engineering proceedings

MDPI

Proceeding Paper

Constructive Approach to the Design of Data Protection Systems: Models and Transformation †

Ivan Gaidarski * and Anastas Madzharov

Unmanned Robotics Systems Laboratory, Institute of Robotics, Bulgarian Academy of Sciences, 1113 Sofia, Bulgaria; a.madzharov@ir.bas.bg

* Correspondence: ivangaidarski@ir.bas.bg

† Presented at the 15th International Scientific Conference TechSys 2026—Engineering, Technologies and Systems, Plovdiv, Bulgaria, 14–16 May 2026.

Abstract

In this article, we present a constructive method for designing an information security system (ISS). The method is based on the IEEE 1471 and IEEE 42010 standards. They provide an architectural framework for describing the system through conceptual modeling from different perspectives. The perspectives reflect the requirements of stakeholders—regulatory, normative, technological or budgetary. As result of analysis of the problem area, conceptual models are constructed. The resulting models are combined into a generalized multilayer model. The transformation of the conceptual model into a technology-independent object-oriented (OO) design model follows. The next stage is selection of an appropriate technological platform and subsequent transformation of the design model into an implementation model. An essential part of the method is the creation of an agent-based simulation model. It allows the simulation of the ISS in different environments, changing the input conditions. The method ensures technological independence of the ISS, due to the fact that the resulting conceptual model reflects the requirements of the system and the methods for implementing the tasks of the ISS without using a specific technological solution. The method also ensures universal communication between the individual stakeholders and unification of the used terminology.

Keywords: data security; data protection; system; conceptual; models; transformation; constructive

1. Introduction

Information technology is shaping more and more aspects of modern life. It determines the way we communicate, learn, work, shop and have fun. Ensuring information security (IS) is becoming a vital factor in our daily lives. Modern healthcare, transportation, educational institutions, factories and organizations of all types and sizes depend on the effective implementation of information security. This is especially true for critical infrastructure facilities that provide electricity, water, telecommunications and transportation. They are completely dependent on information technology and, above all, on ensuring their safety.

Information security is the process of protecting assets—information, hardware, software or processes. For this process to be effective, it is necessary to consider each asset in the context of the risk of loss associated with it and its value. To assess what to protect, it is first necessary to determine which assets are valuable and to whom [1,2].

One of the main objectives of IS is to protect information in all its forms. In the context of organizations, these are intellectual property, patents, production technologies and good

Academic Editors: Nikola G. Shakev, Valyo N. Nikolov, Nikolay R. Kakanakov and Sevil A. Ahmed-Shieva

Published: 22 July 2026

practices, know-how, databases with suppliers and customers. This information is vital for the modern organization and forms its competitive advantage over other organizations. For this reason, the protection of information in all its forms—electronic and physical—is of paramount importance. It is necessary for information assets to be reliably protected from external factors such as hackers or natural disasters, but also from internal factors. Examples of internal factors are partners, suppliers and employees of the organization, both current and former. They have the right to access the organization's resources, which makes them a risk factor. The development of technologies determines new ways of communication, data storage, protocols and operating systems. This determines the emergence of new vulnerabilities, opening up to new threats and the carrying out of successful attacks.

The most critical threats to the modern organization are related to the threat to information systems, communication networks and data. A particularly topical problem is the protection against unregulated leakage of information, leading to a threat to the very existence of the organization. Effective information protection requires the implementation of a strategy that is fundamentally different from traditional protection against external threats [3,4]. For modern information protection, periodic research, study, systematization and development of new protective procedures, techniques, mechanisms and solutions are of vital importance.

In this article, we consider a method for implementing an ISS through a constructive approach to designing an information security system for the purpose of data protection. An example of designing a data leak protection system using a data leak prevention platform is considered. The author's method is used, based on taking into account different points of view on the requirements of the system and its functionality, by constructing appropriate models and their transformation.

2. Constructive Approach to the Design of ISS

Traditionally, the protection of assets in the organization is carried out on the principle of patching the incidents that have occurred. When an incident occurs, related to data loss—either from equipment failure, a successful external attack or loss of information—appropriate new protection measures are applied. The information protection thus obtained over time is incident-based and is characterized by the use of significant resources—technical, human, time and financial. It is based on the principle of accumulating protective measures, as a result of incidents or new requirements for the organization's work, without assessing the effectiveness of these measures.

