Research on the Capability Status of Industrial Internet Security Supervision Platform

Ying Huang[1(✉)], Xiayao Jin[2], Chengsheng Zhou[3], and Yiming Huang[2]

[1] China Academy of Information and Communications Technology (Jiangxi) Science and Technology Innovation Research Institute Co., Ltd., Nanchang 330096, China
huangying5@caict.ac.cn
[2] China Mobile (Hangzhou) Information Technology Co., Ltd., Hangzhou 311121, China
[3] Institute of Security, China Academy of Information and Communications Technology, Beijing 100191, China

Abstract. In order to fully grasp the capacity status of the industrial Internet security supervision platforms, gain a deep understanding of the deficiencies of current platforms, and point out the direction for regulatory agencies to further improve the platform's comprehensive capabilities, it is necessary to carry out research on the status of the industrial Internet security supervision platform. There-fore, this paper first formulates the main research method, which is mainly based on the self-assessment of the research objects and supplemented by score review correction. Secondly, this paper compiles a questionnaire about the capacity status based on the evaluation system of industrial Internet security supervision platforms. In addition, through the in-depth analysis of platform scores, this paper conducts research on status of these industrial Internet security supervision platforms in 19 different provinces, finds four major problems in platform capabilities. Finally, combined with the relevant policy requirements and the requirements of the regulatory agencies, the paper gives three suggestions on improving the platform capabilities, including strengthening the output of platform capabilities, establishing a sound notification and disposal mechanism, and building a special monitoring module.

Keywords: Industrial Internet · Cyber Security · Supervision Platform · Capacity Status

1 Instruction

The Industrial Internet is a new type of infrastructure, application model and industrial ecology that is deeply integrated with the new generation of information and communication technology and the industrial economy. Through the comprehensive connection of people, machines, things, systems, etc., a new network covering the entire industry chain and the entire value chain is built. The manufacturing and service system provides a way to realize the digital, networked, and intelligent development of industry and even industries, and is an important cornerstone of the fourth industrial revolution [1]. In

Y. Cao and X. Shao (Eds.): DIONE 2023, LNICST 515, pp. 167–180, 2025.
https://doi.org/10.1007/978-3-031-80713-8_12

recent years, the Industrial Internet has achieved rapid development in my country and has become an important foundation for promoting a manufacturing power and a network power. However, its open, cross-domain, and interconnected characteristics also make network security issues very prominent [2]. Without network security, there will be no national security [3]. Therefore, doing a good job in industrial Internet network security supervision is an important prerequisite and guarantee for the healthy and rapid development of the industrial Internet. According to the "Guiding Opinions of the State Council on Deepening the "Internet + Advanced Manufacturing Industry" and Developing the Industrial Internet" on "promoting the construction of security technical means, improving technical capabilities such as hidden danger investigation and attack discovery" [4] and "Industrial Internet + Safe Production The "Action Plan (2021–2023)" requires [5] that the construction of technical means for industrial Internet security supervision is an important task for strengthening the national industrial Internet security.

In this context, all localities have actively promoted the construction of industrial Internet security supervision platforms and achieved certain results. However, there are still no definite answers to such questions as the quantitative results of the specific effectiveness of each platform construction, what supervision capabilities the industrial Internet security supervision platform as a whole has initially possessed, and what shortcomings still exist. Therefore, in order to further grasp the status quo of industrial Internet security supervision platform capabilities, it is imminent to carry out research on the status quo of platform capabilities. This research work can discover the specific achievements and deficiencies in the construction and operation of the current industrial Internet security supervision platform, which is conducive to further summarizing the successful experience and failure lessons of platform construction, pointing out the direction for the next step to build or improve related platforms, and to strengthen the national industrial Internet security guarantee. It is of great significance to reduce the risk of industrial Internet network security.

