Security Risk Analysis Model for Identification and Resolution System of Industrial Internet

MA Baoluo, CHEN Wenqu, and CHI Cheng

(Institute of industrial Internet and Internet of Things, China Academy of Information and Communications Technology, Beijing 100191, China)

Abstract: Identification and resolution system of the industrial Internet is the "neural hub" of the industrial Internet for coordination. Catastrophic damage to the whole industrial Internet industry ecology may be caused if the identification and resolution system is attacked. Moreover, it may become a threat to national security. Therefore, security plays an important role in identification and resolution system of the industrial Internet. In this paper, an innovative security risk analysis model is proposed for the first time, which can help control risks from the root at the initial stage of industrial Internet construction, provide guidance for related enterprises in the early design stage of identification and resolution system of the industrial Internet, and promote the healthy and sustainable development of the industrial identification and resolution system.

Keywords: industrial Internet; identification and resolution system; security risk analysis model

DOI: 10.12142/ZTECOM.202001008

http://kns.cnki.net/kcms/detail/34.1294.TN.20200316.1730.006.html, published online March 17, 2020

Manuscript received: 2019-12-01

Citation (IEEE Format): B. L. Ma, W. Q. Chen, and C. Chi, "Security risk analysis model for identification and resolution system of industrial internet," *ZTE Communications*, vol. 18, no. 1, pp. 49 – 54, Mar. 2020. doi: 10.12142/ZTECOM.202001008.

1 Introduction

The security of identification and resolution system of the industrial Internet is one of the keys for securing the industrial Internet. The popularization of industrial identification and resolution may affect production security, social security and even national security. Industrial identification and resolution system is one of the significant parts of industrial internet network architecture, and it is the key to realize the interconnection among equipment, system, data and networks. With the identification and resolution system of the industrial Internet, information can be shared and used across enterprises, industrial sectors and regions; enterprises can vertically and horizontally integrate their global supply chain systems and production systems respectively, to realize intelligent production, personalized customization, important product traceability and product life cycle management. The identification and resolution system is the "neural hub" of the industrial Internet for coordination. Therefore, catastrophic damage to the whole industrial ecology may be introduced or even become a national security threat, if the identification and resolution system is attacked.

2 Concept Design of Security Risk Analysis Model

2.1 Concept Design

Through the analysis of security architecture of the Internet

This work was supported by the 2018 Industrial Internet Innovation and Development Project —— Industrial Internet Identification Resolution System: National Top-Level Node Construction Project (Phase I) .

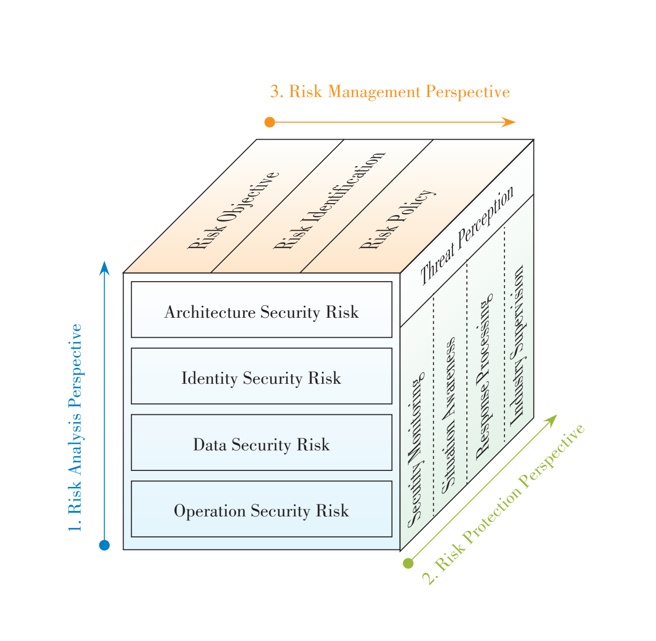
and the industrial Internet abroad [1], an innovative security risk analysis model has been developed combing the characteristic of the industrial identification and resolution system of the industrial Internet, to provide guidance for security construction of the identification and resolution system of industrial internet, help control risks from the root at the initial stage, and improve the security protection capability.