These shortcomings can be avoided by implementing an information security system specifically designed for the needs of the organization. The requirements for such an ISS are as follows:

1. Accurate reporting and formulation of the initial requirements for the system.
2. Potential for easy addition of new requirements to the ISS.
3. Options of expanding the ISS by adding new functionality when the requirements for the system change.
4. Technological independence of the ISS. It is ensured by the next two requirements (5 and 6).
5. Selection of a modern technological basis for the implementation of specific protective measures.
6. Options of changing the technological basis of the SIS in order to modernize and update the technologies used.
7. Potential for scaling the ISS in connection with the growth of the organization itself.
8. Possibility of optimizing the resources used.

The constructive approach proposed by the authors, in contrast to the above-mentioned mechanical accumulation of protective measures, is based on the effective use

of organizational resources—technological, time, financial and, last but not least, human. The proposed method consists of several stages:

1. Clarification of the initial requirements for the system and their formalization for more convenient implementation.
2. Performing a risk analysis for optimization of both the protected assets and organizational resources.
3. Designing an appropriate system architecture capable of fulfilling the requirements for the ISS.
4. Constructing the necessary models.
5. Selecting an appropriate technological platform for implementing specific protective measures.
6. Simulating the system's operation for optimization purposes.
7. Final implementation through the selection of specific platforms and protective measures to achieve the set goals.

The method is based on the capabilities of the IEEE 1471 [5–7] and IEEE 42010 [5,7,8] standards for describing system architecture. The two standards provide a framework for describing architecture through conceptual modeling methods based on different stakeholder perspectives. These perspectives may include regulatory requirements, along with the requirements of various participants in the design and implementation process of the system—management, researchers, technologists, engineers, marketers, customers, etc.

Based on the analysis of the problem area, conceptual models of the problem area are constructed, based on different perspectives. The resulting models are combined into a generalized multilayered conceptual model.

The method ensures technological independence of the ISS, due to the fact that the resulting model reflects the requirements of the system and the methods for implementing the tasks facing the ISS through conceptualization, without using a specific technological solution. This is followed by a transformation of the conceptual multilayer model and the resulting object-oriented design model, which is also technologically independent. This is followed by the selection of an appropriate technological basis, providing appropriate protection measures, and the subsequent transformation of the design model into an implementation model, describing this platform and its settings.

An essential part of the method is the possibility of creating an agent-based simulation model, allowing simulation of the designed the ISS in different environmental variants, changing the input and output conditions and changing or adding requirements to the system. The described approach provides universal communication between the individual stakeholders and unification of the terminology used.

2.1. System Analysis to Formulate System Requirements

To formulate the requirements for the system, a system analysis is performed. The object of the system analysis is the problem area of the ISS and the environment of implementation of the ISS. The problem area includes the problems that must be solved by the designed system, i.e., the set of tasks facing the ISS. The implementation environment encompasses the technological and regulatory constraints within which the designed ISS must operate. It is directly dependent on the nature of the organization and its activities. They determine the requirements for the system [9–11]. On their basis, a model of the problem area is created at a later stage.

https://doi.org/10.3390/engproc2026150053

2.2. Risk Analysis

ISO 27005 [12] defines risk as the probability that a threat source will exploit a vulnerability and cause harm to the organization [13]. The risk analysis of the designed system includes the following basic elements:

- Asset analysis.
- Threat analysis.
- Impact analysis.

Asset analysis includes an analysis of known system vulnerabilities and existing protection measures. Threat analysis refers to the analysis of threats and attack mechanisms. Threats include threat agents and mechanisms. Attack mechanisms include attack vectors, attack methods, and their effectiveness. They are directly dependent on the capabilities of the threat agents and their nature. Attack analysis is expressed in terms of the probability of success of the analyzed attack methods. Impact analysis considers the value of the threatened assets and the consequences of successful attacks.

