Risk Analysis of Industrial Internet Identity System

TANG Kai
(ZTE Corporation, Shenzhen, Guangdong 518057, China)

Abstract: The risks of the current identity system represented by Domain Name System (DNS) and Object Identifier (OID) are studied. According to the characteristics of the industrial Internet Identity (III) system, four open ecosystem planes are divided, and a corresponding risk analysis view is established to analyze risks for various planes. This paper uses Isaiah Berlin's definition of liberty to more generally express the concept of security as positive rights and negative rights. In the risk analysis view, the target system is modeled from four dimensions: stakeholders, framework, architecture, and capability delivery. At last, three defensive lines are proposed to establish the identity credit system.

Keywords: industrial Internet; identity credit system; risk analysis view; right framework; security attribute

DOI: 10.12142/ZTECOM.202001007

http://kns.cnki.net/kcms/detail/34.1294.TN.20200316.1140.004.html, published online March 16, 2020

Manuscript received: 2019-12-10

Citation (IEEE Format): K. Tang, "Risk analysis of industrial internet identity system," *ZTE Communications*, vol. 18, no. 1, pp. 44 - 48, Mar. 2020. doi: 10.12142/ZTECOM.202001007.

1 Introduction

The traditional Internet identity system is based on Domain Name System (DNS) and Public Key Infrastructure (PKI) technologies, with which the Internet Corporation for Assigned Names and Numbers (ICANN)/Certificate Authority (CA) and other institutions maintain the Internet's root of trust and facilitate host-oriented addressing and authentication to meet the identity requirements of massive asymmetric web computing models. As the Internet economy penetrates into all areas of society, infrastructure maintainers and industry regulators have full credit to provide diversified identity endorsement capabilities without relying on the Internet's root of trust. For the sake of security and controllability, independent identity systems have been proposed in the industrial Internet field.

2 Risks of Traditional Industrial Identity Systems

Traditional industrial identity systems are dedicated identity systems for different industries. Object Identifier (OID) is a typical one, jointly proposed by International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) and International Telecommunications Union-Telecommunication Standardization Sector (ITU-T) [1]. An OID consists of identifier system, registration system and resolution system. Its resolution system makes use of the ubiquitous resolution capabilities of DNS.

As an important part of the Internet infrastructure, DNS is designed just like the Internet at the beginning, without security considerations, which has made it a main target and means for various network attacks, such as:

1) Distributed Denial of Service (DDoS) attacks against

DNS servers: including host exhaustion-based DNS query denial of service attacks and bandwidth exhaustion-based DNS reflector denial of service attacks (also known as DNS amplification attacks).

2) DNS hijacking against users: including DNS server address hijacking, hosts file hijacking, cache poisoning, Kaminsky cache poisoning, hacking DNS servers, etc.

Generally speaking, the traditional industrial identity systems have several risks as follows.

· Lack of authentication: Traditional DNS based industry identity systems need to be combined with other technologies to provide authentication capabilities. Due to the diversification of industry authentication scenarios, unified authentication mechanism cannot be specified from top design of the identity system.

· Lack of permission control: Finer-grained permission control is not available to meet the higher security requirements in some special scenarios.

· Lack of credible endorsement for identity: Authorized identity organizations do not have strong credit themselves, and often require third parties (such as regulatory authorities) to endorse in order to provide sufficient credit to the public and industry chain. However, the establishment and maturity of the identity credit system takes time.

· Interoperability risks with international roots: Not all root nodes of the identity system have backup in every country. Therefore, when interworking occurs, risks arise.

· Long authorization chain that leads to the dilution of credit: The superior nodes to inferior nodes lacks visibility and controllability from management to technology. As the authorization chain grows longer, the trust relationship weakens rapidly.

· Inadequate business admittance and certification: Lack of a mature certification standard and practice in the industry identity system is not conducive to the establishment of an identity credit system and long-term healthy development.

3 Ecosystem Planes of Industrial Internet Identity

In the 5G era, the Industrial Internet Identity (III) system is emerging with important meaning and rich connotation, covering all aspects of the industrial Internet in a broad sense. Its essence is an open identity system with a series of ecosystem characteristics. First of all, in an open Internet environment, the asset and value are the main characteristics of an identity ecosystem; secondly, the industrial Internet is based on the integration of Information Technology (IT) and Operational Technology (OT), and the identity has the characteristics of field and environmental relevance. The last, with strong industrialization, vertical regulation and control are often necessary.