2.2 Overall Architecture of Security Risk Analysis Model

The core of the security risk analysis model are three perspectives: the security risk analysis perspective, the security risk management perspective and the security protection perspective. The key elements in each of the perspectives are outlined in **Fig. 1**.

In the architecture, the security risk analysis perspective includes four key risk analysis elements: the architecture security risk analysis, the identity security risk analysis, the data security risk analysis and the operation security risk analysis. The security risk management perspective includes the security risk objective, the security risk identification and the security risk policy. The security risk protection perspective includes industrial sector supervision, security monitoring, situation awareness, threat perception and response processing.

As shown in Fig. 1, these three perspectives form the basis of the security analysis model. They are relatively independent, while they are intertwined and form an organic architecture of the security risk analysis model for the identification and resolution system of the industrial Internet. The security risk analysis often performs within each of the perspectives to which they belong. However, this is not to imply that the risk analysis is always to be resolved within each of the perspectives, being separated with that in other perspectives. In the following sections, a detailed illustration will be introduced.



▲Figure 1. Overall architecture of the security risk analysis model for identification and resolution system of industrial internet.

2.2.1 Security Risk Analysis Perspective

The security risk analysis perspective includes the architecture security risk analysis, the identity security risk analysis, the data security risk analysis and the operation security risk analysis, as shown in **Fig. 2**.

The architecture security risk analysis is mainly composed of the node of identification and resolution availability risk, the inter-node collaboration risk and the key node correlation risk.

The identity security risk analysis mainly includes four kinds of risks about people, machines and objects, which are identity deception, unauthorized access, the authority chaos, and the device vulnerabilities [2].

The data security risk analysis [3] mainly focuses on the risk of theft and tampering identity resolution registration data, resolution data and log data, the risk of privacy data disclosure, and the risk of data loss.

The operation security risk analysis includes the risk of personnel management, institutional management and operation process management.

2.2.2 Security Risk Management Perspective

The objective of the security risk management perspective is to provide guidance for constructing a risk management mechanism with the ability to improve the security continuously, illustrated by **Fig. 3**.

In Fig. 3, the risk objective refers to the object of risk assessment and business guarantee of the identification and resolution system of the industrial Internet.

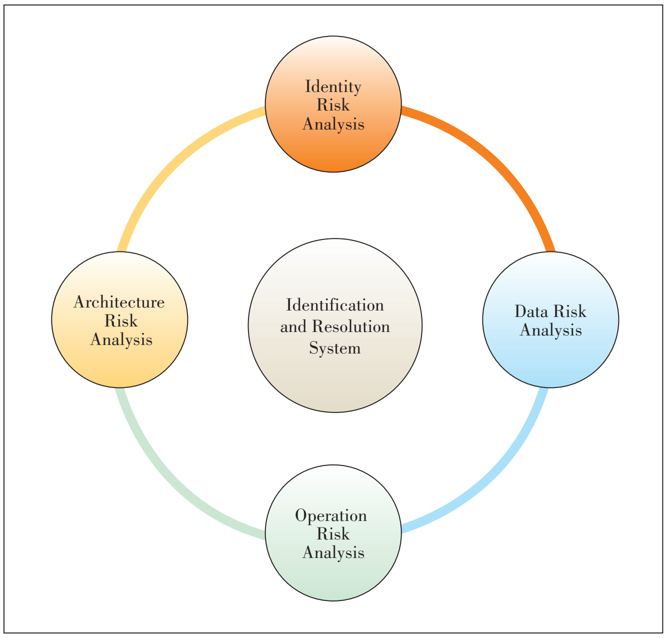
Risk identification refers to possible identified risks that may occur according to the risk objective.

Risk policy provides corresponding security protection strategies according to the existing risks.