The specified basic elements serve as the basis for risk analysis through the well-known and proven approaches—ISO 31000 [14], CAPEC [15], WEF [16], ISO 15408 [17] and OWASP [18]. The main paradigm of risk analysis in information security is the impossibility of 100% protection due to the limited resources of funds, time and human capital. The most effective approach in this case is to evaluate the assets according to their value to the organization, to classify them according to this criterion. The next step is an analysis of how important the loss of the given resource is for the viability of the organization; i.e., how critical the loss of this resource is. An important stage is also the assessment of the resources necessary for the protection and possible recovery of these resources in the event of their loss. Thus, one of the most important goals in designing an ISS is to reduce the risk of losing critically important information resources.

2.3. Designing the System Architecture of ISS

The architecture of the designed ISS is based on the IEEE 1471 and IEEE 42010 standards. They provide capabilities for describing system architectures using conceptual modeling methods. IEEE 1471 provides principles and terminology for describing architectural frameworks of software-intensive systems. The standard defines the architecture of a system as a fundamental description of the organization of this system through its constituent components and their interaction with each other and with the environment. The standard focuses only on the components and their content. IEEE 42010 complements the first standard by providing architectural frameworks for describing arbitrary systems. It adds concepts such as environment and viewpoints.

The two standards provide designers with tools that allow them to focus on the main features of the designed systems and abstract away from unimportant details. They introduce concepts such as environment, framework, problems, stakeholders, perspectives, and views. Conceptual modeling methods ensure technological independence of the analysis model. Figure 1 illustrates the application of IEEE 1471 and IEEE 42010 in the design of the ISS with a defined problem domain and exemplary perspectives—information security perspective, information processing perspective, risk analysis perspective, communication perspective, and technology perspective.

https://doi.org/10.3390/engproc2026150053

Figure 1. ISS area of interest.

2.4. ISS Models

As a result of applying the described method for designing ISSs, numerous models are constructed, the result of analysis and transformations (Figure 2).

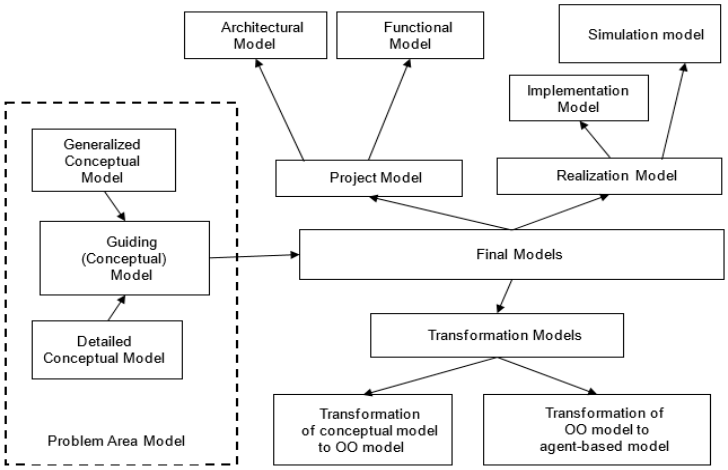

Figure 2. Models for ISS development.

The first of the created models is the problem area model. This model is the result of the analysis of the problem domain and coincides with the analysis model obtained as a result of the analysis. It represents the desired architecture of the system. The model consists of two parts—generalized model and detailed model. As a result of using different viewpoints (Figure 1), a multilayer model is constructed, uniting the obtained models.

Figure 3 shows an example of a multilayer model that combines the "information security" viewpoint and the "information processing" viewpoint.

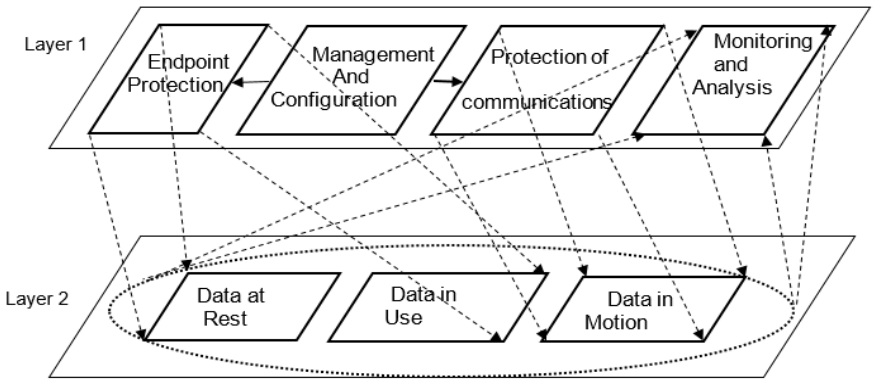

Figure 3. Multilayer conceptual model of ISS.

