CFL Authentication System Solution in Field of Industrial Control Information Security

Chunling Du, Xiubin Fan, Jimin Liu and Huiqi Zhao

ABSTRACT

The paper firstly introduces the relationship between industrial control and national strategy, gives action comparisons among important countries in the fields of industrial control information security (ICIS), and points out the gap of China. It is urgent to study ICIS technology. Then it briefly describes the common industrial control topological structure and corresponding information security management system in China. It is apparent that the current technologies in China does not meet the significant characteristics of ICIS.

Based on this purpose, the Chen, Fan, and Lü (CFL) solution and security architecture Trusted Computing Base (TCB) about ICIS is presented for the first time. Then the basic typical technology and research basis of the TCB are recommended. Lastly, the advantages of CFL solution for ICIS are discussed.

1. INDUSTRIAL CONTROL AND NATIONAL STRATEGY

1.1 Premise of Implementing "Made in China 2025" Strategy

Industry 4.0 focuses on business network integration, networked manufacturing integration and value chain end-to-end digital integration, covering the software and hardware fields of industrial control[1]. "Made in China 2025" strategy has two prominent characteristics: one is the deep integration of informationization and industrialization, another is intelligent manufacturing. To achieve "Made in China
2025” strategy, Construction of industrial control must be started. Based on the importance of industrial control security(ICS), the following proposition is given.

**Proposition 1.** Construction of industrial control security is a necessary condition to achieve the “made in China 2025” strategy.

### 1.2 Action Comparisons of Industrial Control Security between Countries

With the extension of network attacks such as computer viruses and hackers from the open Internet to the closed industrial control network, especially affected by the "Stuxnet virus" incident of Iran's nuclear power plant in 2010, ICIS has gradually become the focus of governments around the world.

In order to ensure the information security of national infrastructure such as electric power, rail transit, water conservancy and petrochemical industry, US and other developed countries, have done a lot of research of ICIS in risk assessment, situational awareness, intrusion detection, attack response, active and passive defense and etc., including the formulation and release of ICIS strategy, the establishment of national laboratory, organization and development in related standards, guidelines and regulations[2], carried out a series of large-scale special plans to research and develop key technologies. Their research progress has been greatly advanced.

China's research of ICIS started late and showed the characteristics of point-like development and weak foundation. For example, research institutes are scattered and mostly alone. However, with the issuance of Document No. 451 of Ministry of Industry and Information Technology [2011], the research and standard-setting of ICS by domestic relevant industry organizations have been actively carried out. Besides, In the opinion of Yao Dong Tao et al and Xiaoshan Wang et al, ICIS current research on safety defense system is not simply a technical problem, but a comprehensive problem of social factors, management factors, laws and regulations and many other aspects[3-4].

Today, attribute of information security has changed significantly in network space. On the basis of industrial control, network space further combines information with physics, forming Cyber-Physical Systems(CPS), which makes the international competition of industry 4.0 more fiercely.

In view of these importance factors, we must sort out theories of ICIS, and develop new technology, so as to support the national strategy.

### 2. INDUSTRIAL CONTROL TOPOLOGY AND PROTECTION

#### 2.1 Industrial Control Logic and Different Layers of Protection

Based on literatures[5-6], industrial control logic level can be divided into four layers: Field Devices; Automatic Control; Supervisory Control and Production Management.

From ICS, emphasis should be placed on strengthening field devices and automatic control[7]. So far, the security management of industrial network is mainly embodied in the supervision and control layer. The shortcomings of this kind of monitoring are as follow: a slow response time; unsatisfactory process security; gradual authentication of equipment security; unsupported millisecond and high
frequency computing; unsupported 5G technology, and it ultimately unable to meet the needs for ICS. It is clear that such management is inconsistent with actual requirements.

2.2 Industry Control Topology and Different Layers of Protection

From industry control topology[8-11], the lack of security authentication of equipment and process is a common phenomenon in recent years. Especially when there is wireless or mobile device access in the industrial control site, the external threat is greater. For example, in the gas industry, Supervisory Control And Data Acquisition(SCADA) system is widely used in its Supervisory center for safety monitoring of production process. According to literature[12], the normal operation of industrial centralized management platform should be based on the premise of secure network communication, secure regional boundary and secure computing environment. In practice, fortress machines, industrial vulnerability scanning systems and encryption authentication devices are commonly used, but there are still problems. As far as the identity security authentication of fortress machine is concerned, it still needs to be realized by a third party. The measure of industrial control vulnerability scanning system is still passive defense measure; Encryption security authentication is also the third party to achieve; Therefore they are not flat certification.

Similarly, industries that cannot meet the above ICIS requirements are also reflected in the petrochemical industry[13], power generation industry[14] and Train Control industry[15-16].

From this series of analysis that no matter from industrial control logic level or industrial control field, it cannot meet the needs of timely response, process security, equipment security certification, millisecond and high frequency computing, 5G technology and ultimately system information security.