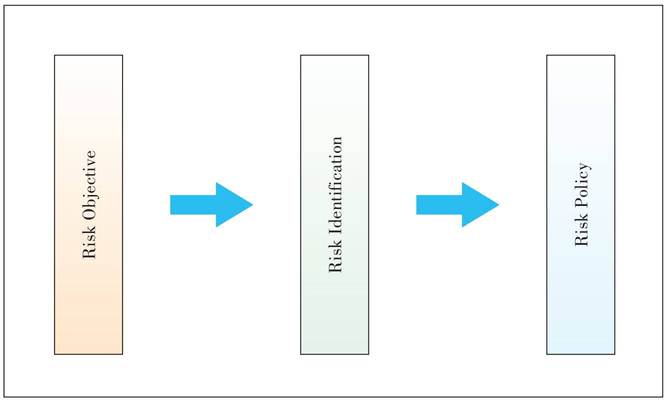
2.2.3 Security Risk Protection Perspective

In view of the various risks faced by the identification and resolution system of the industrial Internet, the security risk protection perspective clarifies the guidance from the whole life cycle and facilitates the risk closed-loop control. **Fig. 4** shows the core of the security risk protection perspective, including five areas: the industrial supervision, the security monitoring, the security situation awareness, the threat perception, and the response processing. The supervision from industrial sectors is centralized in this perspective, which implicates that attention needs to be paid during the construction of the security protection network.

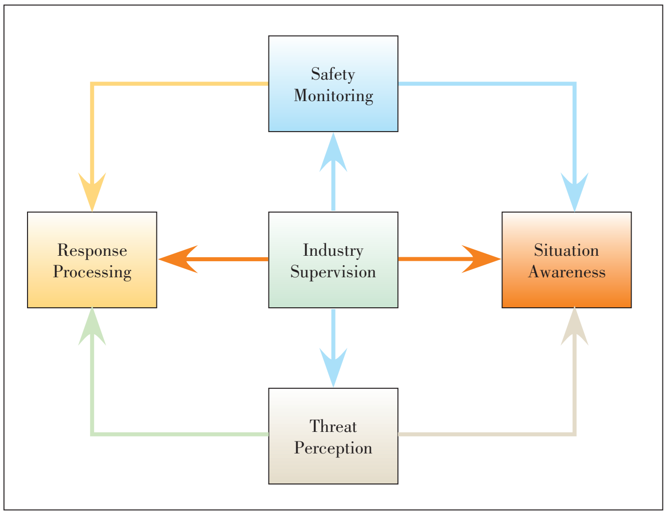
In Fig. 4, the supervision from industry represents the unified leadership and command, in order to establish a joint-action mechanism. The security monitoring aims at four risk



▲Figure 2. Schematic diagram of the security risk analysis perspective.



▲ Figure 3. Schematic diagram of the security risk management perspective.



▲Figure 4. Schematic diagram of the security risk protection perspective.

analysis objects above to carry on risk monitoring. The security situation awareness refers to the deployment response and real-time awareness of security risks. The early threat perception addresses the risks found by the situation awareness and issues early warnings. The response processing deals with security risks in time by the establishment of a response mechanism.

3 Proposed Security Risk Analysis Model

3.1 Architecture of Risk Analysis Model

The architecture of the identification and resolution system of the industrial Internet adopts the tree hierarchical architecture (**Fig. 5**); basically, it is a distributed information system. The identification and resolution system of the industrial Internet consists of clients, resolution servers, mirror servers, proxy servers, and cache servers. The security of this architecture depends on the security of each part. A problem arising at any layer of the architecture may affect the security of the whole architecture to some extent [4].

There are many risks in the identification and resolution system of the industrial Internet, such as the risk of node availability, the risk of inter-node collaboration, and the risk of key node correlation.

1) Risk of node availability.

The risk of node availability refers to the risk of availability faced by each node in each layer of the architecture. If one node is attacked, the availability of the node will be threatened, as a consequence, the node function will be failed or inaccessible. To be specific, the main risk of node availability is Distributed Denial of Service (DDoS) attack.

2) Risk of inter-node collaboration.

