basis of the points assigned by the individual end users. Koza and Öztürk (2022)

For the initial implementation, the WSM tool contains a recommendation for coarse weighting and fine weighting, which can, however, be adapted and modified for specific companies. In the same analogy, the individual criteria can also be adapted and expanded in order to subsequently integrate individual characteristics that are not currently taken into account and to be able to include them in the evaluation. For this purpose, two results are output based on the evaluated main requirements: a) Overview-Result (overview of all analyses with the corresponding IDS solutions) and b) Placement Chart (placement table). The Overview-Result visualizes the evaluation of all analysed IDS solutions. For the purpose of adequate decision-making, the DSOs receive the Placement Chart, in which the individual IDS solutions are placed and classified in a placement table according to the point already achieved and according to the main requirements, both individually and as a whole. Koza and Öztürk (2022)

5. Operationalization of the model

Under Dashboard, the basic functions required for operationalizing the tool can be executed. Multiple WSM can be created and, as a result, the WSMs can be initialized in different decentralized areas if several decentralized OT areas and sites need or want to set up their own solution. The IDS-WSM tool is available in German language.

In the research project, the WSM tool was run by four different users of a DSO, with the goal of selecting the appropriate IDS tool based on their expertise.

At the time of the assessment, there were four IDS products to choose from, which were evaluated by the users with regard to the criteria in the three modules (see Tables 1-3).

Fig. 1. IDS-WSM Dashboard

Table 4. Legend to Figure 1

NWA	WSM
Erfassungsbereich	Coverage
Überarbeitungsbereich	Revision Area
NWA auswählen	Select WSM
NWA löschen	Delete WSM
Analysebereich	Analysis area

If a WSM is created, the analysis of the first module can be executed. Within the first module, the general technical and organizational requirements are defined, which are the overriding requirements for IDS solutions.

These requirements thus represent the common technical, organizational, and process intersection that must be met by individual IDS solution providers, regardless of the dedicated IDS solution. By separating the higher-level and specific criteria, the general requirements can be defined more efficiently and consequently evaluated more efficiently. The following figure illustrates partial extracts of the first module.

Regarding the weighting of the first module, it can be assumed that the defined criteria will be given a higher priority, since this involves the fundamental aspects of A. 15 "Supplier relationship" of ISO/IEC 27001:2013 and, as a result, many regulatory, security-related, and legal aspects must be considered. This must be evaluated in individual cases, e.g., on the part of the DSO, and adapted if necessary. However, the rough weighting of the global requirements should be between 30 and 40 percent.

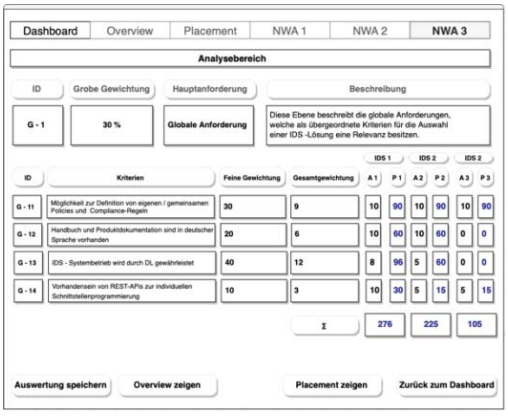

Fig. 2. IDS-WSM Analysis area

This Figure 2 shows the exemplary evaluation of the global criteria (G - 11 to G - 14). The global criteria were evaluated with a total of 30% of the total evaluation. In this example, three products were evaluated by three instances. The results represent in total for three IDS products. With 276 points, the first IDS product was found to be the most suitable. As a result of the joint weighting that has already been carried out, the individual evaluators only must state their opinion on the degree of fulfillment of the individual evaluation areas. Thus, the attempt of an intersubjectivity is undertaken, to be able to represent the individual results of the block evaluations as well as the total result for all involved ones comprehensibly.

The following figures show the individual results for better transparency and consequently can be used as a basis for discussion. Here the evaluators have the possibility to compare not only the overall result but also the person-dependent evaluations (see Figure 3), product-dependent evaluations (see Figure 4) and person- and topic-dependent evaluations in combination (see Figure 5) and to compare them with each other in detail.