In the early stage, Sun Limin and others proposed countermeasures from the technical level by analyzing the industrial Internet security risks under the new situation of intelligent manufacturing [6]; Covering the two scenarios of "in-factory" and "in-factory" [7]; Yang Jianing and others expounded on-line monitoring, honeypot simulation, network traffic analysis, and enterprise side detection from a technical perspective in the analysis of the core technology of industrial Internet security situational awareness. Needle and platform security monitoring five core technologies for industrial Internet security situation awareness [8]; the above research helps us understand the technical capabilities used in industrial Internet security monitoring. Li Jun and others conducted research on the construction and application of the evaluation index system for the industrial Internet platform, and proposed the basic principles for building the platform evaluation framework and index system [9]; Jin Xiayao, Huang Ying, Zhou Chengsheng and others researched and constructed a set of industrial Internet security supervision platform capability evaluation system can effectively evaluate platform capabilities from 12 dimensions in four aspects: function construction, coverage, operation services, and expansion capabilities [10]. The research on the status quo of platform capabilities provides specific indicators and evaluation methods that can be quantitatively and qualitatively analyzed.

2 Research Methods

Based on the self-assessment of the research object, verify the relevant score certification materials provided by the research object, review the self-evaluation score results, and communicate with the research object to adjust the self-evaluation results and confirm the final score results when necessary.

Research scope: Select 19 industrial Internet security supervision platforms located in different provinces to carry out capacity research. In this paper, the 19 platforms are represented by codes A−S.

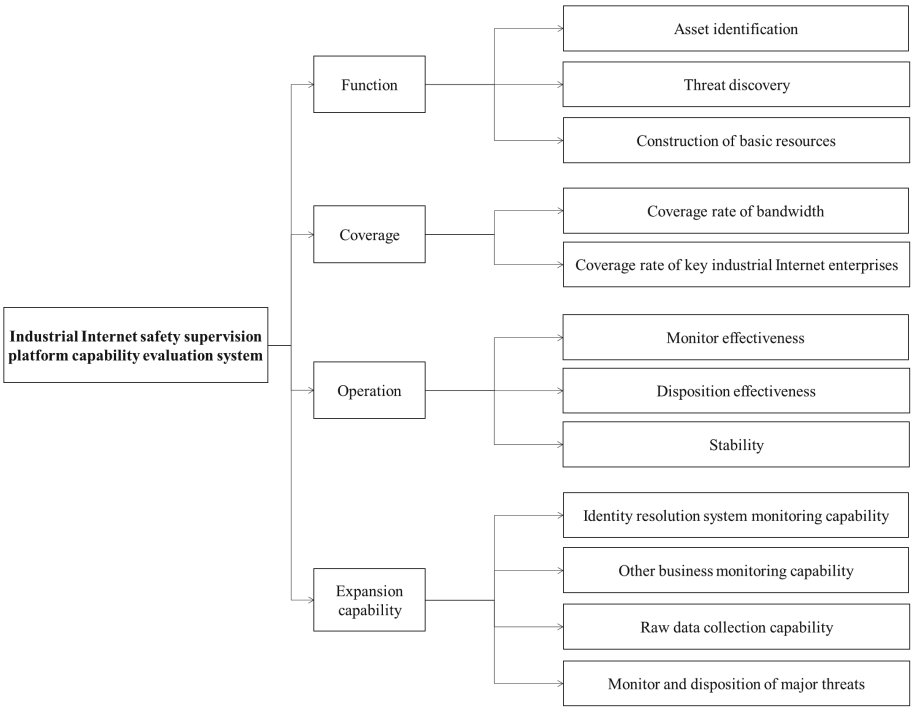

Fig. 1. The capability evaluation system of industrial Internet security supervision platform

Research content: Based on the capability evaluation system of industrial Internet security supervision platform, there are four first-level evaluation indicators, including function, coverage, operation, and expansion capability, and 12 s-level indicators [10], as shown in Fig. 1. Carry out capacity status research on 19 platforms within the research scope, and set up two parts: basic score (100 points) and additional score (20 points). Among them, the basic score mainly includes three first-level indicators such as function, coverage, and operation, focusing on the construction of basic functions such as platform asset identification and threat discover, monitoring and service effectiveness for local industrial internet enterprises, monitor and disposition effectiveness about the threats, etc.; The additional score are mainly evaluation indicators for platform expansion

capabilities, focusing on the security of identity resolution system, Internet of Vehicles system and other important business, and security data retention.