In this paper, the III ecosystem is divided into four planes: the environment plane, service plane, asset plane, and business plane, according to [2]. As shown in **Fig. 1**, the III ecosystem combines new security characteristics at different planes to facilitate risk analysis.

4 Risk Analysis Process, View and Implementation

4.1 Risk Management Processes

In order to manage risks, each III ecosystem plane needs to support risk management processes, which are based on the ISO series of risk management guidelines, including risk analysis, risk evaluation, risk treatment, risk monitoring, etc. This article focuses on risk analysis (including risk identification).

ISO 31000: 2018 [3] and ISO 27005: 2018 [4] define general risk management guidelines and information security risk management guidelines, which can be used to guide the construction of a risk management system.

4.2 Building an III Oriented Risk Analysis View

The view of risk analysis is important for risk analysis and even risk management. As required by the principles in [3], risk management should be structured, comprehensive, customized and inclusive. It is necessary for III risk analysis to study the scope and open ecosystem characteristics of III system, conduct a comprehensive analysis based on a structured plane, and fully consider the demands of different stakeholders.

In order to analyze risks of different identity ecosystem planes, this paper builds a risk analysis view oriented to the characteristics of III system, based on mature methods and practice in the field of risk management and threat modeling. This is a more structured view of risk analysis for more logical processes and results (**Fig. 2**). The following is the analysis process with the proposed view.

1) Determining the scope and boundaries of the target system.

When using the risk analysis view, one first needs to determine the scope and boundaries of the target system and identi-

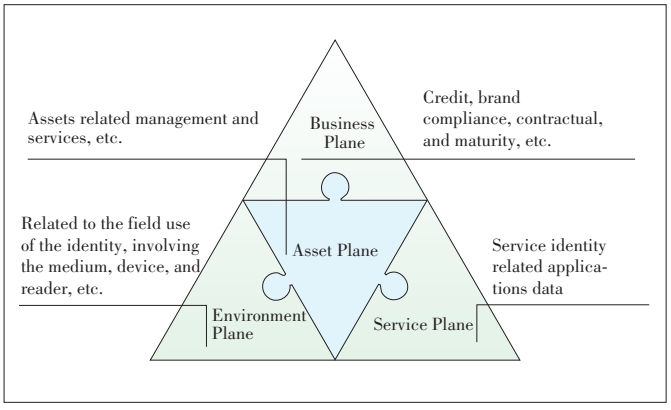
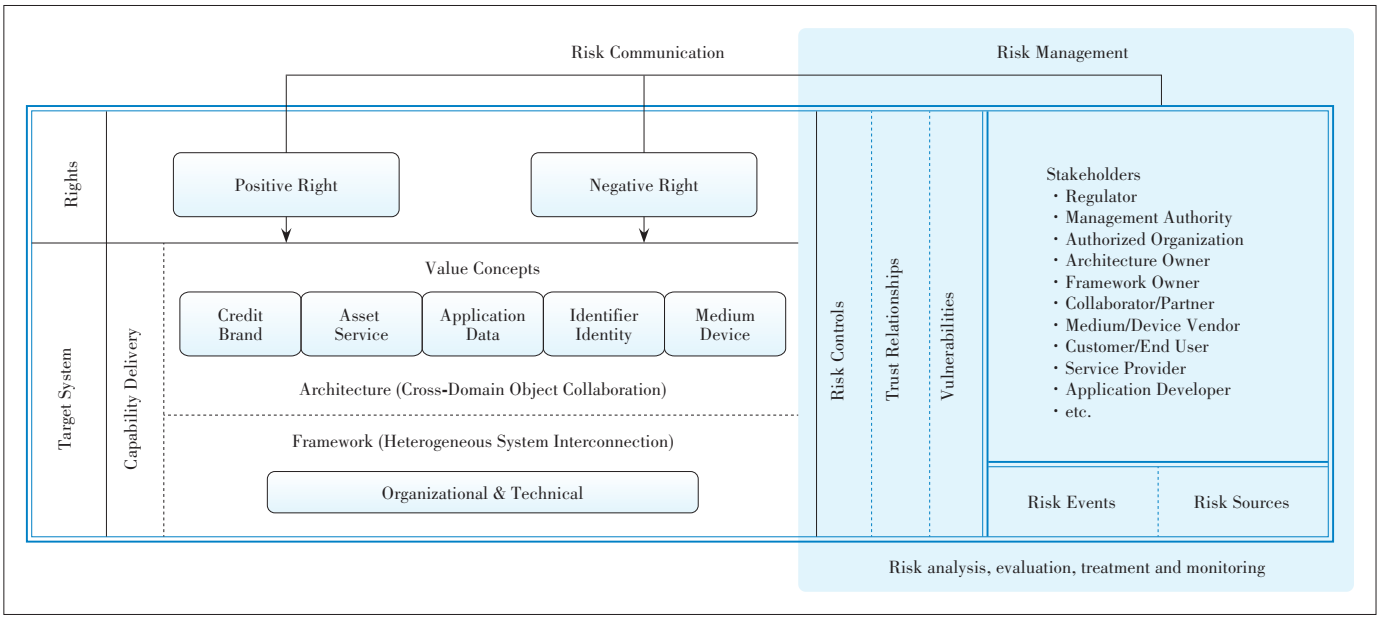


