ANALYSIS OF CYBER THREATS AND METHODS OF MITIGATION THEM AT RADIATION HAZARDOUS FACILITIES
On the example of the Modular Automated Accounting and Control System "Atomic Keeper"

YAUHEN KHAJYNAU, ANDREI SAVIN, ANDREI DRAZHZHYNAU, ALENA KARNILOVICH, DMITRY IVANOV, MAXIM MIKLAS
Applied Systems Ltd.
Minsk, Republic of Belarus
Email: zhenya.khadzhinov@appsys.net

Abstract

A system of accounting for and control of nuclear material should be one of the most secure systems at an NPP. The article describes possible threats and methods of mitigation them in the Atomic Keeper system.

Threats:
1. Misrepresentation – introducing false information about the state of nuclear fuel. The operator may report/make decisions based on such information, which could trigger an accident;
2. Destruction of data to destabilize the system;
3. Introducing false information into the system about the latest changes in nuclear materials;
4. Disclosure of confidential documentation.

Solutions:
1. Atomic Keeper tracks the history of changes in the database – all data is validated against existing ones. Therefore, it is unlikely to introduce distortions into the data that will go unnoticed;
2. If the database is damaged, the data can be restored from a backup;
3. Operators have access to their MBA data only. Damage from an attacker's access is limited by the transactional mechanism of operations, IP verification and the "two persons" rule. An audit system prevents collusion and identifies who made any changes;
4. Advanced cybersecurity tools in Atomic Keeper minimize the data leakage chances.

The database structure in Atomic Keeper prevents sabotage even if the attacker is acting inside.

1. INTRODUCTION

In recent times, the rapid development of information technology has paved the way for an increase in cyberattacks worldwide. Data breaches — in which hackers steal personal data — continue to increase year-on-year: there was a 20% increase in data breaches from 2022 to 2023. Some of the trends around this uptick are disturbing. For example, globally, there were twice the number of victims in 2023 compared to 2022 [1]. These attacks target not only private entities but also government infrastructure facilities, including successful breaches that lead to theft, critical data alterations, and operational failures, e.g. Colonial Pipeline ransomware attack [2]. Thus, increased attention is being paid to this issue.

Considering the specifics of nuclear power plants and the grave threat in the event of successful cyber attacks from various hacker or terrorist groups, the development and construction of information security logic in systems at such facilities should be of primary importance.

Information security is ensured by a set of measures aimed at preventing unauthorized access, use, disclosure, distortion, modification, recording or destruction of information [3]. The elaboration of information security logic, like in any other security system, should begin with an examination of threats and their assessment. The key assessment criterion involves prioritizing threats based on their potential consequences.

The paper deals with countering cyber threats for accounting systems used at NPPs on the example of the Modular Automated Accounting and Control System "Atomic Keeper".

Initially, it's essential to observe a significant yet not immediately apparent aspect – accounting systems are not directly involved in the technological processes of management and therefore, temporary disruptions in their work are not

of critical significance for the entire enterprise. Moreover, in the event of server failure and even complete destruction of such systems, having a backup copy of the database ensures that the production process remains largely unaffected by any significant consequences. Recovery within a few hours or even days is generally acceptable, although it does cause some inconvenience.

At the same time a system of accounting for and control of nuclear material, sources of ionizing radiation or/and radioactive materials must be protected from external interference in the most thorough manner. The reason behind this is the fact that the data stored within these systems directly influence decision making, and any mistake in this process could result in the severest consequences including nuclear material losses, equipment damage, etc.

Based on the above, it is needed to concisely outline **the list of threats**.

The most dangerous threat is **the deliberate hidden misrepresentation of information with the aim of forming a false idea about the state of the controlled objects**. The primary focus of such an attack is individuals who base their decisions on the data provided by the accounting system. A particular danger lies in the fact that historical data, entered long before the current day, is altered, i.e. such alterations are unlikely to arouse suspicion among those who interact with the system regularly.

On the contrary, **falsification (spoofing) of current data** is significantly less dangerous. The current work relies on up-to-date data, and any interference should be promptly identified. Colleagues will thoroughly review the entered data, rectify any errors, and ensure seamless continuity. The primary concern associated with this threat is potential time loss.