Research process: The research process is mainly divided into five steps:

1) Based on the index description and evaluation method content in the capability evaluation system of industrial Internet security supervision platforms [10], compile the "Industrial Internet Security Supervision Platform Capability Evaluation Questionnaire";
2) Through online communication, introduce the evaluation index system in the "Research on the Capacity Evaluation System of Industrial Internet Security Supervision Platforms" to the construction and operation units of 19 platforms, and explain the specific indicators and scoring methods; introduce the content and filling method of "Industrial Internet Security Supervision Platform Capability Evaluation Questionnaire";
3) The research object conducts self-evaluation according to the requirements, submits the self-evaluation results of the "Industrial Internet Security Supervision Platform Capability Evaluation Questionnaire", and provides certification materials as required;
4) Review the self-assessment results and certification materials, carry out necessary communication and confirmation of doubts, and make corresponding adjustments to the platform self-assessment scores as needed to obtain the final score;
5) Sort out the scoring results, analyze the status quo of the platform capabilities, find out the problems existing in the construction and operation of the platform, and give suggestions for the next step (Fig. 2).

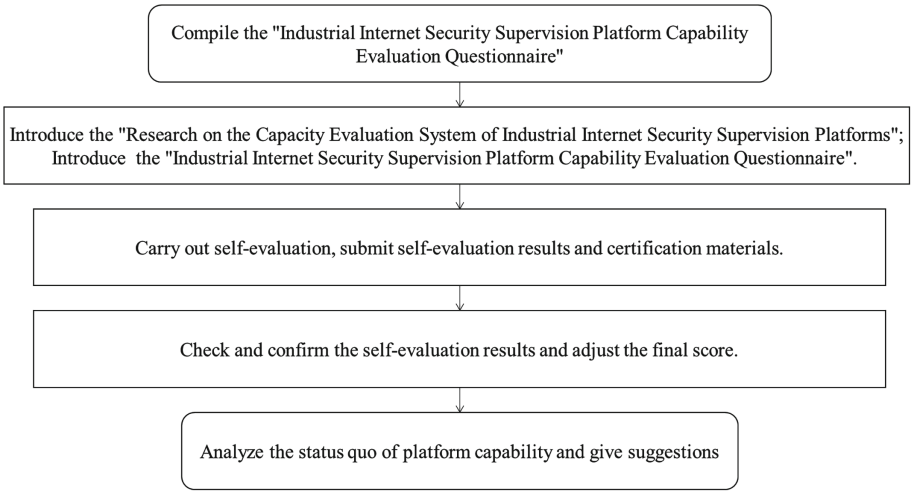

Fig. 2. Process of the research

3 Platform Capability Survey Results

According to the main research method of the research object self-assessment, supplemented by score review and correction, 19 platforms were carried out to investigate the status quo of platform capabilities, and the final investigation results were sorted out. The scores of various secondary indicators are shown in Table 1. Analyze from two dimensions of scores and scoring rate. The scores are used to comprehensively judge the overall capability of the platform, and the scoring rate is used to judge the specific achievement of various functional indicators of the platform.

3.1 Score

The analysis of score is divided into total score (including additional score) and basic score. The rankings of the total score and basic score of each platform are basically the same, and there is no major deviation.

1) Total score

The full score is 120 points, and the average score of 19 platforms is 84.95 points. Among them, 9 platforms scored above the average score, 10 platforms scored below the average score; 5 platforms scored over 100 points, and 5 platforms scored below 70 points. The total score is shown in Fig. 3 and specific score details are shown in Table 1 and Table 2.

2) Basic score

The full score is 100 points, and the average score of 19 platforms is 72.95 points. Among them, 10 platforms scored above the average score, 9 platforms scored below the average score; 5 platforms scored over 90 points, and 5 platforms scored below 60 points. The basic score is shown in Fig. 4 and specific score details are shown in Table 1 and Table 2.

3.2 Scoring Rate

Formula for calculating the scoring rate of first-level indicators:

Scoring rate of first-level indicators = average score of first-level indicators/full score of first-level indicators × 100%

The average score of the first-level indicator is the average score of 19 platforms in first-level indicator. After calculation, the scoring rate of the first-level indicator is 89% for the function indicator, 51% for the coverage indicator, 74% for the operation indicator, and 60% for the expansion capability indicator. The overall scoring rate is shown in Fig. 5, and the scoring rates of each platform are shown in Table 3.

