工业互联网产业联盟
Alliance of Industrial Internet

Industrial Internet Security
工业互联网安全

Tao Yaodong PhD
Excutive-Chairman of Safety Group of AII
Deputy Chief Engineer of 360ESG

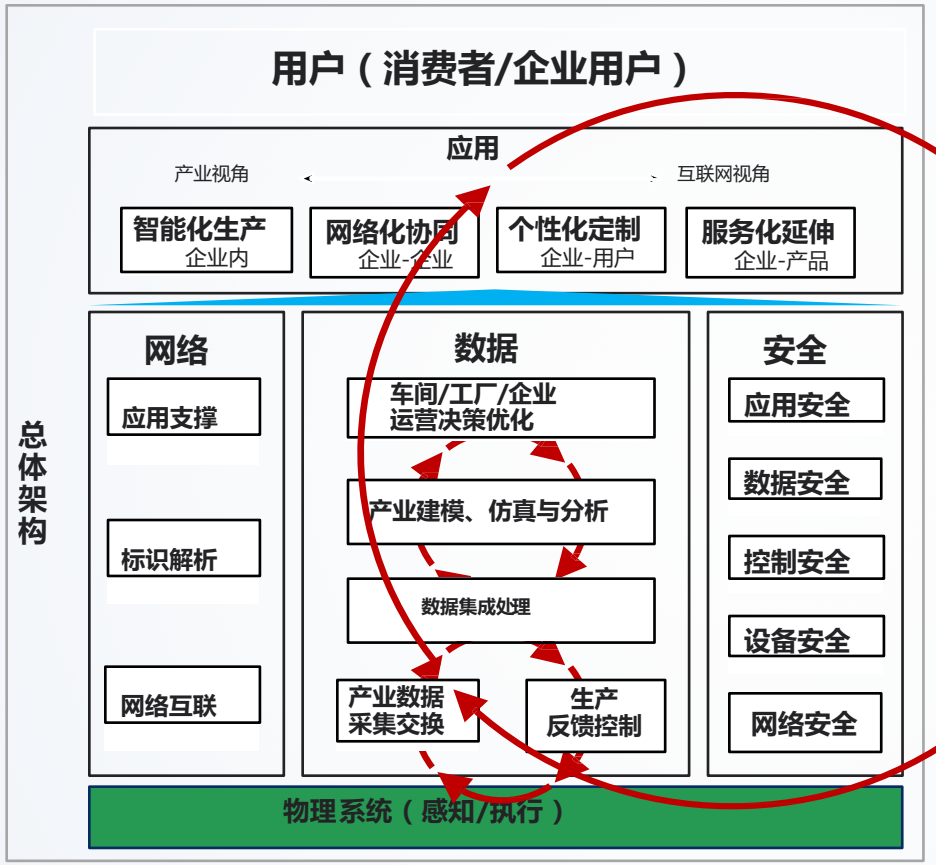
360 企业安全 安全第一™

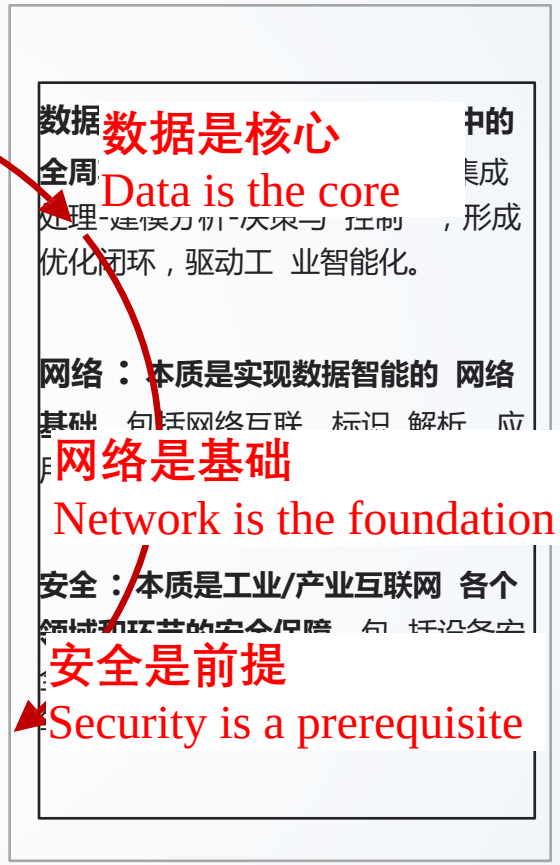
目 录
CONTENT

总体架构 China's Industrial Internet overall architecture

工业互联网产业联盟 Alliance of Industrial Internet

三大智能化闭环：智能生产控制、智能运营决策优化、消费需求与生产制造精确对接





中国的工业互联网= 工业网络（OT） + 工业关联的互联网（IT）

Chinese Industrial Internet = Industrial Internet of Things (OT) + Industry-Linked Internet (IT)

IT/OT一体化安全 / Industrial Internet IT/OT integrated security