The models shown reflect the respective viewpoints, with the individual layers representing the respective conceptual models created by stakeholders of the given viewpoint. The arrows in the model reflect the interrelationships between the individual models and the respective protective measures that need to be taken.

After creating the multilayer model, optimization of the necessary protection measures can be performed, and on this basis, the next model can be created—project model. Based on the constructed architectural model, we can construct a model that will enable the implementation of a real ISS. The project model is based on the model-to-model transformation, implemented as a transformation of a conceptual model to an object-oriented model.

When constructing the object-oriented model, only those characteristics and properties of the system that are related to solving the specific problem are taken into account, while the rest are ignored. For this purpose, the capabilities of the object-oriented language UML are used, which allows for the description, analysis and modeling of the architecture and functionality of the ISS [19,20]. The UML tools, represented by different types of diagrams, allow the creation of an architectural model and a functional model, which together form a project model.

Figure 4 shows an example of an ISS architecture described using a UML composite structure diagram. The ISS architecture is described using a combination of other static UML diagrams, such as the class diagram, object diagram, packet diagram and component diagram.

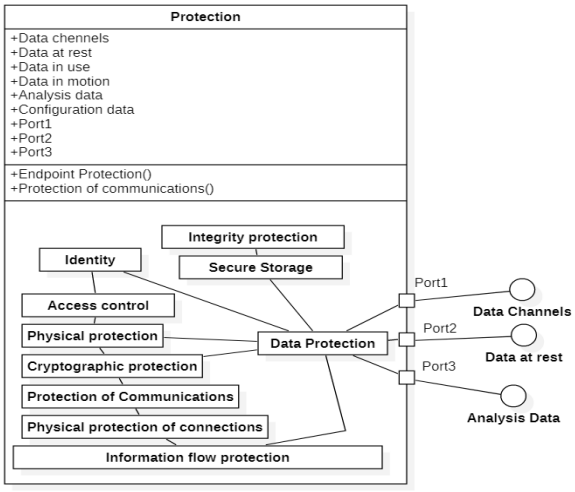

Figure 4. UML composite structure diagram of the class "protection".

The functional description of the ISS is carried out using the dynamic diagrams of UML—interaction, behavior, use case, activity and state diagrams. The behavior of each component of the ISS can be described as an interaction with other components or with the environment using interaction diagrams, and the behavior of the system is described using activity and behavior diagrams. The state of the components of the ISS is described using the state diagram.

The next step is to construct a realization model, consisting of two parts—realization model and simulation model.

The realization model describes the implementation of ISSs through a specific platform. Such a platform can be data leak prevention (DLP) to protect information from insiders, intrusion detection systems (IDSs) and intrusion prevention systems (IPSs) to protect against external factors, and many others. The realization model describes the components of the real IT security platform, its configuration and setup. The purpose of the model is to create a description of a real ISS before its final implementation in real conditions. The

model can be transformed into a simulation model, through which the system can be tested when changing external conditions without spending resources in a real implementation.

The simulation model is created by transforming the object-oriented project model into an agent-based model. By definition, an agent is an entity that has the ability to interact with the environment using sensors, has the ability to process the information obtained from the interaction and can affect the elements of the environment through executive mechanisms [21]. In the design of systems, an agent can be an independent unit, capable of autonomous actions within the environment in which it operates, this environment system, in order to perform individual tasks. Thus, a simulation model consists of multiple agents, with specific goals and algorithms, and each of the agents can be responsible for a certain characteristic of the environment—changing input parameters, interacting with users, changing the configuration of components, etc. The behavior of the agents also determines the reaction of the ISS to these parameters. This allows for a complete simulation of a potential real environment without implementing the system in real conditions. This allows for testing and optimization of the system before actual implementation.