The threat of accidental or intentional **database destruction** is on approximately the same level of danger. It is extremely difficult to imagine nowadays the absence of backups, therefore, the main requirement for the system is the ability to completely restore from a backup within a limited time.

Next in importance are all threats associated with **data leakage and disclosure of confidential documentation.** It covers a wide range, from compromising user passwords to intercepting network packets and server hacking.

Measures aimed at reducing the risk of threats emerging should be divided into organizational and technical ones. Organizational measures include restricting physical access, two-person rule etc.

The implementation of technical measures in the paper is considered on the example of the Modular Automated Accounting and Control System “Atomic Keeper”.

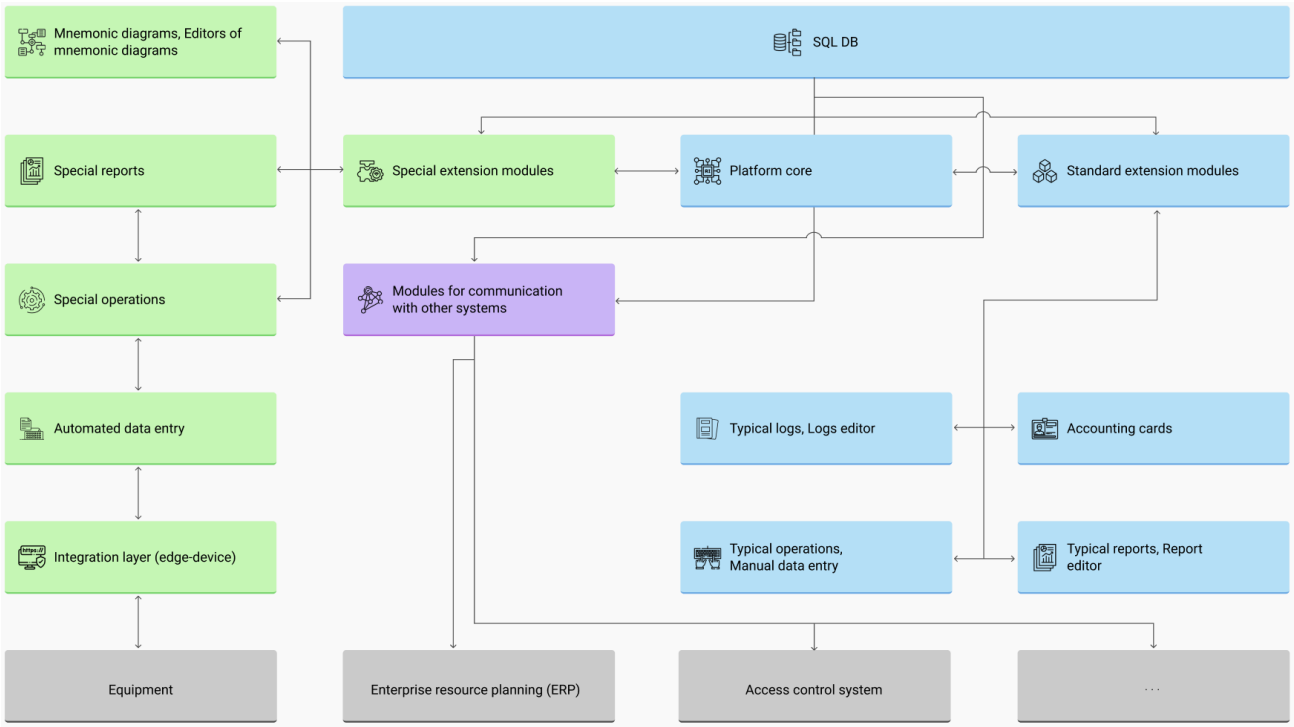
2. DESCRIPTION OF ATOMIC KEEPER

2.1. Universal Accounting Platform and extension modules

The Atomic Keeper system is based on the Universal Accounting Platform (UAP), which implements basic accounting functions and ensures information security of the entire solutions. The platform can be extended with extension modules that implement specific functionality for a particular solution.

Modules interact with each other and with the platform, and are configured by configuration settings. The latter are the rules and entities that describe the enterprise technological process. It includes accounting units with all the necessary fields and connections, using logs and reports with reference to the structure of the organization and diagrams of buildings and premises.