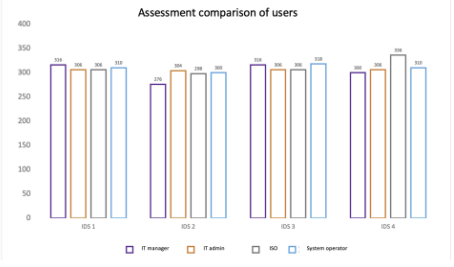

Fig. 3. Assessment overview

Figure 4 below depicts the different ratings per IDS product.

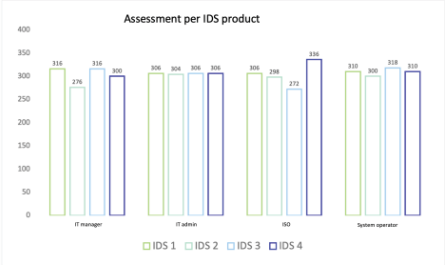

Fig. 4. Assessment per IDS product

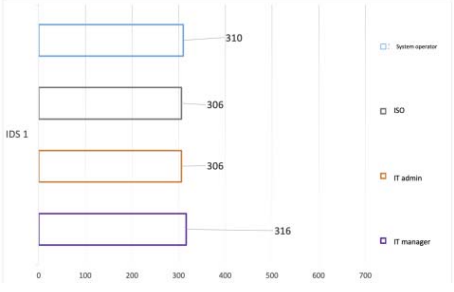

Fig. 5. Placement chart - end selection

To enable efficient deployment of the WSM, the following procedure should be followed (see Figure 6). Within the conceptualization phase, the basic characteristics will first be defined, such as whether IDS solution should be integrated as a pure appliance solution into the technical-organizational infrastructure. As an output of this phase, a rough concept will be created by defining the objectives, responsibilities, preliminary considerations and a rough timeline, which in turn will be shared and harmonized with the project stakeholders for the purpose of transparent communication. In a second step, an initial requirements analysis is to be carried out with the participation of several business users, including management and the information security officer in which, depending on the objectives defined in the rough concept, the requirements are identified that will be embedded in the WSM as decision criteria in a later process. After the integration of the WSM, this is to be synchronized with the procurement department technically and added if necessary modifications, which could not be considered on the part of the technical users within the WSM. The designed WSM tool starts exactly at this point and can also be individually adapted and specified in individual DSO-relevant areas. The WSM tool thus forms a basis for decision-making, which is designed on the basis of specific requirements and their weighting. Consequently, in the next step, the IDS solutions on the market must be embedded in the evaluation methodology of the WSM and evaluated accordingly by the business users.

In the initial evaluation, monetary considerations should first be disregarded. This process therefore examines whether the IDS solutions available on the market meet the defined requirements.

In a later process, the evaluated IDS solutions are compared. Monetary ratios are also used in this comparison. This is initially intended to ensure that monetary ratios do not represent the dominant decision criterion, but rather are taken into account and embedded alongside the technical decision criteria in the sense of an economic decision-making process. Based on the results obtained from the WSM, the IDS solution to be implemented can be selected.

In the integration phase, the migration and integration of the selected IDS solution should take place. Here, it is important that a successive integration (no big bang integration) and embedding takes place from the inside out. Both technical (rollout, configuration, testing, commissioning) and organizational core aspects, such as the requirements for the organizational structure and process organization of an incident response management team, must be considered.

6. Conclusion

A relevant implementation of an IDS solution can only be effective and lead to the desired results if the organizational aspects for the response with the associated personnel, escalation levels, communication links, etc. are also defined. An IDS solution identifies events and incidents, which in turn must be answered with a response. If the response fails to materialize at this point, even the best IDS solution is of no use. A corresponding procedure for defining and designing adequate incident response management is defined in ISO/IEC 27035-1, 2 and 3 and in NIST SP 800-61. NIST (2008) The

integration phase is followed by the operational phase, in which all relevant core elements must be recorded in the associated manuals and training documents. After the IDS solution has been put into operation, the correctness of the IDS solution as well as its expansion and updating are now checked at regular intervals through the use of continuous processes. Koza and Öztürk (2022)

The tool is compatible with the requirements of the new ISO 27001:2022 after a review. The IDS-WSM will be aligned with the requirements of the Network and Information Security (NIS) Directive 2.0 in the next step.