The final model is the implementation model, which provides specific instructions to the implementation team on how to install and configure the ISS in the real world.

2.5. Practical Implementation of ISS

The described method for building the ISS architecture can be used for the practical implementation of an information security system. For this purpose, we formulate the following initial conditions:

1. We must design an ISS that ensures compatibility with the new EU GDPR regulation [22].
2. The ISS must prevent the leakage of personal data outside the protected perimeter of the organization.
3. The direction of data protection must be from the inside to the outside.
4. The system must provide protection from the actions of insiders, i.e., persons with legitimate access to the organization's resources.
5. The system must monitor for accidental leakage of information outside the organization—accidentally sent emails, lost flash drives, stolen laptops, etc.
6. The system must prevent the leakage of sensitive information.
7. The system must allow easy expansion with new functionalities when the regulatory framework changes.

When designing an ISS, the following must be defined: a method for detecting the leakage of sensitive information outside the organization, reporting the leakage, activating an alarm, documenting the violation, the consequence of which is the leakage itself, and most importantly—providing measures to prevent leakage outside the organization. To do this, the following steps must be performed:

- Defining the information sensitive to the organization.
- Defining a list of keywords used to identify sensitive information.
- Defining RegEx rules for identifying personal data, according to the rules of the EU GDPR.
- Selecting a platform through which to perform these steps and the above-mentioned initial conditions for the system.

Figure 5 shows the UML diagram that performs the identification of sensitive and personal data. For this purpose, a predefined security policy is required, including a list of keywords and RegEx rules with which the information flowing through a given data channel is compared. When the keywords or RegEx rule match, a security policy violation is reported and appropriate measures are taken to report and document the violation, prevent data leakage, and collect metadata for evidence and further investigation.

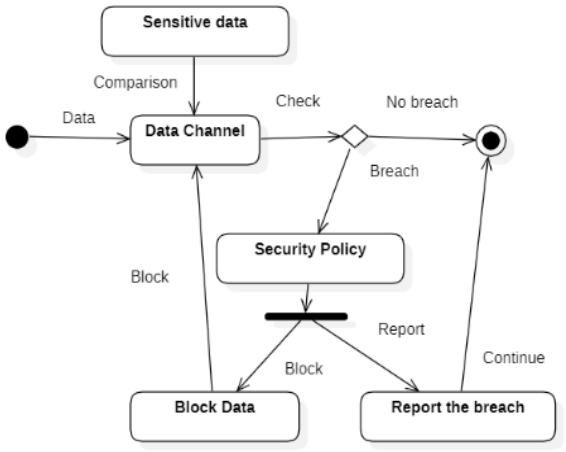

Figure 5. UML activity diagram of the endpoint protection method.

For the practical implementation of the specified ISS, a data leak prevention (DLP) platform is selected [23]. DLP platforms are capable of controlling all three types of data—data-in-motion, data-in-use and data-in-rest. Such a platform is shown in Figure 6. It consists of several modules, each of which is responsible for a specific functionality. The device control module is responsible for managing and controlling data channels—LAN, Wi-Fi, USB and Bluetooth ports. The content-aware protection module is responsible for monitoring passing data and identifying sensitive data. The eDiscovery module is used to discover sensitive data-in-rest data that is stored on hard disk drives, storage devices and shared partitions.

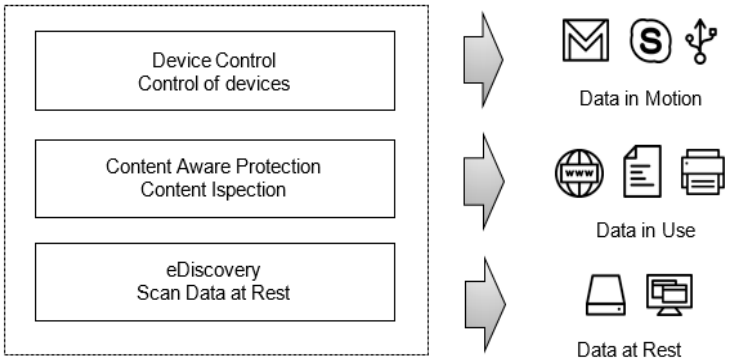

Figure 6. Data leak prevention platform.

