Research on Security and Safety Requirements of Industrial APP

Min Yu[1], Sen Zhang[2*]

[1]yumin@ceprei.com

[2]zhangsen@dtsjy.com

[1]China Electronic Product Reliability and Environmental Testing Research Institute Guangzhou, P.R. China

[2]Guangzhou Metro Design & Research Institute Co., LTD Guangzhou, P.R. China

Abstract—This paper analyzes the security and safety requirements of industrial APP from the perspectives of industry and Internet. From the perspective of industry, industrial APP need to be used more and more to perform safety functions. In order to avoid the occurrence of safety accidents, functional safety requirements are put forward. From the perspective of the Internet, industrial APP need to ensure the safe operation of applications based on the industrial Internet to provide continuous service capabilities, and also need to pay attention to information security. In order to meet the needs of information security and functional safety of industrial APP, this paper studies the requirements of industrial APP covering information security and functional safety, which can provide certain support for the design, development, testing and evaluation of industrial APP with security and safety requirements.

Keywords-industrial APP; information security; functional safety; requirements

1 INTRODUCTION

The new era is accelerating the expansion of manufacturing industry to the direction of digitization, networking and intelligence. The characteristics of software definition, data driven, platform support, value-added services and intelligence are becoming increasingly obvious. The industrial Internet accelerates the promotion of intelligent manufacturing, and the industrial Internet platform enables industrial software to provide services for the industry with a new architecture [1]. With the rapid development of industrial Internet, industrial application software (referred to as "industrial APP") based on industrial Internet, bearing industrial knowledge and experience and meeting specific needs has become the consensus of the industry from quietly happening. Industrial APP developed based on the new architecture and

ICIDC 2022, June 17-19, Qingdao, People's Republic of China

DOI 10.4108/eai.17-6-2022.2322616

concept provides a better technical path and application practice for the development and application of industrial software. The development of industrial APP and industrial Internet forms a good situation of mutual promotion and progress [2].

Industrial APP is a software that bears industrial knowledge and experience (best practice) and is oriented to the industrial field to solve specific business needs in development & design, manufacturing, operation and maintenance, management [3]. In order to solve specific problems and meet specific needs, industrial APP abstracts industrial technical elements such as processes, methods, data, information, rules, experience and knowledge in the industrial field through data modeling and analysis, structuring and systematic abstraction, and based on unified standards. These industrial technical elements are packaged and solidified into a highly reusable and widely disseminated industrial application program, which generally has characteristics of specificity, applicability, independence and expansibility. As the carrier of industrial technical knowledge, industrial APP essentially solves the problem of application efficiency of industrial technology, and has a significant impact on industry, manufacturing model and software industry. Industrial APP bears foundation and future of industry. However, security & safety are important guarantee for the healthy development of industrial APP. This paper will study security & safety requirements of industrial APP on the basis of analyzing the security & safety needs.

2 SECURITY & SAFETY NEEDS OF INDUSTRIAL APP

At present, there are various classification methods for industrial APP, which can be classified from the scope of application, business links, knowledge types, operating environment and other dimensions [4]. For example, according to the scope of application, industrial APP can be divided into basic generic industrial APP, industry general industrial APP, enterprise-specific industrial APP and other industrial APP. According to business links, industrial APP can be divided into R & D industrial APP, production and manufacturing industrial APP, operation and maintenance service industrial APP and operation and management industrial APP. According to the type of knowledge, industrial APP can be divided into business informatization industrial APP, data analysis industrial APP and knowledge modeling industrial APP. According to operating environments, industrial APP have different software forms, which can be divided into embedded industrial APP, local end industrial APP, mobile end industrial APP, cloud end industrial APP and cloud-side collaborative industrial APP.

Security and safety are important guarantee for the healthy development of industrial APP. The security and safety needs of industrial APP can be analyzed from the perspectives of industry and the Internet. From an industrial perspective, industrial APP is used in industrial production environments, and which is increasingly used to perform safety functions, such as: production and manufacturing industrial APP, etc., industrial APP is more and more prone to interference with other devices, and their execution errors will not only bring about data errors, but may lead to serious consequences. The focus of safety consideration should be on the functional safety of related intelligent equipment, industrial control equipment and system in the process of production and manufacturing. Higher requirements for functional safety are put forward to avoid accidents and ensure the real-time, continuity and reliability of production and manufacturing. From the perspective of Internet, security mainly ensures the operation of

industrial Internet applications such as personalized customization, network collaboration and service extension to provide continuous service capabilities, such as: operation and maintenance service industry APP, operation and management industry APP, business informatization industry APP, data analysis industry APP, mobile end industry APP and cloud industry APP, etc., need to pay attention to information security. Information security is closely related to the functions realized by the information system. Confidentiality, integrity, availability, and in some cases authenticity, verifiability, repudiation resistance requirements of information and system carrying the information can be protected and maintained.