The configuration of Atomic Keeper is developed directly for a specific customer. This approach provides high flexibility. In addition, the end solution has a high technical reliability due to the fact that the system is adjusted to the customer's needs without source code changes.



Pic. 1. Universal Accounting Platform and extension modules

Currently available the following extension points:

- Accounting unit cards;
- Ledgers;
- Reports;
- Operations;
- Catalogs.

Atomic Keeper supports the work with tamper indicating devices, which enables restricting the activities on sealed objects.

Besides, Atomic Keeper enables to create and configure a particular monitoring screen that show the location of monitored objects with reference to a diagram of premises. The monitoring screens show accessible and sealed objects in different ways, displaying the applied seals.

2.2. Solutions based on Atomic Keeper

Currently, the following solutions based on the Atomic Keeper system exist: accounting for nuclear material, ionizing radiation sources and radioactive waste. These solutions can be used both in aggregate and in the form of separate configurations, depending on the objectives pursued by the customer.

A standalone Atomic Keeper solution of accounting for and control of nuclear material is positively operated at NPPs of the Republic of Belarus and the Republic of Turkey. Moreover, the Atomic Keeper system was included in the "Innovation for the Future of Nuclear Energy" list by GFNI (Global Forum for Nuclear Innovation Network organized by the IAEA) in 2020 and ranked as the innovation of April/May according to GFNI magazine's "The Network".

All work with the system is carried out with a web browser. The use of modern technical means of information protection such as the HTTPS protocol and Microsoft Identity mechanism and the presence of a blacklist and whitelist of

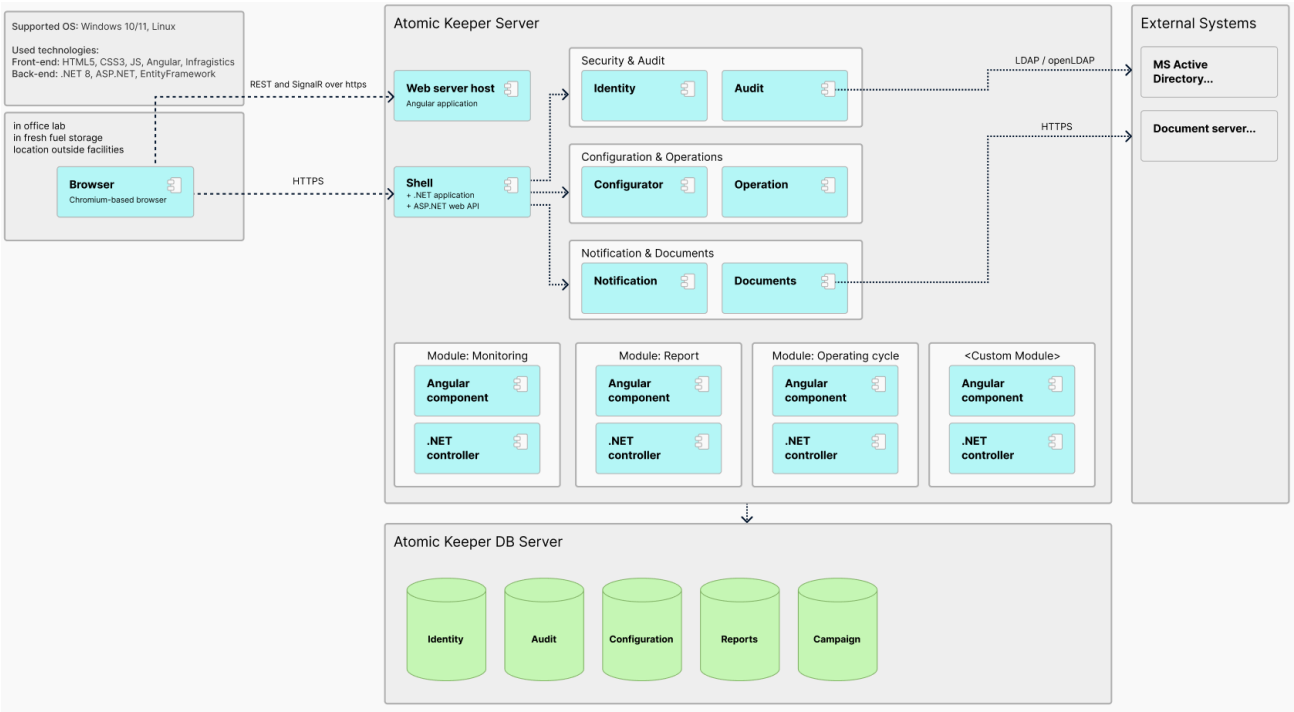
IP addresses, where no one outside the allowed list cannot be authorized in the system, enable to create *a basic level of cybersecurity*.