Figure 7 shows a UML deployment diagram through which the DLP platform can be implemented in the real world.

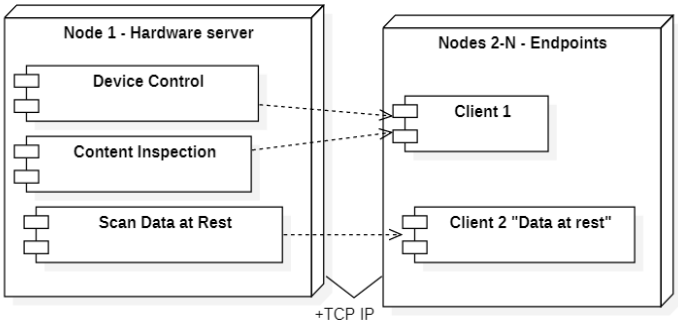

Figure 7. UML deployment diagram.

https://doi.org/10.3390/engproc2026150053

It consists of agents that are installed on protected workstations and servers and a server part. The agents control the data channels of the respective endpoint, and the server part processes the results and controls compliance with the specified security policy.

2.6. Experimental Results

The practical tests in real conditions are based on the implementation of the ISS in five organizations, under the following conditions—expanding the functionality of existing systems, through a new ISS for the protection of sensitive information based on the DLP platform. The results of the practical tests are shown in Figures 8 and 9.

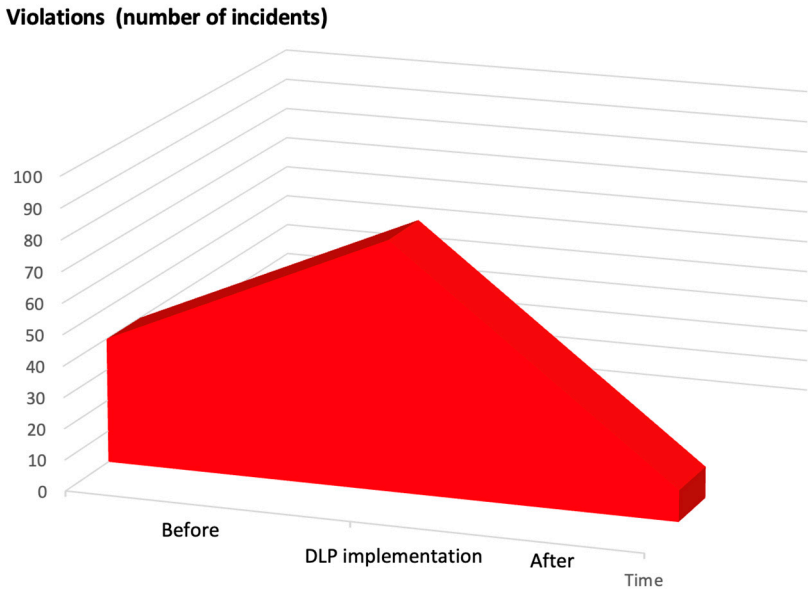

Figure 8. Registered violations of information security.

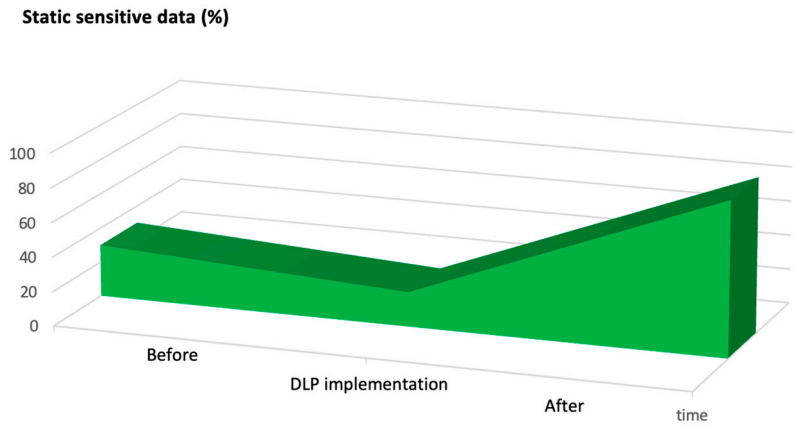

Figure 9. Discovery of sensitive data-in-rest.