工业互联网产业联盟 Alliance of Industrial Internet

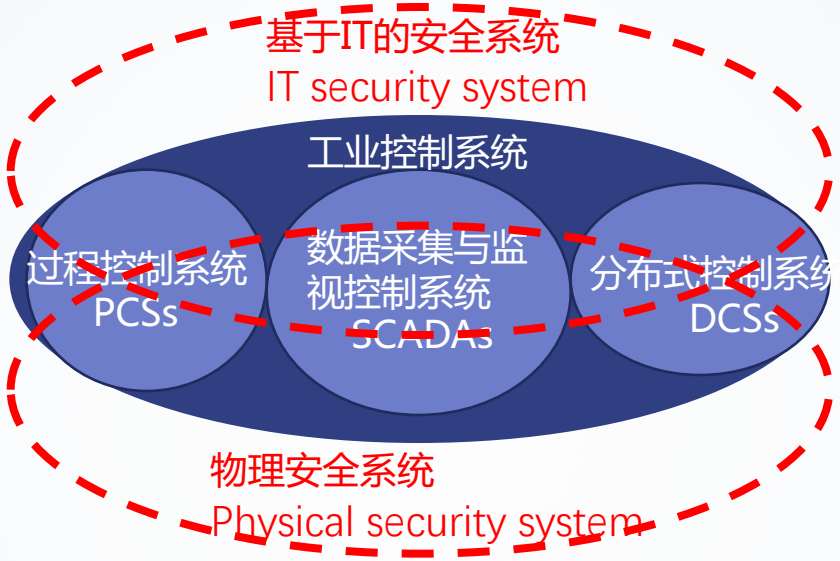
IT security: information-centric

IT管理是企业IT部门在IT系统运营阶段中在管理方面采用的方法论、手段、技术、制度、流程、文档的统称。

OT Security: Production-centric

是以下方面涉及的技术和实践：

1. 保护人、资产、信息
2. 监控和控制物理设备、过程、事件
3. 控制企业OT系统的状态变化



OT(Operational technology) as :
Hardware and Software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in asset-centric enterprises, particularly in production and opertions

OT Security is defined as :
the practices and technology used to protect people, assets and information involved in the monitoring and/or control of physical devices, processes and events.