Formula for calculating the scoring rate of second-level indicators:

Scoring rate of second-level indicators = average score of second-level indicators/full score of second-level indicators × 100%

Table 1. Scores of second-level indicators

Platform code	Function			Coverage		Operation			Expansion capability			
	Asset identification	Threat discovery	Construction of basic resources	Coverage rate of bandwidth	Coverage rate of key industrial Internet enterprises	Monitor effectiveness	Disposition effectiveness	Stability	Identity resolution system monitoring capability	Other business monitoring capability	Raw data collection capability	Monitor and disposition of major threats
A	14	16	10	15	15	8	12	6	3	3	8	0
B	14	16	10	15	15	12	4	6	3	6	8	0
C	14	15	10	15	9	12	12	6	3	3	8	0
D	14	16	10	9	15	12	12	6	1	0	8	0
E	14	12	10	15	12	12	12	6	1	0	8	0
F	12	8	10	15	6	12	12	6	3	6	8	0
G	14	16	10	9	6	12	8	6	3	3	8	0
H	14	16	10	15	9	12	0	6	3	0	8	0
I	14	16	10	15	0	6	4	6	0	6	8	0
J	14	14	10	6	12	12	0	6	1	0	8	0
K	8	16	8	9	12	12	4	6	0	0	8	0
L	10	16	10	9	3	12	0	6	0	6	8	0
M	14	16	10	3	0	4	8	6	3	3	8	0
N	14	16	6	0	0	6	12	6	1	3	8	0
O	14	16	10	3	0	6	0	6	1	3	8	0
P	10	12	6	3	3	6	12	6	0	3	6	0
Q	6	14	8	6	3	4	4	6	0	6	8	0
R	14	16	6	0	0	12	0	6	1	0	8	0
S	2	12	2	3	6	6	12	6	0	0	8	0
Average score	**12.11**	**14.68**	**8.74**	**8.68**	**6.63**	**9.37**	**6.74**	**6.00**	**1.42**	**2.68**	**7.89**	**0.00**

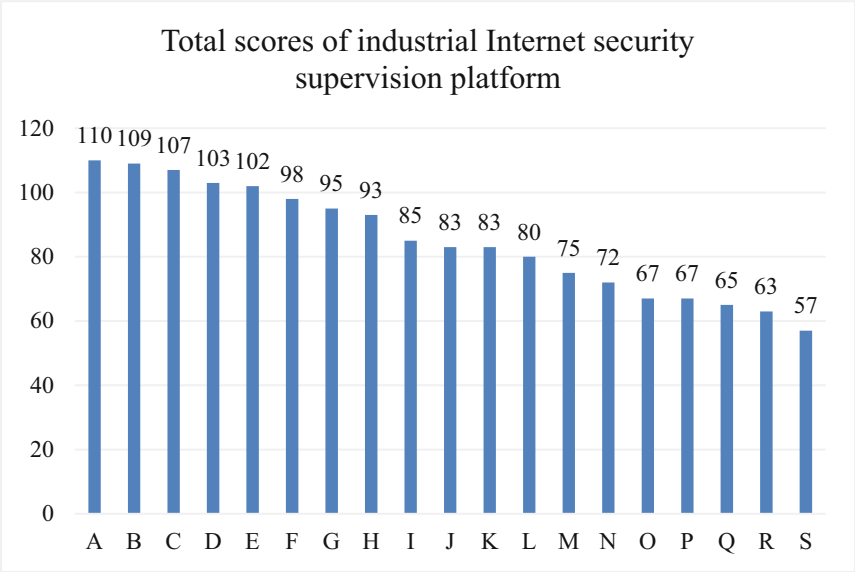

Fig. 3. Total scores of industrial Internet security supervision platform

The average score of the second-level indicator in this paper is the average score of 19 platforms in second-level indicator. After calculation, the scoring rate of the second-level indicator under function indicator is 86% for the asset identification indicator, 92% for the threat discovery indicator, 87% for the construction of basic resources indicator; The scoring rate of the second-level indicator under coverage indicator is 58% for the coverage rate of bandwidth indicator, 44% for the coverage rate of key industrial Internet enterprises indicator; The scoring rate of the second-level indicator under the operation indicator is 78% for the monitor effectiveness indicator, 56% for the disposition effectiveness indicator, 100% for the stability indicator; The scoring rate of the second-level indicator under the expansion capability indicator is 47% for the identity resolution system monitoring capability indicator, 45% for the other business monitoring capability indicator, 99% for the raw data collection capability indicator, 0% for the monitor and disposition of major threats indicator. Among them, major threat events are determined in accordance with the relevant requirements of the "Emergency response plan for public Internet security emergencies" [11]. The overall scoring rate is shown in Fig. 6, and the scoring rates of each platform are shown in Table 4.