Figure 1. Industrial Internet Identity (III) ecosystem.



▲**Figure 2. Proposed view of the Industrial Internet Identity (III) risk analysis.**

fy III related objects. Different ecosystem planes have different scopes and objects. It is not appropriate to extend the scope and boundaries outside the III ecosystem. The main objects related to identity include identity related organizations and individuals, identified equipment or assets, various identity media such as Quick Response (QR) code, various basic identity services and auxiliary services, identifier and identity, various business information and data related to identity, etc.

2) Identifying stakeholders and right frameworks.

Isaiah Berlin has two definitions of the liberty: negative liberty and positive liberty [5]. Liberty is a sociological right, and security is a more general concept of rights. Here we use the definition of Isaiah Berlin to divide security into positive rights and negative rights. The right is closely related to the concept of stakeholders, and risk analysis always focuses on the rights of different stakeholders for different value concepts. Sometimes right is also treated as a security attribute.

The opposite of stakeholders is various sources of risks. They will use system vulnerabilities to launch attack events and bring risks to stakeholders.

Different ecosystem planes have different sets of right frameworks depending on the value concept of interest. For example, information security is mainly concerned with availability, confidentiality and integrity. Corresponding to security control, it is further expressed as Authentication, Authorization, Auditing (AAA) capabilities. This is also the theoretical basis of the six dimensions that Microsoft's Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege (STRIDE) threat model focuses on [6]. The privacy right that General Data Protection Regulation (GDPR) is concerned about is another type of right for human. Risk analysis requires more consideration of the sensitivity of different stakeholders to different rights.

The rights of different stakeholders may conflict, especially with the rights of regulators or decision makers. At this time, the use of a right framework can more clearly express this conflict relationship and help to form a balanced solution. In this process, risk communication is essential.

3) Reference industry mature practices.

After the above work is completed, mature reference models (attack models and abuse models) can be leveraged to conduct further risk analysis for capability delivery, object collaboration, and target system's framework, respectively. If required, further cuts can be made to the target system, with independent risk analysis for each subsystem.

Some examples of reference models are the Common Attack Pattern Enumeration and Classification (CAPEC) basis, DNS basis, cases of abuse based on traditional industry identification systems, and credit risk cases.

4) Analyzing the risks of capability delivery.

The goal of any system is to deliver some form of capability. Capability delivery risks are related to other risks of the target system, as well as to risks existing in the delivery process.

5) Analyzing the risks of object collaboration.

Security is the isomorph of the target system, the logical collaboration between objects is the foundation of the target system's capabilities and the basis to identify the value concepts. For different value concepts, objects have different types and different observation granularities, and need to be mapped to the corresponding stakeholders and right frameworks for further analysis. The risks of objects in different states and locations need to be fully considered, such as storage state, processing state, and transmission state.

The logic of the collaboration process between the objects is also subject to risks, which will bring risks to some types of value concept.

Object collaboration architecture needs to be mapped onto the target system's framework in order to achieve its basic functions. If the target system's framework does not provide the corresponding risk control or is not trusted, object collaboration architecture needs to implement risk control independently.