工业互联网安全(Industrial Internet Security) = OT Security + IT Security

IT and OT is convergling in Industrial Internet developments

360 企业安全 安全第一™

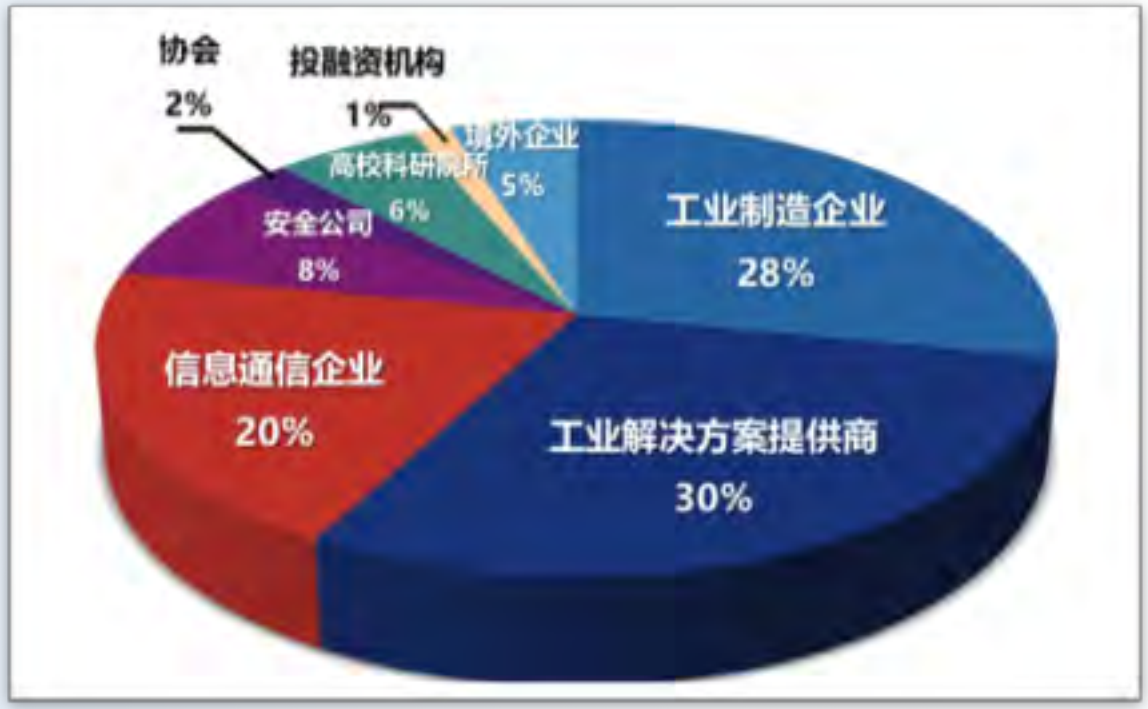
目 录
CONTENT

Security Companys in AII

工业互联网产业联盟
Alliance of Industrial Internet

At present, there are 834 formal member units :

- There are 1 Security Companies in the 15 vice chairman members.
- 65 enterprises of information security



About 8% of members is security enterprises in AII

No.	Chinaman Name	Logo
1	360	
2	CEC6	
3	6cloud	
4	ZTE	
5	CAICT	
6	ChinaMobile	
7	HuaWei	
8	SANY	
9	ChinaTele	

主要活动 Output and Activities of Security Group

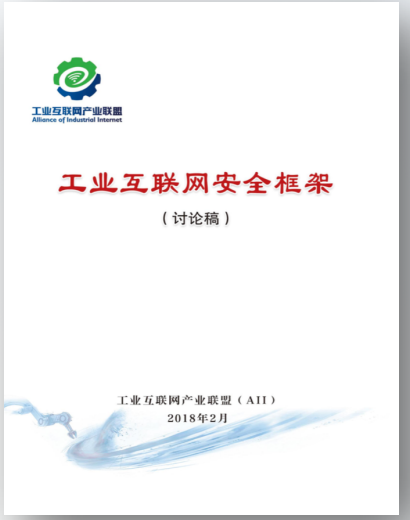
工业互联网产业联盟 Alliance of Industrial Internet

安全组主要的输出（Output of Security Group）：

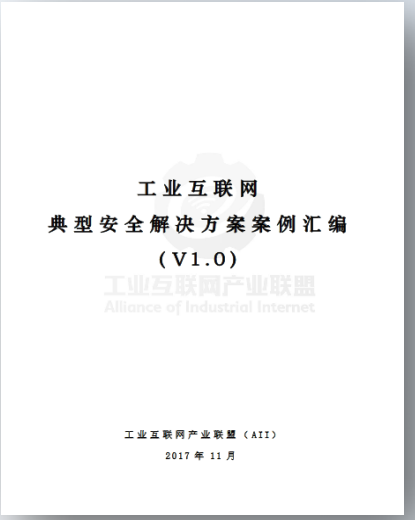
- 安全参考架构（Framework）
- 安全标准（Standards）
- 安全优秀案例评选（Typical Case）
- 安全测试床（Testbed）