Table 2. Scores of first-level indicators、basic score and total score

Platform code	Function	Coverage	Operation	Expansion capability	Basic score	Total score
A	40	30	26	14	96	110
B	40	30	22	17	92	109
C	39	24	30	14	93	107
D	40	24	30	9	94	103
E	36	27	30	9	93	102
F	30	21	30	17	81	98
G	40	15	26	14	81	95
H	40	24	18	11	82	93
I	40	15	16	14	71	85
J	38	18	18	9	74	83
K	32	21	22	8	75	83
L	36	12	18	14	66	80
M	40	3	18	14	61	75
N	36	0	24	12	60	72
O	40	3	12	12	55	67
P	28	6	24	9	58	67
Q	28	9	14	14	51	65
R	36	0	18	9	54	63
S	16	9	24	8	49	57
Average score	**35.53**	**15.32**	**22.11**	**12.00**	**72.95**	**84.95**

4 Analysis of the Status of Platform Capabilities

The basic function construction of Industrial Internet security supervision platform has reached the expected goal overall, the coverage needs to be improved, and the operation and expansion ability need to be further improved through the analysis of the score and scoring rate results of Industrial Internet security supervision platform. Based on the above analysis of the current situation, there are four main issues:

1) At this stage, the comprehensive capabilities of Industrial Internet security supervision platforms are varying considerably. About 26% of the platforms (the basic score is more than 90) can basically meet the regulatory business needs of collecting, monitoring, analyzing, reporting and disposing relevant data; About 26% of the platforms (the basic score is lower than 60) still cannot play a practical role in the daily work of Industrial Internet security supervision due to insufficient coverage, lack of notification and disposal mechanism and other reasons, even though their functions are well built.