Therefore, in order to meet the security and safety needs of industrial APP, its requirements will include information security requirements and functional safety requirements. Information security requirements mainly focus on the installation and uninstallation, identification and authorization, access control, data security and operation security. Functional safety requirements define the requirements for the safety-critical function, including requirements analysis, design and realization. The details are shown in Figure 1.

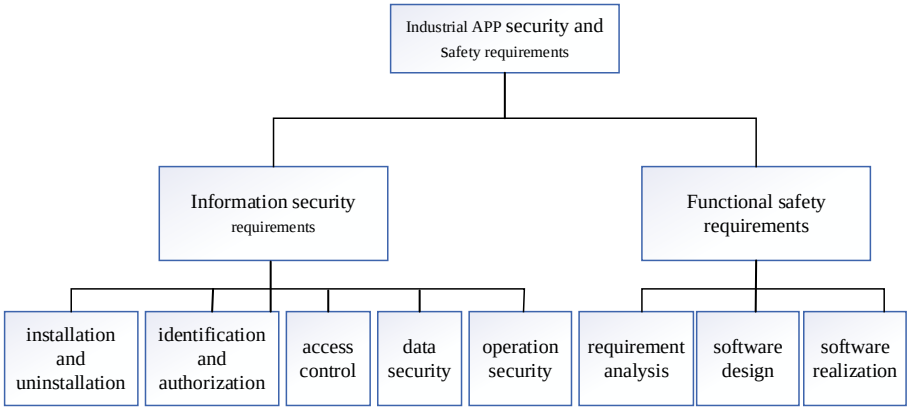

Figure 1. Industrial APP security and safety requirements framework

3 INFORMATION SECURITY REQUIREMENTS

Information security is to protect and maintain the confidentiality, integrity and availability of system carrying information, and can also include authenticity, verifiability, repudiation resistance, reliability and other properties [5]. At present, there are standards related to software information security, such as: GB/T 28452-2012 [6], GB/T 34975-2017 [7], the security requirements of application software and mobile intelligent terminal application software are stipulated in the standard. On basis of reference to the above standards, this paper analyzes the information security requirements of industrial APP. Suggestions include the following five aspects: installation and uninstallation, identification and control, access control, data security and operation security.

3.1 Installation and Uninstallation

Installation function easily to industrial APP itself or potential threat to the safe operation of terminals, therefore, need to strictly control the installation operation, in case of unsafe industrial APP to "settle", should meet the following security requirements: Include signature information, software attribute information that can effectively identify the supplier or developer; During installation, users should be prompted to confirm terminal resources and terminal data; It should be correctly installed on the terminal, and should not affect the normal operation of other software on the terminal. Similarly, the uninstallation of industrial APP does not affect the normal use of terminals. The uninstallation requirements should at least meet the following requirements: Resource files, configuration files and user data generated during installation and use should be deleted; There should be prompt when deleting the data generated in the process of user use; Do not affect the functions of other software on the terminal.

3.2 Identification and authorization

Identification and authorization are the most basic requirements for access control [8]. Identification is used to verify a user's identity and is usually a prerequisite for granting access to an industrial APP. If the industrial APP involves user sensitive data and industrial control equipment control instructions, access to user accounts should be managed and effective identification and authorization functions should be provided, including: authorized users should be supported to manage and maintain user identification to ensure that it is not accessed, modified or deleted without authorization; Before users access application services, industrial APP should successfully authenticate their identity, only provide the least feedback (such as the number of characters entered) to the authenticated users, and provide measures to deal with authentication failure (such as locking account); It can lock or log out after login timeout; Provide active user lock or logout function; If users access security-related industrial control apps, they should implement separation of responsibilities and minimum permissions according to applicable security policies and procedures; For safety-related control industrial APP, where necessary, local emergency operations and the basic functions of industrial APP should not be hindered by the need for identification, and access to these systems can be restricted by appropriate physical security mechanisms. It should be noted that password authentication is the simplest and most commonly used authentication technology. If user passwords are involved, the followings should be met: they should not be displayed and stored in plain text during use; The last account and password should not be saved by default; There should be a password intensity check mechanism, password timeliness check mechanism; When changing or retrieving a password, an authentication mechanism should be in place.