主要活动形式（Activities of Security Group）：

- 全会（Annual Summit）
- 季度会议（Quarterly meeting）
- 沙龙(Security Salon）
- 安全大会（Internet Security Conference）
- 企业调研（the field study ）



Industrial Internet Security Framework



A typical case of industrial Internet security solution V2.0

Release a series of security reports

- Industrial Cloud Security Reference Solution
- Industrial Internet Security Situation Report of China
- Industrial Internet Typical Security Solutions

360企业安全 安全第一™

输出：参考框架 Output：Security Framework

工业互联网产业联盟 Alliance of Industrial Internet

2018年5月框架已同步征求美国工业互联网联盟IIC的意见

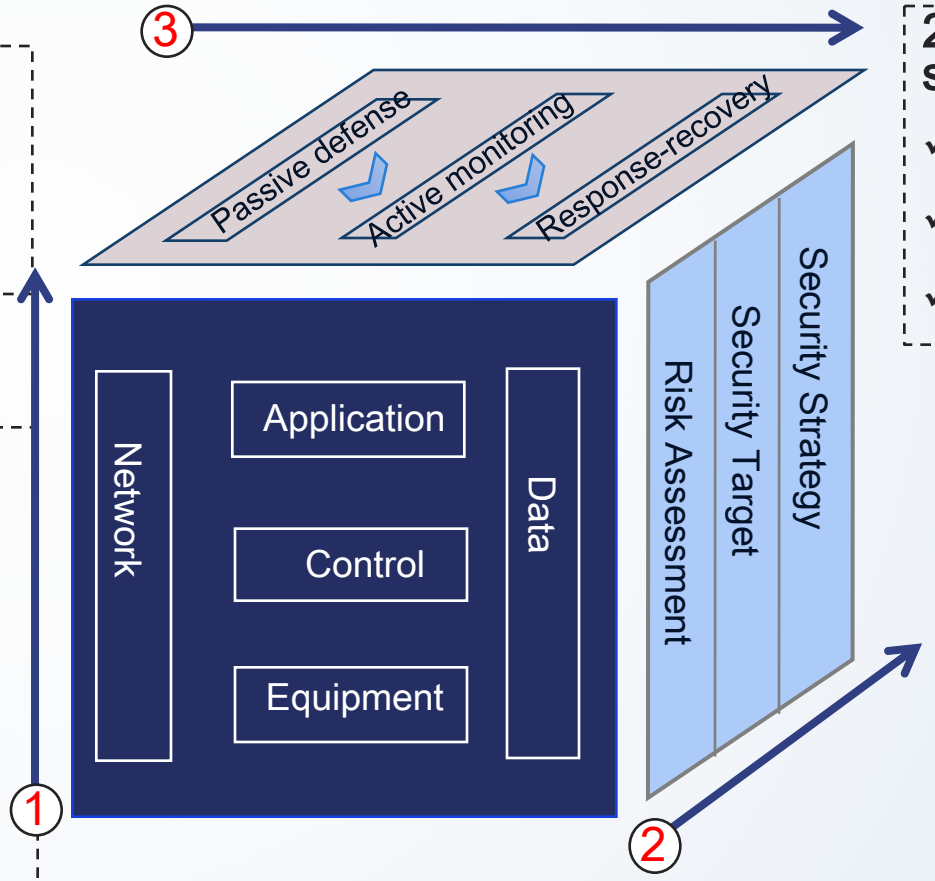
The framework has been seeking the advice of IIC

Security Framework

Establish the three dimensions security Framework covering object, measure, strategy three perspectives.