The risk of inter-node collaboration is an intrinsic risk of identification and resolution system of the industrial Internet. It refers to the risk of delay in the process of data synchronization or replication, which may consequently result in data inconsistency or data integrity problems, when there is a problem in the process of resolution. The risk of inter-node collaboration mainly includes proxy service delay, mirror server delay, and more.

3) Risk of key node correlation.

The risk of key node correlation exists in the failure of key node functions caused by the problems of other key nodes in the identification and resolution system of the industrial Internet, weakening the system ' s reliability or robustness. The risk of key nodes correlation includes cache breakdown, cache penetration, and attack reflection/magnification.

3.2 Identity Risk Analysis

Identity security is the important entrance of identification and resolution system of the industrial Internet. The user system requires users to authenticate first; obviously, the identity security is of great importance. Different roles, from people, machines to objects, in the identification and resolution system have different authentication levels, and any risk point can cause authority or trust to be infringed [5].

The main risk points for different identity roles are shown in **Table 1**.

1) Identity deception.

Identity deception can also be called identification defraud in the identification and resolution system of the industrial Internet. The related risk analysis will be conducted in three perspectives: people, machines and objects.

2) Unauthorized access.

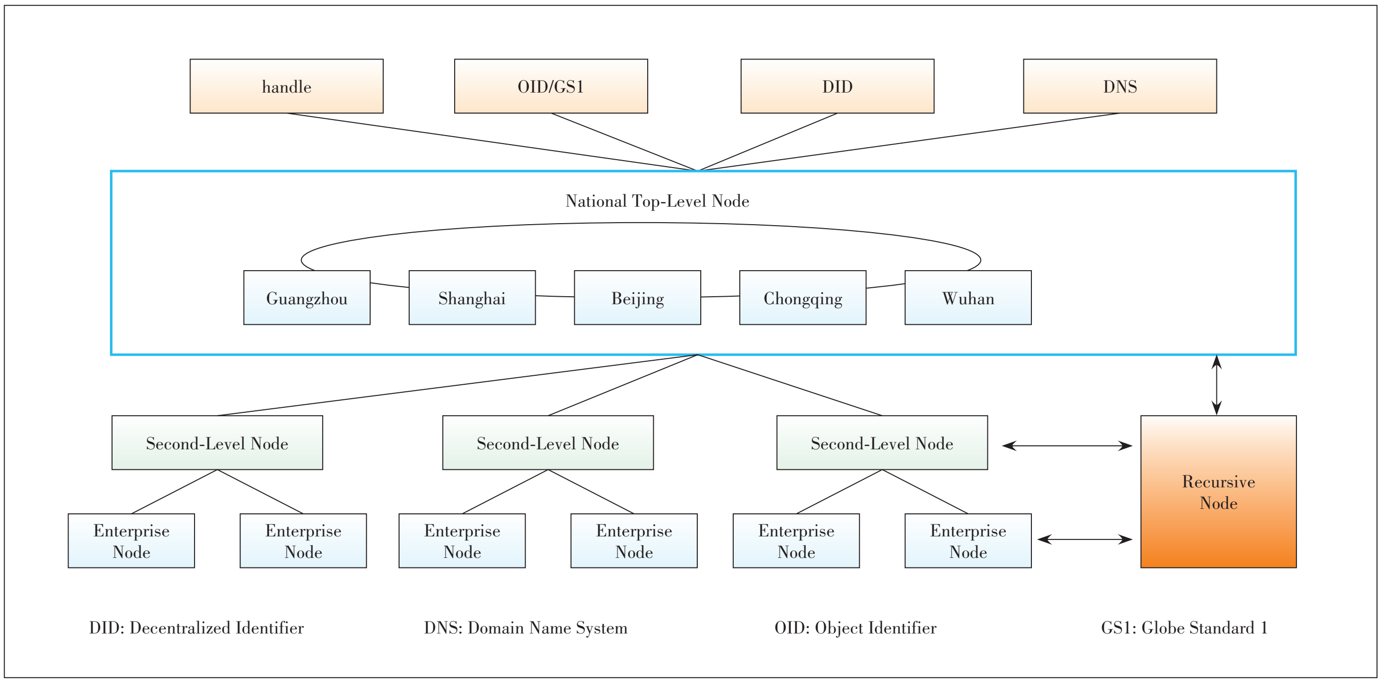
Unauthorized access mainly refers to the ability to access resources that exceed the user's authentication. For example, the identity administrator should only manage the identity function without the function of the ordinary user; if the identity administrator appears to have the function of the ordinary user, this is unauthorized access.