3. STATUS OF MANAGEMENT AND RISK ASSESSMENT IN ICIS

3.1 Status of Management System in ICIS

The field of industrial control is dominated by large group enterprises. According to the analysis of literature[17], the ICIS management system covers two major modules: information security technology and information security operation and maintenance. In terms of its information security technology module, it includes the following five layers: physical layer, network layer, system layer, application layer and terminal layer. Each level involves five major functions: identity authentication, access control, content security, monitoring and auditing, backup and recovery. From the above argumentation, it can be seen that its identity authentication is not planar authentication, its access control depends on firewall and fortress machine, and its content security and monitoring audit depend on passive defense. Similar ideas are also continued in the discrete manufacturing digital workshop security guarantee system of literature[18], the unified ICIS management system architecture of literature[6] and the information security product system of industrial control system.
3.2 Status of Industrial Control Fault management

Fault management of Industrial control adopts Failure Mode and Effects Analysis (FEMA) model, namely Failure Mode and consequence Analysis. On the basis of analysis, literature[7], it can be known that there are different types of industrial control faults from engineer station, operation station, control station and control network. Such as hardware resource exhaustion, network failure and blocking, forge/replay real-time data failure. These failures often endanger the following aspects: safety of industrial control in time, process safety, security of time millisecond and high frequency calculation; Other faults often endanger the industrial control authentication security, such as unauthorized operation fault, control instruction and control algorithm tamper fault, and the like.

3.3 Status of Risk Assessment in ICIS

The risk assessment of ICIS is generally guided by the technical specification of industrial control network security, focusing on checking whether the ICIS strategy can meet the requirements of safety monitoring and security protection under the isolation of internal and external network. From the analysis of the overall risk assessment process, it can be seen that[19], the implementation of the information security strategy of the field equipment layer still depends on the application level. Thus the same problem has not been solved yet.

4. REQUIREMENTS OF ICIS

Based on the above analysis, ICIS needs should be met:
(1) safety in time;
(2) process security;
(3) complanation certification;
(4) support 5G technology;
(5) millisecond safety;
(6) security support high frequency calculation;
(7) systematic information security.

Obviously, through the analysis at present, we can know that:
No matter from the perspective of topological structure, or ICIS management scheme, they cannot meet the significant characteristics of ICIS requirements. Therefore, we give the following CFL solution to meet the needs of ICIS.

5. CFL SOLUTION IN ICIS

5.1 Technical Architecture of CFL Solution

Through the use of CFL system to ensure the security of identity authentication; the use of BLP technology to achieve flexible control of various permissions; by using block chain to ensure the security of the systematic operation process, and CFL_BLP_BC_CCA model is eventually formed by integrating the Chinese hardware
cryptographic algorithms. Due to the built-in safety genes, the model and its series of products ensure the endogenous safety of the system and realize innate immunity. The model is autonomous, controllable, safe and reliable. It can be proved as safe, zero knowledge interaction, high availability and high credibility. On the basis of this model, we give the technical framework sketch of CFL solution as follows (Figure 1.), and abbreviations are shown in TABLE I.

![Figure 1. CFL Authentication System's Scheme TCB for ICIS.](image_url)

**TABLE I. ABBREVIATIONS MEANING (IN FIGURE 1).**

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Meaning</th>
<th>Abbreviation</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCB</td>
<td>Trusted Computing Base</td>
<td>BC</td>
<td>Block Chain</td>
</tr>
<tr>
<td>CFL</td>
<td>Identification based certificate authentication system</td>
<td>CCA</td>
<td>China Cryptography Algorithms</td>
</tr>
<tr>
<td>BLP</td>
<td>A hierarchical classification mandatory access control technology</td>
<td>SG_CFL_UKey</td>
<td>Second Generation CFL UKey</td>
</tr>
</tbody>
</table>

5.2 Industrial Control Trusted Computing Base (ICTCB)

ICTCB, namely CFL_BLP_BC_CCA model, consists of four parts:
(1) CFL authentication system

CFL is an identity-based certification system. In the world's first cyberspace authentication theory[20] written by us, it is proved that authentication technology is the first technology of information security, and CFL is the authentication system...
satisfying the scientific logic of authentication theory. Based on Shannon information theory, it is strictly proved that parameter authentication including fingerprint, iris, face, password and identification does not have the function of information security authentication in essence. The existing functional authentication systems, such as public key infrastructure (PKI) and identity-based cryptography (IBC), have encountered serious bottlenecks. CFL authentication system, independent and controllable, with China's independent intellectual property rights, high security, high availability, high credibility, fully meet the protection of version 2.0 version of the above three levels of security requirements. It has been appraised as innovative system and "reaching international leading level" by several academicians and front-line experts from the party, government and army of China. The above CFL features can fully meet the significant characteristics of ICIS.