Figure 8 shows the results of the implementation of the ISS with a DLP platform for detecting violations related to the leakage of sensitive data. After the implementation and exploitation of the ISS, a reduction in incidents of up to 85% was recorded.

Figure 9 shows the results of the implementation of the ISS with the DLP platform for the discovery of static sensitive data-in-rest.

This is a very important process, due to the fact that this data does not pass through the data channels and, accordingly, it is impossible to identify it. It can leak accidentally and uncontrollably when data carriers are lost or when workstations or laptops are changed.

Protection from leakage or loss of static data is possible only if it is previously identified and marked. Then, it can be moved or deleted.

The results of the implementation of a DLP-based ISS show an increase in the successful discovery of static sensitive data up to 70%.

3. Discussion and Conclusions

As a result of the application of the constructive approach, the designed ISS covers all the requirements for the system (Table 1).

Table 1. Matching requirements and method characteristics.

Requirements	Characteristics of the Method
Accurate reporting of ISS requirements	Implementation of IEEE 1471 and IEEE 42010 standards with the ability to create meta-models from different viewpoints and integrate them into a multilayer model. The viewpoints take into account the requirements of the environment and different stakeholders.
Covering different perspectives	Implementation of IEEE 1471 and IEEE 42010 standards with the ability to create meta-models from different viewpoints and integrate them into a multilayer model.
Flexibility and expandability	Flexible architecture, with the ability to add new scenarios (use cases) through OO modeling. The project model provides for adding functionality before the actual implementation of the system.
Technological independence	Using conceptual modeling that is not tied to a specific implementation environment.
Selection of a modern technological basis with the possibility of expandability and change in the technological basis of the ISS	The construction of separate models, playing the role of an intermediary between the ISS architecture (conceptual model) and the final implementation model—project model and realization model, ensures a change in the technological platform and the specific implementation environment.
Opportunities to optimize the used resources	Using an agent-oriented simulation approach that shows the dynamics of the system and its behavior when changing various input impacts and parameters.
Traceability	Model-to-model transformations (conceptual model -> OO model -> agent model), preserving the logic and goals of the system.

The presented constructive approach provides opportunities for flexible design of ISSs, taking into account the maximum volume of requirements from stakeholders and focusing on critical assets and data for the organization, platform independence and expanding the capabilities of the system as needed. The approach combines conceptual, object-oriented and agent-based modeling, ensuring technological independence in the design of ISSs. Conceptual modeling, based on different perspectives, through the IEEE 1471/42010 standards, ensures compliance with the requirements of stakeholders at all stages of design, testing and implementation.