The system has two installation options: “Enterprise solution”, which is worked through the local enterprise network and “Local server solution” for a specific restricted laboratory.

2.3. Software architecture

From a technical point of view, Atomic Keeper is a cross platform solution that is written in .NET and compiled from sources directly into a machine code. The target Operating Systems are Windows Server and Linux, including Astra Linux, and PostgreSQL is used as a database.

The system has been thoughtfully structured. The platform is responsible for security, storing data and ensuring consistency when it changes. However, the logic behind such changes and the lion's share of functionality are implemented in extension modules.



Pic. 2. Software architecture of Atomic Keeper

There is a term *"operation"* in the Atomic Keeper system, i.e. a certain activity that changes the state of accounting units. Such changes are transactional and stored one by one. The system performs the validation of data relative to existing ones. In turn, the validation is performed by the values and its timestamps. Accordingly, if data changes in the past, the system checks validity of more recent operations and offers to correct them.

The universal reporting mechanism is implemented in the system core and, based on data entered into the system by operations, stores a list of operations on the basis of which each specific report is generated. Whenever changes occur in such operations, the system will generate a correcting report and compare it with the previous version. If differences exist, the system can notify the user.

The proposed approach enables to extend and change the system functionality by developing new modules and ensures information security on the system core level simultaneously.

3. INFORMATION SECURITY OF ATOMIC KEEPER

As mentioned above, ensuring information security is not a mandatory requirement for any one subsystem but is performed through a wide set of measures. Let's examine the measures implemented in the system according to the above list of threats.

3.1. Misrepresentation and fictive report generation

The transactional mechanism of operations, data integrity control and reports binding to operations, outlined above, allow automatic detection of changes in reports and notification of the user. This functionality fully performs the task of monitoring hidden changes; however, it was originally intended solely for automatically making corrective entries in reports according to Code-10.

There is the possibility in Atomic Keeper of generating any reports for any date in the past. Certainly, the old existing report can be always automatically compared with the newly generated for the same date.

Thus, based on the above, it seems highly unlikely to make modifications without logical conflicts, successfully bypassing various validation mechanisms, or rather it is needed to replace the entire database, including all generated reports to trick validation mechanisms.

3.2. Falsification (spoofing) of current data

For any system, there is always the possibility of introducing false information into it. There are several reasons for this:

- Intentional misrepresentation of information by an operator;
- Human error at any stage of information processing;
- Introducing false information into the system coming from other automated systems;
- Introducing false information into the system on behalf of the operator whose identification data was stolen.

The damage from such actions in Atomic Keeper is limited by the transactional mechanism of operations and, in addition, *the two-person rule*. The latter means that the information entered into the system (deleted from the system) by one user must be confirmed by another. Even if there is a conspiracy between operators, all changes made by attackers can be canceled in one move. All generated reports based on falsified data are detected automatically. In the event that such a report has already been published, Atomic Keeper will automatically create additional corrective reports.

Technical means aimed at protecting confidential information and user identification data are discussed below.

3.3. Database destruction

In case of damage or complete destruction of the database, there is a backup system, therefore, the system can be recovered within a few hours or even days which is absolutely acceptable for such systems.

3.4. Data leakage and disclosure of confidential documentation

Measures aimed at protecting data leakage and disclosure of confidential documentation should be divided into organizational and technical.