3) Disordered authority.

There are a vast number of devices and people using the identification and resolution service. This gives hackers the chance to enter the system without proper authentication, by means of injection, infiltration, etc. , to cross the access management system.

4) Device vulnerabilities.

The servers, clients or terminals in the identification and resolution system of the industrial Internet may have security vulnerabilities or use components with known vulnerabilities. Device vulnerability [6] makes it easier for attackers to pass the set access control policy, get remote control and tamper the device data.



▲**Figure 5. Architecture of identification and resolution system of industrial Internet.**

▼**Table 1. Security risks for identity**

Identity Category	Specific Identity	Risk Points
People	Administrator for identification data	Identity deception; unauthorized access; authority chaos
	User	
	Administrator for identification	
	Third party supervisor	
Machines	International root node	Identity deception; device vulnerability
	National top level node	
	Secondary node	
	Enterprise node	
	Recursive resolution node	
	Industrial client	
Objects	Industrial Internet terminal	Identity deception; false correlation between identification and product; device vulnerability

3.3 Data Risk Analysis

There are three types of data in the identification and resolution system of the industrial Internet, including identification registration data, identification resolution data, and log data. Data security includes three dimensions: data integrity, data confidentiality and data availability. According to GB/T 37988/2019 "Information Security Technology Data Security Capability Maturity Model" [7], identification data security involves data acquisition, data transmission, data storage, data usage, data exchange, and data destruction. Based on the aforementioned, the security risk is mainly composed of the risk of date theft and tampering, the risk of privacy data leakage, and the risk of data loss.

1) Data theft.

The risk of industrial identification resolution data theft is mainly to destroy the confidentiality of data. The data is obtained by unauthorized users, which makes the identification registration data, identification resolution data or log data breach. It may occur in the data acquisition process, data transmission process, data exchange process and data storage process.

2) Data tampering.

When industrial devices are connected to the industrial Internet, attackers have the opportunity to read and modify the data stored in the devices by physical or remote access to the connected devices. There is a risk that the data is maliciously tampered and falsified, which makes the algorithm and processing cracked, leading to the registration data, the resolution data and the log data in the identification system are tampered.

3) Private data leak.

The absence of effective safety protection measures is high likely to cause private data leak of industrial enterprises such as key equipment data, product data, management data, and customer data in the process of using identification and resolution service. The consequence could be significant loss for person and enterprise. In some case, it could even bring incalculable losses to the whole country.

4) Data loss.

In the process of using identification data, if there are no secure protection measures and proper backups, data may be lost due to several reasons. First, illegal operative may maliciously delete the data after obtaining access through attacks on the cache or proxy server. Second, data loss may be caused by the server damage in natural disasters. Last but not least, data loss may be caused by operation mistakes, like unintentionally deleting data. Data loss and failure in recovery of important data such as key equipment data, key product data and user data, could be great losses to industrial enterprises.

3.4 Operational Risk Analysis

Operational risk management plays a vital role in identifying, measuring, supervising, controlling and reporting the operational risk of second-level nodes. With the development of identification ecology, more and more participants involved. The increasingly growth of user number and continual system expanding bring new challenges to the operation of identification and resolution system of the industrial Internet. The internal and external risks will affect the security and controllable operation of the whole identification and resolution system. The operational risks include risks from personnel management, branch management and process management.

1) Risk from personnel management.

The operation of the identification and resolution system of industrial internet requires high reliability and high security. All employees who may affect the operation of identity allocation, identity resolution, business management, data management, etc. (collectively referred to as "personnel") may affect the normal operation of the system. They are referred to as trusted roles. The risk of personnel management includes the risk of role identification, key position role management, personnel operation and personnel control.