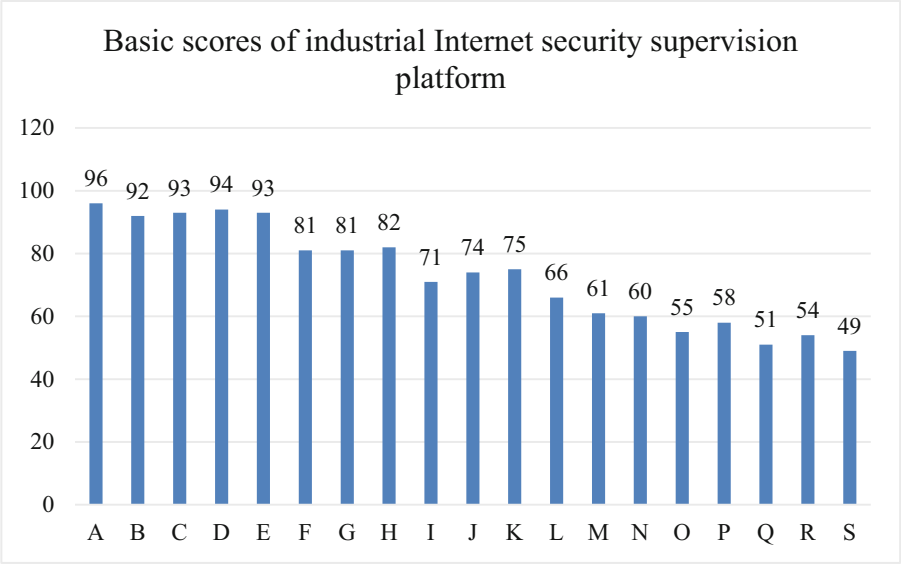

Fig. 4. Basic scores of industrial Internet security supervision platform

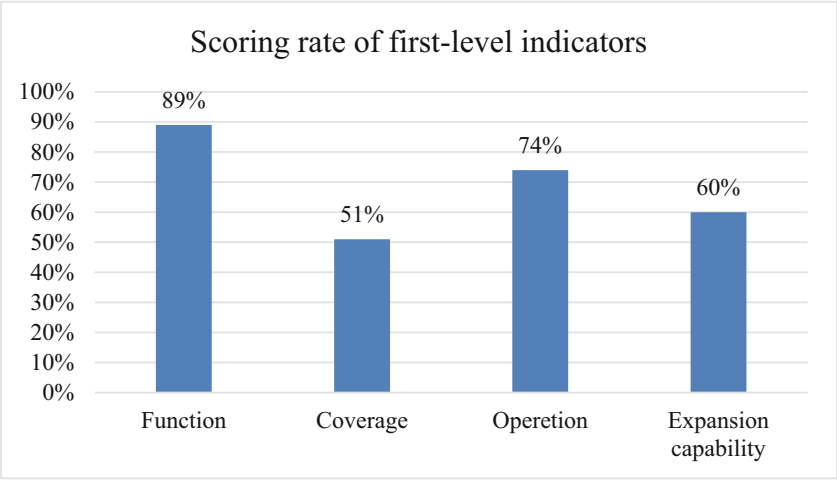

Fig. 5. Scoring rate of first-level indicators of industrial Internet security supervision platform

2) The platform's capacity building has basically met the standards, but the scope of capacity output needs to be strengthened. The scoring rate for function indicator is relatively high (89%). From the details of the scoring rate for each platform function indicator in Table 4, it can be shown that, except for a few platform functions that are not ideal, majority of platform functions are good. However, the scoring rate of

Table 3. Scoring rate of first-level indicators, basic score and total score

Platform code	Function	Coverage	Operation	Expansion capability	Basic score	Total score
A	100%	100%	87%	70%	96%	92%
B	100%	100%	73%	85%	92%	91%
C	98%	80%	100%	70%	93%	89%
D	100%	80%	100%	45%	94%	86%
E	90%	90%	100%	45%	93%	85%
F	75%	70%	100%	85%	81%	82%
G	100%	50%	87%	70%	81%	79%
H	100%	80%	60%	55%	82%	78%
I	100%	50%	53%	70%	71%	71%
J	95%	60%	60%	45%	74%	69%
K	80%	70%	73%	40%	75%	69%
L	90%	40%	60%	70%	66%	67%
M	100%	10%	60%	70%	61%	63%
N	90%	0%	80%	60%	60%	60%
O	100%	10%	40%	60%	55%	56%
P	70%	20%	80%	45%	58%	56%
Q	70%	30%	47%	70%	51%	54%
R	90%	0%	60%	45%	54%	53%
S	40%	30%	80%	40%	49%	48%
Average scoring rate	**89%**	**51%**	**74%**	**60%**	**73%**	**71%**

coverage(51%), operation(74%) and expansion capability (60%) are low, the bandwidth covered by the platform is not large, and the number of key Industrial Internet enterprises is insufficient, showing that the platform is powerful but nowhere to use.

3) The platform has good risk monitoring and discovery capabilities in cyber security, but the disposal closed-loop work still needs to be improved. The overall scoring rate of the monitor effectiveness in second-level indicator was 78%, and nearly 60% platforms get full scores in monitor effectiveness indicator, but the overall scoring rate of Disposition effectiveness indicator was only 56%, nearly 30% platforms get 0 in this indicator, and nearly 60% platform's scoring rate was not higher than 33%, indicating that the platform's daily operation work can basically monitor and discover the security risks of key Industrial Internet enterprises that have been covered, However, there is a lack of further notification and disposal measures for the identified security risks, resulting in the continued existence of security risks, which means that the security situation has been grasped but has not been effectively reduced.