(2) BLP model

BLP model was proposed and perfected by D. Bell and J. LaPadula in 1973. It is widely used to describe the security problems of computer systems. BLP, the information system security technology of compulsory access control based on hierarchical classification, is essential technology for hierarchical protection above three levels. It belongs to the white list model of mathematic, modelling and systematization, provides the security protection at the operational level, and adds the hidden channel protection. It is a general technology, and it’s also the core of the high level secure operating system, security database, security network.

Based on BLP model and covert channel prevention, American scholars have developed information systems used by the US military. Chinese experts have also developed similar high-level information security systems, such as Kylin operating system. Their design principles are based on the whitelist mechanism of BLP model. However, in the form of theorem, literature[20] points out that the information security algorithm of pure software has no information security function in essence. Therefore, the security root and trusted root must be protected by hardware, and the white list must be locked by signature. literature[21] gives the CFL_BLP model and detailed safety operation rules. Based on SG_CFL_UKey, the trusted root and security root of industrial control can be guaranteed. Because of the decentralization and high security characteristics of CFL application, the CFL_BLP model is more usable, reliable, credible and controllable than the previous white list model based on BLP model.

BLP model implements the confidentiality of operations. In the world, Biba model[22] has been used to ensure general operational integrity. But in industrial control, we adopt the contemporary BC technology, block chain, to protect the integrity of operation. See literature[23].

(3) block chain (BC)

Nakamoto first proposed the concept of block chain in 2008. The design of block chain can ensure the communication security of trading order and make it difficult to forge. Its timestamp mechanism can ensure that the order of transactions is not changed. In addition, many nodes of P2P network keep unified transaction records throughout the network, which makes the electronic cash system run in a point-to-point environment and prevents double payment problems. As we all know, BC's payment feature is based on cryptography rather than credit, which enables any agreed parties to pay directly without the participation of third-party intermediaries (decentralization).
Because BC is decentralized, and CFL is precisely a decentralized authentication technology, which has the characteristics of application de-storage, and supports the authentication of secure process. Therefore, CFL can fully support the authentication in block chain to achieve the static and dynamic integrity of transaction records, and further provide the protection of the five aspects of information security (confidentiality, integrity, availability, controllability and authentication) of block chain. At the same time, CFL can achieve one person one private key, one certificate one key, high security degree of root, support hierarchical classification mandatory access control.

The research on CFL and block chain is referred to literature[23].

(4) China cryptography algorithms(CCA)

CCA is a hardware-based Chinese cryptography algorithm, including physical noise source, Chinese hardware symmetric cryptography algorithm, Chinese hardware public key cryptography algorithm, Chinese hardware digest algorithm, etc.

From literature[23], literature[21] and literature[20], we integrated BLP, BC and Chinese hardware cryptography algorithm with CFL to form CFL_BLP_BC_CCA model.

CFL_BLP_BC_CCA model constitutes TCB of industrial control security. From literature[20], the model has built-in security genes, endogenous security, innate immunity, active defense, high availability and high credibility.

5.3 Implementation Technology of TCB industrial control security

In the CFL solution of ICIS, the specific implementation technology of TCB involves nine aspects (Figure 1.). The most basic typical technologies are:

(1) SG_CFL_UKey technology

SG_CFL_UKey technology can be used for PC, mobile terminal, embedded and so on. The implementation of this technology conforms to the strong security of CFL theory and patents. The device can prevent internal ghosts. See literature[24].

(2) SG_CFL_UKey client driver technology

The technology is SG_CFL_UKey safe and trusted operation technology. Based on CFL_BLP_BC_CCA model, the technology is fully applied to local file security management, security browser, security transmission, security cloud application, security trusted monitoring and audit, information security defense, security database and data warehouse, etc. Limited to space, the above-mentioned full application of a series of implementation technologies will not be described here.

The working basis of the above two typical technical researches:

Now the CFL team has developed pc-oriented FG_CFL_UKey, which is the first-generation CFL UKey. Based on this, FG_CFL_UKey client driver technology has also been developed. The two products are stable in performance, and have been applied in a number of projects such as the Belt and Road, army, cloud center and so on.

6. CONCLUSIONS

Proposition 2. CFL Authentication System's scheme meets the requirement of ICIS.
The major bases are as follows:

(1) meet timely security: CFL_BLP_BC_CCA Model Certification Procedure Centerless;
(2) meet process security: CFL_BLP_BC_CCA model can achieve process level with fine security granularity;
(3) meet planarization certification: CFL_BLP_BC_CCA model application does not need a third party;
(4) support 5G: CFL_BLP_BC_CCA model with high availability and high security;
(5) meet millisecond level security: CFL_BLP_BC_CCA model application has no center and calculation is fast;
(6) support high-frequency computing security: CFL_BLP_BC_CCA model application has no center and calculation is fast;
(7) meet systematic information security: CFL_BLP_BC_CCA model attribute.

REFERENCES