3.Measures
- ✓passive defense
- ✓active monitoring
- ✓response-recovery

1.Object
- ✓Equipment
- ✓Control
- ✓Application
- ✓Nework
- ✓Data



2.Protection strategy ：
- ✓Risk assessment
- ✓Security target
- ✓Security strategy

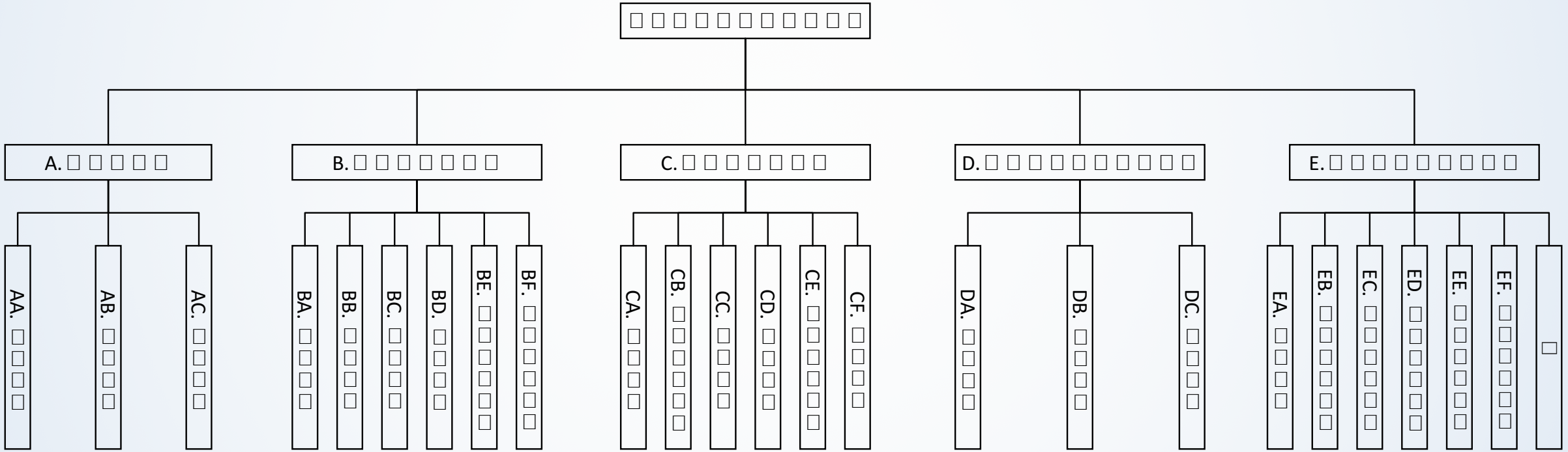
输出：标准体系 Security Standard Framework

工业互联网产业联盟 Alliance of Industrial Internet

The framework of industrial Internet security standard system is classified into 5 categories：

A： General Standard , B：Basic Common Standard, C：security Protection Standard,

D： Safety Management and Service Standard, E： Vertical field application domain standard



工业互联网安全标准体系框架包括“A总体类标准”、“B基础共性类标准”、“C安全防护类标准”、“D 安全管理与服务类标准”、“E 垂直领域应用领域类标准”五个部分。

360 企业安全 安全第一™

活动：峰会/季会/ Annual Summit/ Quartanly Meeting/Salon

工业互联网产业联盟 Alliance of Industrial Internet

特色活动——安全沙龙（ Featured Activities——Security Salon)

- **From the user‘s perspective，Invite** famous enterprises and users to share relevant Security applications, practices and experience
- CITIC Heavy Industries, Foxconn, SANY, 360ESG，VENUSTECH etc. have shared their experience and practices

Notice: MOXA, Honeywell and BYD will share their experience in security salon of Q4 at Shenzhen.

活动：ISC2018

Industrial Internet Security Forum of ISC

工业互联网产业联盟
Alliance of Industrial Internet

ISC is the largest and most influential annual cyber security event in the Asia-Pacific region. It has been successfully held for Six times since 2013, attracting more than 30,000 guests to attend, and more than 100 million people to watch the live show online each year.