Organizational measures primarily include limiting physical access to servers, workstations and local networks. The completeness of implementation of this type of measures falls on the shoulders of the system owner, its IT administration and security service. These measures are described in the installation guide, should be applied during deployment of Atomic Keeper and include the following:

- Secure configuration of the database - lack of Internet access;

- Application of a special security configuration - only the app and authorized users can have the access to servers and application environment: database, file system, services;
- Prohibition the use of default passwords;
- Registration of a dedicated account for running a web server, ban on running it under an administrator account;
- Only catalogs for uploading files can have permissions to write;
- Prohibition of running applications from catalogs intended for uploading files;
- All unused server ports must be blocked.

From the Atomic Keeper system side, it is proposed a built-in user role separation, rights management and use of manager accounts. There are roles of administrator, commissioner and accounting expert in the system. This separation does not allow the administrator or commissioner to grant access to confidential data. Moreover, the administrator role has a separate right to access audit logs allowing them to monitor the situation around without a chance of sabotage by their side.

Options for restricting rights for accounting experts include the following:

- By MBA and premises;
- By departments;
- By types of operations performed;
- By access to the accounting unit cards and their history;
- By access to the monitoring displays, showing object locations on the enterprise diagram;
- By creating and/or having access to existing ledgers and reports.

The last point highlights a separate group of people with access to reports, but unable to make changes in the system. The presence of such a group in the system enables to further reduce the risk of deliberate hidden misrepresentation of information (see above) without compromising its integrity.

Technical measures aimed at protecting data leakage and disclosure of confidential documentation include the following:

- Data transmission protection, encrypted data transmission, use of SSL/TLS protocols;
- Maintaining and monitoring tracking records and user activity audit in the system, including unsuccessful activities;
- Presence of information about database recovery in the audit logs does not allow secretly replacing the database;
- Publishing the audit logs on an external server guarantees its safety even if servers of Atomic Keeper are destroyed;
- Implementation of precautions against known attacks targeting authentication vulnerability, adoption of SQL- and command code, Cross-Site Request Forgery (CSRF), memory overflow;
- Lack of data caching on the client and application server side;
- Use of a security certificate in Atomic Keeper and auditing it.

It should also indicate that during development of Atomic Keeper, the latest stable version of third-party technologies is used. This is guaranteed by applying the automatic analyzer of third-party dependencies, working during the compiling and building stage with subsequent monitoring of updates.

4. CONCLUSION

At radiation hazardous facilities are used control and accounting systems. Information security of accounting systems have its own peculiarities in threat assessment. The unique priorities of threats require appropriate approaches to protect against them. The approaches and measures adopted to implement protection against them in the Atomic Keeper system are presented in the following form:

(a) Transactional data changes.
(b) Tracking the history of data changes.
(c) Built-in ability of data correction.
(d) Validation of new data relative to existing ones.
(e) Binding reports to data change history.
(f) Generating reports for any date.
(g) Ability to automatically compare reports.
(h) Generating corrective reports.
(i) Use of the two-person rule.
(j) Logging of all activity in audit logs with the ability to publish it on an external server.
(k) Database backup with automatic recovery option within a limited time.
(l) Separation of user roles in the system into administrator, information security administrator, commissioner and accounting expert with access only to specific functionality of the system.
(m) Only accounting expert has the access to confidential accounting data.
(n) Within accounting expert role, rights are additionally distributed by departments, premises etc.
(o) Use of organizational measures to restrict physical access.
(p) Implementation of the security recommendations during deployment stage of the system.
(q) Use of modern technical means of information protection in Atomic Keeper minimize the chances of interception of transmitted data.

The approaches to implementing information security measures described in the paper allow us to confidently assert that accounting systems based on the Modular Automated Accounting and Control System “Atomic Keeper” are highly secured.

REFERENCES

[1] Madnick, S., Why Data Breaches Spiked in 2023 (2024) www.hbr.org/2024/02/why-data-breaches-spiked-in-2023

[2] Bing. C., Kelly S., Cyber Attack Shuts Down U.S. Fuel Pipeline (2021) https://www.reuters.com/technology/colonial-pipeline-halts-all-pipeline-operations-after-cybersecurity-attack-2021-05-08/

[3] CHANCHALA, J., SINGH, U. K., Information security risks management framework – a step towards mitigating security risks in university network, J. Inf. Secur. Appl. **35** (2017) 128–137.