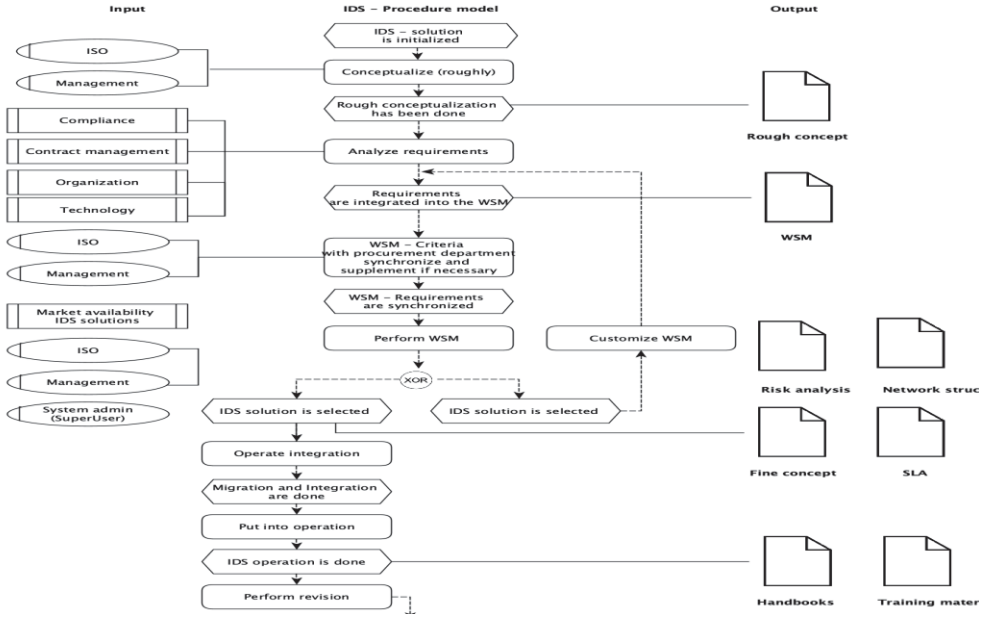

Fig. 6. Procedure model of the IDS-WSM

References

Bgbl (2021), "Second Act to increase the security of information technology systems". Accessed: March 12, 2023. [Online]. https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl121s1122.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl121s1122.pdf%27%5D__1680099117369

Federal Office for Information Security (n. D.), "Federal Office for Information Security Guideline for the Introduction of Intrusion Detection Systems". Accessed: February 21, 2023. [Online]. https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Studien/IDS02/gr1_htm.html

Federal Network Agency, (2015). "IT Security Catalog Pursuant to Section 11 Paragraph 1a of the Energy Industry Act" Accessed: March 29, 2023.[Online]. https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Energie/Unternehmen_Institutionen/Versorgungssicherheit/IT_Sicherheit/IT_Sicherheitskatalog_08-2015.pdf?__blob=publicationFile&v=1.

ISO/IEC 27001:2017-06 (2017), "Information technology- Security techniques- Information security management systems- Requirements," Beuth Verlag, Berlin, Germany, pp. 1-35.

Koza, E. (2022): "OODA Loop as a Decision Support Model to Continuous and Dynamic Vulnerability Management and Incident Response Management of Critical Infrastructures," Proceedings of the 32nd European Safety and Reliability Conference Edited by Maria Chiara Leva, Edoardo Patelli, Luca Podofillini, and Simon Wilson Copyright ©2022 by ESREL2022.

Koza, E., Öztürk A. (2022): "Entwicklung eines adaptiven Anforderungsanalyse-Tools zur bedarfsgerechten Ermittlung von CERT und IDS-Dienstleistungen für die Akteure in der Energiewirtschaft," in book: Cyber-Sicherheit ist Chefinnen und Chefsache! - Tagungsband zum 18. Deutschen IT-Sicherheitskongress. Publisher: Bundesamt für Sicherheit in der Informationstechnik (Hg.), SecuMedia-Verlag Gau-Algesheim 2022.

NIST (2008), "Computer Security Incident Handling Guide," U.S. Department of Commerce, Washington, D.C., Federal Information Security Management Act (FISMA), Special Publication 800-61.