6) Analyzing the risks of the target system's framework.

The target system's framework includes organizational framework and technical framework, which is the physical foundation of object collaboration. For example, software is a technical framework component of digital object collaboration. The overall availability and integrity of the target system's framework is the primary consideration for risk analysis. The risks of the various components that constitute the target system's framework need to be considered as risks for another target system.

4.3 Risk Analysis Implementation and Risk Classification

This section adopts the above risk analysis view and combines the new security characteristics of various vertical industries proposed in [2] to carry out risk analysis on the four III ecosystem planes and obtain a risk list (**Table 1**). Due to the complexity of risks, this table only lists some important objects and value related risks.

5 Risk Control

Risk means uncertainty. Finding deterministic attacks and abuse patterns from these uncertainties is a long-term task for the security industry. Risks can be treated by multiple ways after risk evaluations. The trust framework is a positive assumption that exists among stakeholders. Stakeholders can ignore risks and reduce costs based on trust from each other. The more general way to treat risks is to implement risk control for the target system.

From the perspective of trust, the target system's framework, collaboration architecture, and capability delivery of the target system respectively reflect the characteristics of heterogeneous system interconnection and cross-domain collaboration. Risk analysis and control need to focus on the trust boundaries of these interconnections and collaborations.

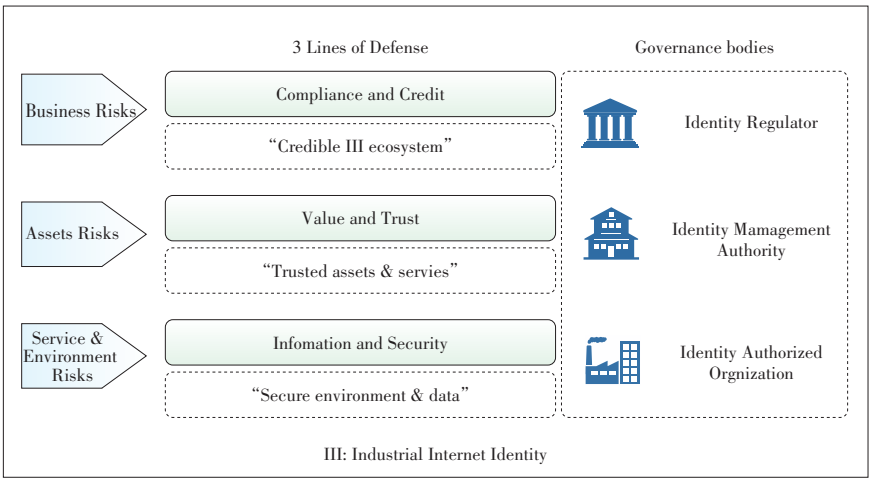
There are different types of risk control such as deterrent, preventative, detective, corrective, and restorative, based on three different dimensions: people, process, and technology. Risk control requires reference to mature standards, imple-

▼**Table 1. Examples of the Industrial Internet Identity (III) risks**

Ecosystem	Right Framework	Stakeholders	Examples of Vulnerability and Risks
Business plane	Credit, Brand Compliance, Contractual, Maturity	Identity regulator (IDR), Identity management authority (IDMA), Identity authorized organization (IDAO)	Lack of penetrating regulatory capacity Inappropriate regulation Falsify/delete/tamper with identity-related date to avoid regulatory responsibility Lack the ability to identity business operations Lack of control over agencies and authorized organizations Emergency response mechanism failed Identity spam Failure to use the Identity for the intended purpose and manner
Asset plane	Identity management service, Identity resolution service, Identity authentication service, Identified asset ownership, Administrator right, Income right, Right to use	IDR, IDMA, IDAO, Identity collaborator	Lack of long-term and continuous identity services operation Insufficient identity service performance and unresponsiveness Interoperability risks Lack of auditing for identity services Insufficient privacy protection for users of identity services Lack of sufficient strength for identity authentication Inadequate protection of ownership and administrative rights of identity, and easy to be misappropriated Improper use of identity and the disposal of income rights are prone to disputes Identity information and services that have been tampered with and redirected Supply chain collusion attack
Service plane	Identity application, Identity data availability, Confidentiality, Integrity	IDAO, Application developer, Partner, Customer, End user	Signaling storm brought by massive III related equipment Reliance on external identity services compromises low latency and high availability
Environment plane	Identity, Identifier, Medium, Device Confidentiality, Integrity, Fault tolerance, Efficiency, Manageability	IDAO, Device vendor, Medium vendor, End user	The identity medium lacks anti-fouling and error correction capabilities The identifier code can be maliciously modified The length and structure of the identifier affect the efficiency of field identification Low-power devices are difficult to achieve high-intensity authentication and encryption for identity related tasks Unmanned environment lacks field maintenance for identity security In an open environment, identity credentials and information can be stolen