2) Risk from branch management.

Branch management risk mainly refers to the life cycle management risk of entities that provide corresponding identification services in the identification and resolution system of the industrial Internet. The risk of branch management mainly includes the authorization risk of branch office, the operation risk of branch office and the risk of service termination of branch office.

3) Risk from process management.

The operation of the identification and resolution system of the industrial Internet involves a series of business processes. The management of business processes is necessary. Otherwise, operators can only use their own experience in their work with great arbitrariness, negatively affecting the system operation and potentially bringing the risk of application process management of secondary nodes.

4 Conclusions

An innovative unified security analysis model for identification and resolution system of the industrial Internet is proposed in this paper, based on the thorough study of the security risk in industrial internet. This is significant for promoting the industrialization of identification and resolution system and corresponding service. First, it helps control risks from the root at the initial stage of identification and resolution system of industrial internet construction. Within this model, the risk points, risk events including their cause and possible consequence, appropriate protection measures, can be identified in early stages. Second, it provides guidance for security construction of the identification and resolution system of industrial internet. Last but not least, it promotes the industrial common view to develop and use the identification and resolution system of industrial internet healthy and sustainability, to achieve the tremendous economic benefits that the industrial internet offers.

References

[1] DOLEZEL D, MCLEOD A. Managing Security Risk Modeling the Root Causes of Data Breaches [J]. Health Care Manager, 2019, 38(4): 322 – 330. DOI: 10.1097/HCM.0000000000000282

[2] HUANG K, KONG N. Research on Status of DNS Privacy [J]. Computer Engineering and Applications, 2018, 54(9): 28 – 36. DOI: 10.3778/j. issn. 1002-8331.1801-0101

[3] XU K, ZHAO Y D, CHEN W L, et al. Paradigm-Based Routing & Switching System for Data Interception Attacks [J]. 2017, 40 (7): 1649 – 1656. DOI: 10.11897/SP.J.1016.2017.01649

[4] DAI F F, Fan X H, CUI X F, et al. Analysis on Typical Application Architecture Security Risk and Countermeasures of Blockchain [J]. Information and Communications Technologies, 2018, 12(6): 51 – 59

[5] GROTHOFF C, WACHS M, ERMERT M, et al. Toward Secure Name Resolution on the Internet [J]. Computers & Security, 2018, 77: 694 – 708. DOI: 10.1016/j.cose.2018.01.018

[6] ZHENG Y W, WEN H, CHENG K, et al. A Survey of IoT Device Vulnerability Mining Techniques [J]. Journal of Cyber Security, 2019, 4(5): 61 – 73. DOI: 10.19363/J.cnki.cn10-1380/tn

[7] Standardization Administration of the People's Republic of China. Information Security Technology-Data Security Capability Maturity Model: GB/T37988-2019 [S]. 2019

Biographies

MA Baoluo received the B.S. and M.S. degrees in information and communication engineering from Xinjiang University, China in 2013 and 2016 respectively. He is currently a researcher of Institute of industrial Internet and Internet of things, the China Academy of Information and Communications Technology. His research interests mainly include identification and resolution security of industrial Internet and network security. He has published severa papers in various journals and conferences in the field of industrial Internet and network security.

CHEN Wenqu received the Ph.D. degree in mechanical engineering from the University of Sheffield in 2015. She is currently a researcher of Institute of industrial Internet and Internet of things, the China Academy of Information and Communications Technology. Her research interests mainly include identification and resolution of the industrial Internet, digital manufacturing, and digital twin. She has published five papers in various journals and conferences.

CHI Cheng (chicheng@caict.ac.cn) received the B.S. degree in electronic information engineering from Nanjing University of Posts and Telecommunications, China in 2013, and M.S. degree in electronic technology from the University of Sheffield in 2016. He is currently a deputy director of Institute of industrial Internet and Internet of things currently, the China Academy of Information and Communications Technology. His research interests mainly include identification and resolution security of the industrial Internet, as well as industrial Internet architecture. He has published several white papers in the field of the industrial Internet.