3.3 Access Control

Access control is one of the key technologies of information security. Its purpose is to protect the object from unauthorized operations of the subject. It determines who can access industrial APP, what resources can access industrial APP and how to use these resources. Proper access controls can prevent unauthorized users from accessing data either intentionally or unintentionally. About industrial APP access control should consider the following two aspects: one is about access control of the industrial APP, when industrial APP involves user sensitive

data, industrial control equipment control instructions, should the user access control function independently, to design and implement of access users with effective authorization mechanism, authorized users access to content cannot be beyond the scope of authorization, that is to say, allows authorized users to access, and prevent unauthorized users from accessing (note: access includes read, write, execute, etc.); Second, the access control of industrial APP on the platform data or terminal resources should be explicitly approved by the platform users. Before obtaining the permission, it should not access platform data and platform resources, modify or delete terminal data, or modify the configuration of platform resources.

3.4 Data Security

Industrial Internet platform provides a security mechanism to protect the platform, but it still can not stop attacks of countless attackers on vulnerabilities of platform or software. The data security of industrial APP is severely challenged in this process, especially with user privacy data or important account password data. When developing applications, on the basis of the existing security mechanism of industrial Internet platform, developers should also consider taking corresponding security measures to protect the data security of the industrial APP. Therefore, if the industrial APP involves a user sensitive data, it should have user data integrity and confidentiality protection function, can consider the following aspects: User data shall not be viewed or modified without authorization; User sensitive data should not be stored or transmitted in the database or file system in the form of "plaintext", it should be encrypted or hidden to prevent unauthorized access of data; If the data deletion function is available, the user should be prompted before deleting the data and the user should confirm whether to delete the data again; For industrial APP applications with high data security requirements, it should have data backup and recovery functions.

3.5 Operation Security

Operation security is an important part of industrial APP security. Only when the security of industrial APP is guaranteed during operation, can it achieve the correct function and achieve the purpose of giving full play to the functions of software. Operation security of industrial APP generally includes the realization of security, stability, fault tolerance, resource availability and software upgrade. In terms of the realization of security, industrial APP ensures the security of the program itself by implementing security-related technologies, including: protection mechanisms should be used to prevent, detect, slow down and report detected malicious codes; No entry of any type that violates or circumvents security rules and any pattern not described in the documentation should be designed; There should be a security mechanism to prevent the program from being decompiled and debuggable; There should be no published high-risk vulnerabilities. In terms of stability, industrial APP should ensure its stable operation and avoid similar phenomena such as failure, including: no collapse or abnormality; Avoid loss of response, flash back and other phenomena; Allow to stop and exit at any time. In terms of fault tolerance, when the industrial APP is attacked or has predictable wrong operation, it should be able to output the predefined state without affecting the normal operation of the program, including: Ideally, the operation can continue to be normal without affecting the normal operation of the program; If it cannot maintain normal operation, it should output a default failed state. In terms of resource availability, the operation of industrial APP should not affect

the access to resources for legitimate terminal users, and should provide the ability to limit the use of resources through security functions. Terminal resources should not be fixed or unrestricted for a long time to prevent resource exhaustion. In terms of software upgrade, generally speaking, industrial APP should support software update, including: at least adopt a security mechanism to ensure the timeliness and accuracy of the upgrade (such as automatic upgrade, update notification, etc.); In the event of an upgrade failure, industrial APP should be able to roll back to ensure software integrity.

4 FUNCTIONAL SAFETY REQUIREMENTS

Functional safety is the ability of the system not to cause casualties, system destruction, major property loss or endanger human health and environment [9]. The functional safety of industrial APP runs through the whole software life cycle and should be closely combined with software engineering process activities. The basic process of life cycle including acquisition, supply, development, operation and maintenance, a total of five process. And the software development process is the most complex process of the basic software life cycle process, is also directly affect the other basic process. Software development process is the most complex process among the five basic processes of software life cycle, and it also directly affects other basic processes. This is because a good development process is necessary for the success of the provisioning process, and it is also the foundation for the smooth operation and maintenance process. Therefore, this paper mainly considers the core of industrial APP development process, namely requirements analysis, design and realization process.

The software development process of industrial APP should meet the traditional requirements for requirements analysis (e.g., the tracking relationship between each software requirement and software development requirement should be established), design requirements (e.g., low coupling degree should be met between modules, and high cohesion should be met within modules) and realization requirements (e.g., After debugging, the software should remove unnecessary statements used for debugging in the program in a timely manner). This paper does not make special requirements for the general requirements of the software development process of industrial APP. This paper only considers the requirement analysis, design and realization process of the safety-critical function of industrial APP. Through fault tolerance and failure tolerance, interface design, data design and other safety design methods, and through software coding, code verification and other software realization methods, so as to minimize the system safety risk, where possible, through the design to eliminate identified risks or reduce related risks.