mentation and deployment at different stages of the target system's lifecycle, and monitoring and management in accordance with the unified requirements of risk management.

Trust and control are parallel concepts and their relationship is of a supplementary character in generating confidence [7]. Trust can be established or strengthened in the process of continuous collaboration, but the trust relationship and risk control itself will also bring abuse risks to the system. Therefore, the target system needs to fully analyze and dynamically monitor the changes of the three.



▲**Figure 3. Three lines of III credit system.**

6 Building an Identity Credit System with Governance

The III system is an emerging technology system. In the short term, it is short of management and operation experience of ecosystem and also lacks mature governance and assessment standards, which will lead to the absence of admittance and regulation. Participants' capabilities are uneven, which is not conducive to the establishment of an identity credit system and long-term healthy evolution. Therefore, in the early stage of the III ecosystem, it is necessary to clarify governance responsibilities, and build three risk control defense lines with regulation as the core: the identity authorized organization line of defense, the identity management authority line of defense, and the identity regulator line of defense (**Fig. 3**). In the course of continuous operational practice, various incentive mechanisms should be implemented to strengthen the credit of the III system.

The risk governance of the III system should not be limited to the risks associated with the identity business identified in this paper, but should be based on a series of comprehensive organizational governance such as compliance of regulations, corporate governance, IT and information security governance, and field and personnel security governance. III-related risk governance need to be integrated into the basic activities of organizational governance.

Because the governance of the III system is often cross domain and organization, unified standards and specifications will be a very important part.

7 Conclusions

The III system needs to strengthen the awareness of comprehensive risk management. Through the introduction of a systematic risk analysis view, it comprehensively identifies various risk factors and establishes corresponding governance systems and standards. With the continuous enrichment of industrial Internet applications, various new technologies and scenarios including 5G, blockchain, and OLE for Process Control Unified Architecture (OPC UA) plus Time Sensitive Networking (TSN) will continue to emerge, which will pose new challenges to the security of the III system, and simultaneously bring new opportunities.

References

[1] ITU-T. Information Technology—Procedures for the Operation of Object Identifier Registration Authorities: General Procedures and Top Arcs of the International Object Identifier Tree:X.660, Jul. 2011
[2] TANG Kai. New Characteristics and Countermeasures for Vertical Industries Security in 5G [J]. ZTE Technology Journal, 2019, 25(4): 50 – 55. DOI: 10.12142/ZTETJ.201904009
[3] ISO. 2018 Risk Management: ISO/TC 31000 [S]. 2018
[4] ISO/IEC. Information Technology—Security Techniques—Information Security Risk Management: ISO/IEC 27005 [S]. 2018
[5] SHOSTACK A. Threat Modeling: Designing for security [M]. Hoboken, USA: John Wiley&Sons, 2014
[6] BERLIN I. Liberty: Incorporating Four Essays on Liberty [M]. Oxford, UK: Oxford University Press, 2002
[7] DAS T K, TENG B S. Between Trust and Control: Developing Confidence in Partner Cooperation in Alliances [J]. Academy of Management Review, 1998, 23 (3): 491 – 512. DOI: 10.5465/amr.1998.926623

Biography

TANG Kai (tang.kai2@zte.com.cn) is a senior system architect of ZTE Corporation. He is also a member of the Security Technology Expert Committee and Blockchain Technology Expert Committee. He has been engaged in the research, architecture design and R & D management of 3G core network systems and IMS systems, as well as research and project incubation in the Internet of Things identity, blockchain and security. Currently, he focuses on solutions and new technology research in 5G security, the Internet of Things and its applications in vertical industries. He has participated in the writing of a number of Chinese national standards and proposed more than 10 patents of invention.