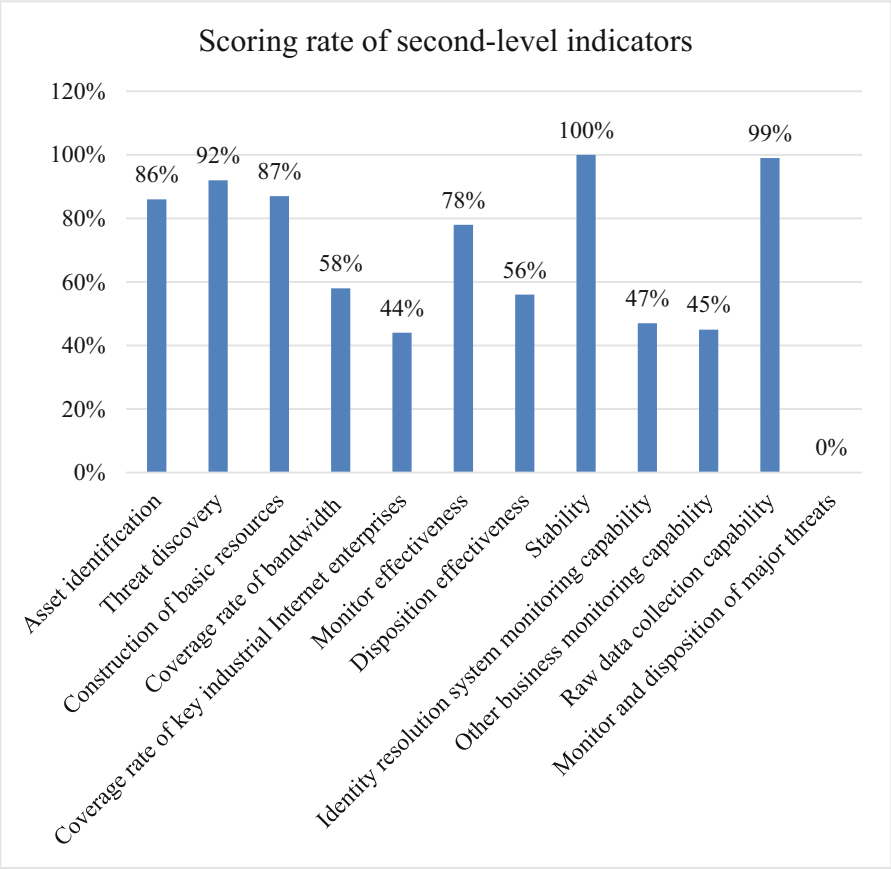

Fig. 6. Scoring rate of second-level indicators of industrial Internet security supervision platform

4) The platform can collect raw data, but lacks the ability of identity resolution system monitoring and other important business monitoring. The scoring rate of the platform's raw data collection capability is as high as 99%, with only one platform lacking in raw data collection capability, and the remaining 18 platforms getting full scores for raw data collection capability. However, the scoring rate of platform's identity resolution system monitoring capability (47%) and other business monitoring capability (45%) are relatively low, with over 50% platforms not establishing monitoring capabilities in relevant areas, such as identity resolution system, Internet of Vehicles, Internet of Things, etc.. It indicates that the platform has not fully explored the value of raw data collection and has not conducted in-depth thematic classification analysis on the raw data. Furthermore, when there is a need for relevant special supervision in the future, it may lead to a new approach to build a separate supervision platform, repeatedly collecting raw data, and causing resource waste.

Table 4. Scoring rate of second-level indicators

Platform code	Function			Coverage		Operation			Expansion capability			
	Asset identification	Threat discovery	Construction of basic resources	Coverage rate of bandwidth	Coverage rate of key industrial Internet enterprises	Monitor effectiveness	Disposition effectiveness	Stability	Identity resolution system monitoring capability	Other business monitoring capability	Raw data collection capability	Monitor and disposition of major threats
A	100%	100%	100%	100%	100%	67%	100%	100%	100%	50%	100%	0%
B	100%	100%	100%	100%	100%	100%	33%	100%	100%	100%	100%	0%
C	100%	94%	100%	100%	60%	100%	100%	100%	100%	50%	100%	0%
D	100%	100%	100%	60%	100%	100%	100%	100%	33%	0%	100%	0%
E	100%	75%	100%	100%	80%	100%	100%	100%	33%	0%	100%	0%
F	86%	50%	100%	100%	40%	100%	100%	100%	100%	100%	100%	0%
G	100%	100%	100%	60%	40%	100%	67%	100%	100%	50%	100%	0%
H	100%	100%	100%	100%	60%	100%	0%	100%	100%	0%	100%	0%
I	100%	100%	100%	100%	0%	50%	33%	100%	0%	100%	100%	0%
J	100%	88%	100%	40%	80%	100%	0%	100%	33%	0%	100%	0%
K	57%	100%	80%	60%	80%	100%	33%	100%	0%	0%	100%	0%
L	71%	100%	100%	60%	20%	100%	0%	100%	0%	100%	100%	0%
M	100%	100%	100%	20%	0%	33%	67%	100%	100%	50%	100%	0%
N	100%	100%	60%	0%	0%	50%	100%	100%	33%	50%	100%	0%
O	100%	100%	100%	20%	0%	50%	0%	100%	33%	50%	100%	0%
P	71%	75%	60%	20%	20%	50%	100%	100%	0%	50%	75%	0%
Q	43%	88%	80%	40%	20%	33%	33%	100%	0%	100%	100%	0%
R	100%	100%	60%	0%	0%	100%	0%	100%	33%	0%	100%	0%
S	14%	75%	20%	20%	40%	50%	100%	100%	0%	0%	100%	0%
Average scoring rate	**86%**	**92%**	**87%**	**58%**	**44%**	**78%**	**56%**	**100%**	**47%**	**45%**	**99%**	**0%**