4.1 Requirements Analysis

In order to realize the functional safety of the system to which industrial APP belongs, safety requirements are put forward for safety-related industrial APP. Industrial APP should consider the needs of system safety. It should search for safety key functions and determine safety requirements based on system safety requirements, environmental requirements, interface requirements, system risk report and system risk analysis report, etc. The following aspects should be considered: Safety requirements shall be clearly identified in requirements

specifications and shall be complete, clear, accurate, unambiguous, verifiable, testable, maintainable, implementable and traceable; Safety requirements should specify operational modes or states that are valid, as well as prohibited or inapplicable modes or states; The safety criticality of requirements should be ranked according to the probability and severity of the occurrence of hazards; Components such as modules and units used to realize safety-critical functions should be identified, and the interaction of safety-critical components with other non-critical components should be limited as far as possible; The number of safety-critical components should be minimized, and interfaces between them should be designed to minimize interaction.

4.2 Software Design

In design process of the industrial APP, in order to realize the safety design, should consider the following eight aspects:

- Safety operation mode, operation state and condition. It should find out whether there are conditions and potential failure risks that may lead to the unsafe state of industrial APP, and formulate appropriate response requirements for all conditions and potential failure risks of unsafe state, so as to avoid the forbidden or inapplicable mode or state of industrial APP. Conditions for an unsafe state may include out-of-order or incorrect events, inappropriate values, unintentional commands, errors caused by environmental interference, and so on.

- Interface safety design. The characteristics, the error mode and error probability of the interface should be analyzed. On this basis, the communication method, data coding, error checking, synchronization method and check and error correcting code method should be determined. Interface types include hardware-related interfaces, indirect interfaces of software modules, and man-machine interfaces.

- Data safety design. Data safety design should consider the following aspects: identify safety-critical data and isolate it from other data so that non-safety-critical components cannot access it; The reasonable range of data should be specified, which should be explained in implementation and checked in operation; If the data exceeds the specified range, error processing should be carried out; Check important data and return to specified state (e.g., safe state) in case of error; The operation of safety-critical functions should be performed only after receiving two or more identical data; Safety-critical data will not cause a system failure due to one or two errors.

- Margin design for timing, throughput and scale. For safety-critical functions, timing, throughput and scale allowances should be designed with system resource and time constraints in mind and allowance requirements taken into account. Generally, no less than 20% allowance should be left.

- Mistake proofing design. Error-proof design should consider the following aspects: unauthorized or unintentional access or modification of programs and data should be prevented; Unintentional jumps within or between safety-critical software should be detected and recovery measures should be provided to enter the fail-safe state from the unintentional instruction jumps; Monitor at key points, isolate faults when faults are found, and make the system enter a safe state when necessary; To prevent programs from mistaking data for instructions, store them separately.

- Fault-tolerant and fail-tolerant design. Fault tolerance can prevent most of the small errors from spreading into failure; Most faults are ignored and only higher-level faults that may cause system failures are handled. Industrial APP should have certain fault-tolerant and fail-tolerant capabilities, which can detect its own internal errors and prevent the transmission of errors to prevent the spread of faults. Redundancy design, such as recovery block technology, shielding technology and N version program design, is a common method of fault tolerance and failure tolerance.

- Self-checking design. The self-checking design should consider the following: monitoring timers or similar measures should be provided to ensure that the microprocessor or computer is capable of handling program timeouts or dead-loop failures; Memory, instruction and data buses should be checked periodically to ensure the integrity of safety-critical code; Fault detection and isolation procedures should be written to detect potential safety-critical failures, isolate faults to the lowest practical level using fault isolation procedures, and provide this information to operators or maintenance personnel.

- Abnormal protection design. The design of anomaly protection should consider the following aspects: It should analyze all kinds of possible anomalies during software operation and design corresponding protection measures for them; Automatic safety protection is often required when the critical time is less than the real operator response time, or when there is no human intervention in the operating loop; The exception handling measures should make the system into a safe state, save the field information of the exception, and keep the computer in the running state.

4.3 Software Realization

Coding and verification are collectively referred to as the software realization, encoding is designed to further embodiment, quality mainly depends on design of the industrial APP, however, industrial APP each stage of the life cycle will inevitably produce errors, the purpose of verification is before it running, as much as possible to find errors in the software.