Author Contributions: Conceptualization, I.G. and A.M.; methodology, I.G. and A.M.; software, I.G.; validation, I.G. and A.M.; formal analysis, A.M.; investigation, I.G.; resources, A.M.; data curation, I.G.; writing—original draft preparation, A.M. and I.G.; writing—review and editing, A.M.; visualization, I.G.; supervision, A.M.; project administration, A.M.; funding acquisition, A.M. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the NSP DS program, which has received funding from the Ministry of Education and Science of the Republic of Bulgaria under the grant agreement no. D01-74/19.05.2022.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Diogenes, Y.; Ozkaya, E. *Cybersecurity—Attack and Defence Strategies*; Packt Publishing Ltd.: Birmingham, UK, 2018.
2. Pfleeger, C.P.; Pfleeger, S.L.; Margulies, J. *Security in Computing*, 4th ed.; Prentice Hall: Hoboken, NJ, USA, 2015.
3. Suryateja, P.S. Threats and Vulnerabilities of Cloud Computing: A Review. *Int. J. Comput. Sci. Eng.* **2018**, *6*, 297–302. [CrossRef]
4. Rhodes-Ousley, M. *Information Security the Complete Reference*, 2nd ed.; The McGraw-Hill: Columbus, OH, USA, 2013.
5. Hilliard, R.; Emery, D.; Maier, M. ANSI/IEEE 1471 and Systems Engineering, Systems Engineering. *Syst. Eng.* **2004**, *7*, 257–270. [CrossRef]
6. *IEEE 1471*; IEEE Recommended Practice for Architectural Description of Software-Intensive Systems. IEEE: Piscataway, NJ, USA, 2000. Available online: https://standards.ieee.org/standard/1471-2000.html (accessed on 17 March 2026).
7. *ISO/IEC/IEEE 42010:2022*; Software, Systems and Enterprise—Architecture Description. ISO: Geneva, Switzerland, 2022. Available online: https://www.iso.org/standard/74393.html (accessed on 17 March 2026).
8. Mora, M.; Reyes-Delgado, P.Y.; Phillips-Wren, G.; Gómez, J.M.; Galvan-Cruz, S.; Diaz, O. A Review of Main Non-proprietary Domain-Independent Data Science Analytics AI/ML Reference Architectures—A Dual ISO/IEC/IEEE 42010 and IT Service Design Approach. ITService Design Approach. In *Engineering and Management of Data Science, Analytics, and AI/ML Projects*; Intelligent Systems Reference Library; Springer: Cham, Switzerland, 2025; Volume 282. [CrossRef]
9. Nurbojatmiko, N.; Karimiyah, M.S.K.; Asnadi, N.M.; Anisyah, R. ISO 27001 As Information Security Solution In Society 5.0 Era: Systematic Literature Review. *Sink. J. Dan Penelit. Tek. Inform.* **2025**, *9*, 484–492. [CrossRef]
10. Olivé, A. *Conceptual Modeling of Information Systems*; Springer: Berlin/Heidelberg, Germany, 2007. [CrossRef]
11. Mallikaarachchi, V. *Data Modeling for System Analysis, Information Systems Analysis—IS 6840*; University of Missouri: St. Louis, MO, USA, 2010.
12. Metin, B.; Sevim, S.B.; Wynn, M. Cybersecurity Strategy Development: Towards an Integrated Approach Based on COBIT and ISO 27000 Series Standards. *Standards* **2025**, *5*, 33. [CrossRef]
13. ENISA Threat Landscape. 2025. Available online: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025 (accessed on 17 March 2026).
14. *ISO 31000:2018*; Risk Management—Guidelines. ISO: Geneva, Switzerland, 2018. Available online: https://www.iso.org/standard/65694.html (accessed on 17 March 2026).
15. Common Attack pattern Enumeration and Classification. Available online: http://capec.mitre.org (accessed on 17 March 2026).
16. Risk and Responsibility in a Hyperconnected World—Pathways to Global Cyber Resilience. Available online: http://www3.weforum.org/docs/WEF_IT_PathwaysToGlobalCyberResilience_Report_2012.pdf (accessed on 17 March 2026).
17. *ISO/IEC 15408-1:2022*; Information Security, Cybersecurity and Privacy Protection—Evaluation Criteria for IT Security—Part 1: Introduction and General Model. ISO: Geneva, Switzerland, 2022. Available online: https://www.iso.org/standard/72891.html (accessed on 17 March 2026).
18. Open Web Application Security Project. Available online: https://www.owasp.org/ (accessed on 17 March 2026).
19. The Unified Modeling Language (UML) Web Page. Available online: https://www.uml-diagrams.org (accessed on 17 March 2026).
20. Dennis, A.; Wixom, B.; Tegarden, D. *Tegarden System Analysis & Design—An Object-Oriented Approach with UML*, 5th ed.; John Wiley & Sons: Hoboken, NJ, USA, 2015; pp. 19–52.
21. Russel, S.; Norving, P. *Artificial Intelligence: A Modern Approach*; Prentice Hall: Hoboken, NJ, USA, 1995.
22. Kosenkov, O.; Zabardast, E.; Fucci, D.; Mendez, D.; Unterkalmsteiner, M. Privacy by design: Aligning GDPR and software engineering specifications with a requirements engineering approach. *Inf. Softw. Technol.* **2025**, *190*, 107946. [CrossRef]
23. Halyna, H.; Marchenko, V.; Borsukovskyi, Y.; Dmitriiev, V.; Sofiia, T. Dlp System as A Component of Countering Insider Threats To Information Confidentiality. *Cybersecur. Educ. Sci. Tech.* **2025**, *2*, 583–592. [CrossRef]