5 Suggestions for Platform Capabilities Building

To solve the four main problems found in the research on the Industrial Internet security supervision platform, three suggestions are put forward to improve the platform coverage, operation and expansion capabilities, as follows:

1) Further strengthen the security capability output of Industrial Internet security supervision platform. Accelerate network flow of key Industrial Internet enterprises, key information infrastructure and other key locations within the regulatory area of relevant units accessing to the platform, effectively output monitoring capabilities to key points, improve the coverage of Industrial Internet cyber security supervision, make up for the lack of enterprise cyber security capabilities, and continue to provide cyber security monitoring services.
2) Establish and improve the notification and disposal mechanism of Industrial Internet cyber security risks. In order to make sure that regulatory agencies can take further action on the risks, it is necessary to establish an effective mechanism for risks notification and disposal, form a closed-loop workflow for monitoring, analysis, notification and disposal, and effectively reduce the Industrial Internet cyber security risks.
3) Strengthen the construction of Industrial Internet related special monitoring capacity. Based on the good foundation of raw data collection capability, fully utilize existing data. Completing in data extraction, classification, analysis, and utilization; establish regulatory special modules on the platform related to identity resolution system, Internet of Vehicles, Internet of Things, etc., effectively expanding the application scope of platform capabilities.

References

1. Luo, X., Zhou, J.: 5G+Industrial Internet development status and prospects. China Radio **11**, 28–31 (2020)
2. Alliance of Industrial Internet. China industrial internet security situation report (2018). China Inf. Secur. (6), 62–65 (2019)
3. Xi, J.: There is no national security without cyber security. Informatization China Constr. **6**, 62–65 (2019)
4. Interpretation of the《Guiding Opinions on Deepening the Development of the Industrial Internet of "Internet +Advanced Manufacturing"》. Mech. Res. Appl. **30**(06), 222 (2017)
5. Interpretation of "Industrial Internet + Safe Production" Action Plan (2021–2023). China Plant Eng. (22), 1 (2020)
6. Sun, L., Pan, Z., Lv, S., et al.: Risk analysis and countermeasure design for Industrial Internet under the scenario of Intelligent. Inf. Commun. Technol. Policy **47**(08), 24–29 (2021)
7. Yang, J., Chen, K., Cao, K., et al.: The core technology analysis of industrial Internet security situational awareness. Cyberspace Secur. **10**(04), 61–66 (2019)
8. Chen, X., Cai, L., Fu, Q.: Industrial internet security monitoring and situational awareness platform solution. Inf. Technol. Stand. **09**, 33–36 (2019)
9. Li, J., Qiu, J., Yang, L., et al.: Construction and application of assessment index system for industrial internet platform. Forum Sci. Technol. China **12**, 70–86 (2018). https://doi.org/10.13580/j.cnki.fstc.2018.12.009

10. Jin, X., Huang, Y., Zhou, C.: Research on the capability evaluation system of industrial internet security supervision platform. Cyber Secur. Data Governance **41**(11), 72–77 (2022)
11. Ministry of Industry and Information Technology of the People's Republic of China issued 《Emergency response plan for public Internet security emergencies》. China Emerg. Manage. (11), 22–25 (2017)