- Software coding. In order to ensure the safety of industrial APP realization, the following aspects should be considered during coding: standardized programming language should be used for programming, and corresponding programming standards should be followed during coding; Safety-critical function codes should be clearly identified and annotated in sufficient detail; Non-safety-critical function code should not affect safety-critical function; In order to facilitate later testing and maintenance, the complexity of procedures should be controlled; The program detection points should be set on the key points for monitoring safety key functions, and fault isolation should be carried out when faults are found. If necessary, the system should enter a safe state. Running and supporting programs should contain those features and capabilities that are required by documentation, not features that are not documented.

- Software verification. The purpose of the software verification process is to detect and report errors that may be introduced in the software development process, and achieve the goal of the software verification process through walking, analyzing, developing test cases and procedures, as well as executing test procedures and other activities [10]. Verification of industrial APP should consider the following aspects: verify that all safety-critical code units can be traced to safety-critical design, verify that all safety-critical design elements can be

traced to safety requirements, and vice versa; Verify that the design does not violate any safety controls or processes, that any additional hazards, causes of hazards, or contributing factors to hazards are documented, and that the design maintains the system in a safe state in any operating mode; Verify that safety requirements for all safety-critical functions are correctly implemented in the software code; The conformance of the code to safety programming standards should be verified; Verify that the code implementation does not violate any safety controls or procedures, does not create any additional risks, and maintains the system in a safe state under all operating modes; Should use code to check software logic errors in logic analysis, using the data from the data analysis, software structure and usage, use code to check the parameters properly interface analysis through interfaces are analyzed in transmission, using interrupt to prove the validity of the interrupt to use, analyze the unused code, an analysis of the influence domain changes.

5 CONCLUSION

Security and safety are the guarantee for the healthy development of industrial APP. Firstly, this paper analyzes the security and safety requirements of industrial APP from the perspectives of industry and the Internet. From an industrial perspective, industrial APP are increasingly used to perform safety functions. The focus of safety consideration should be the functional safety of relevant intelligent equipment, industrial control equipment and systems in the process of production and manufacturing, so as to ensure the real-time, continuity and reliability of production and manufacturing. From the perspective of the Internet, industrial APP should focus on information security, protecting and maintaining the confidentiality, integrity and availability of information and the system carrying it. In some cases, it also includes authenticity, verifiability, repudiation resistance and other requirements. Then, on the basis of analyzing the security and safety requirements of industrial APP, this paper studies the security and safety requirements of industrial APP covering information security and functional security. Among them, the information security requirements mainly focus on the installation and uninstallation, identification and authorization, access control, data security and operation security of industrial APP. This section describes the functional safety requirements of the security-critical software, including the requirements analysis, design, and realization of safety-critical functions. This paper can provide some support for the design, development, testing and evaluation of industrial APP with safety requirements.

ACKNOWLEDGMENT. This work was supported by the 2018 Industrial Internet Innovation and Development Project "Industrial Internet Security & Safety Standard System and Experimental Verification Environment Construction", Guangdong Basic and Applied Basic Research Foundation under Grant No. 2019B1515120086 and the Ministry of Industry and Information Technology Key Laboratory of Industrial Software Engineering Application Technology.

REFERENCES

[1] Y. Z. Li, “Some understanding of the development of industrial APP industry”, Satellite & Network, 2020, pp. 28-30.

[2] Y. Y. Zhang, Z. Z. Liu, and X. J. Liu, etc, “Suggestions on Promoting the Development of Chinese”, Standard Science, 2020, pp. 49-52.

[3] China Industrial Technology Software Industry Alliance. Industrial Internet APP Development White paper, 2018.

[4] T/CESA 1046-2019, Classification, grading and evaluation of industrial APP, 2019.

[5] Y. Jiang, S. Wu et al., Secure Data Transmission and Trustworthiness Judgement Approaches Against Cyber-Physical Attacks in an Integrated Data-Driven Framework, IEEE Transactions on Systems, Man, and Cybernetics: Systems.

[6] GB/T 28452-2012, Information security technology – Common security technique requirement application software system, 2012.

[7] GB/T 34975-2017, Information security technology – Security technical requirements and testing and evaluation approaches for application software of smart mobile terminals, 2017.

[8] P. Huang, “Information security testing and application of mobile intelligent terminal application software”, Electronic components and information technology, 2021, vol 5, pp. 232-233+236.

[9] IEC 62279:2015, Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems, 2015.

[10] P. H. Liu, and S. L. Wang, “Application of software functional safety verification activities”, Microcontrollers & Embedded systems, 2021, vol 21, pp. 22-25.