Since 2016, the Industrial Internet Security Forum is one of the important sub forum of ISC conference，more than 400 participants each time

360企业安全 安全第一™

目 录
CONTENT

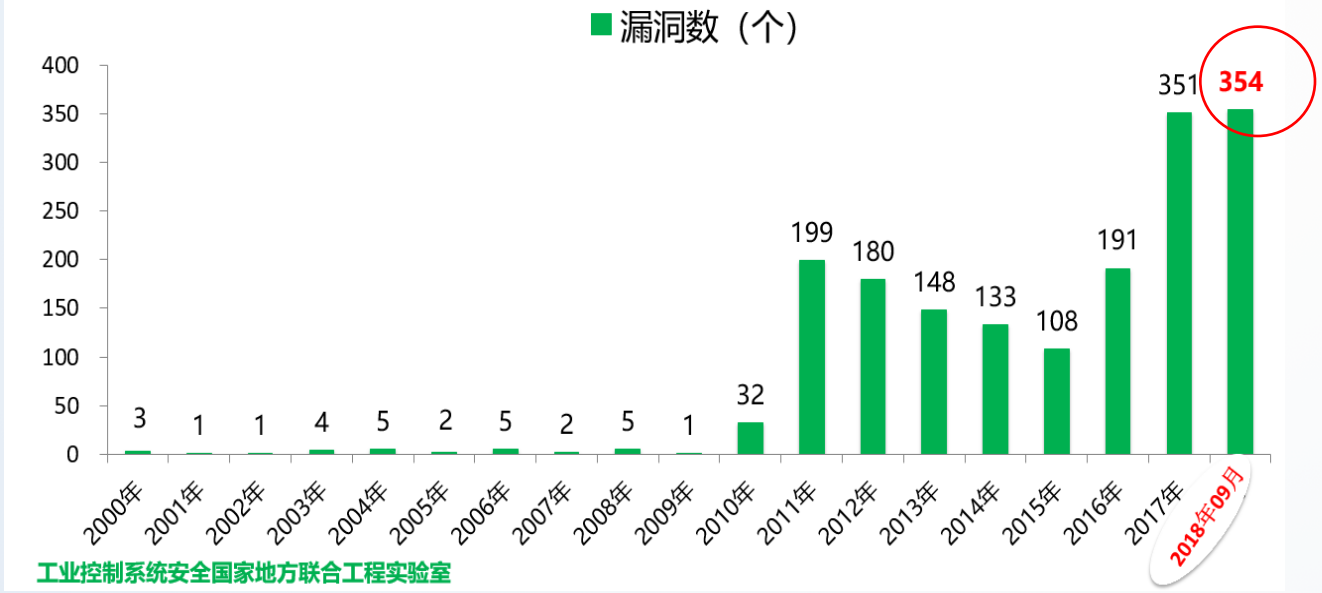
态势一：风险突出 Security vulnerabilities has increased rapidly in China

工业互联网产业联盟 Alliance of Industrial Internet

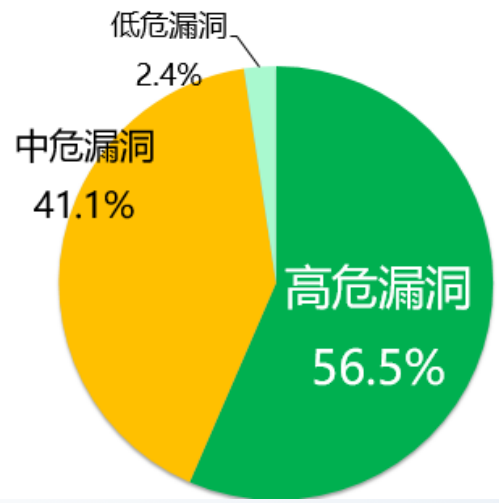
安全漏洞数量快速增长，高危漏洞呈高发态势，安全形式日益严峻

From January 2018 to September, CNVD added 354 Vulnerabilities about ICS, and more than 2017’ s total vulnerabilities. The high-risk vulnerabilities is 56.5%, accounting for the highest proportion. There are serious security risks in industrial control system. Once used, it will cause serious consequences.

CNVD工控新增漏洞年度曲线图



2018年工控系统行业漏洞危险等级饼状图



Source：360 ICS Lab

工业互联网安全风险突出，整体形式严峻

Industrial Internet security risks are prominent, and the overall situation is serious

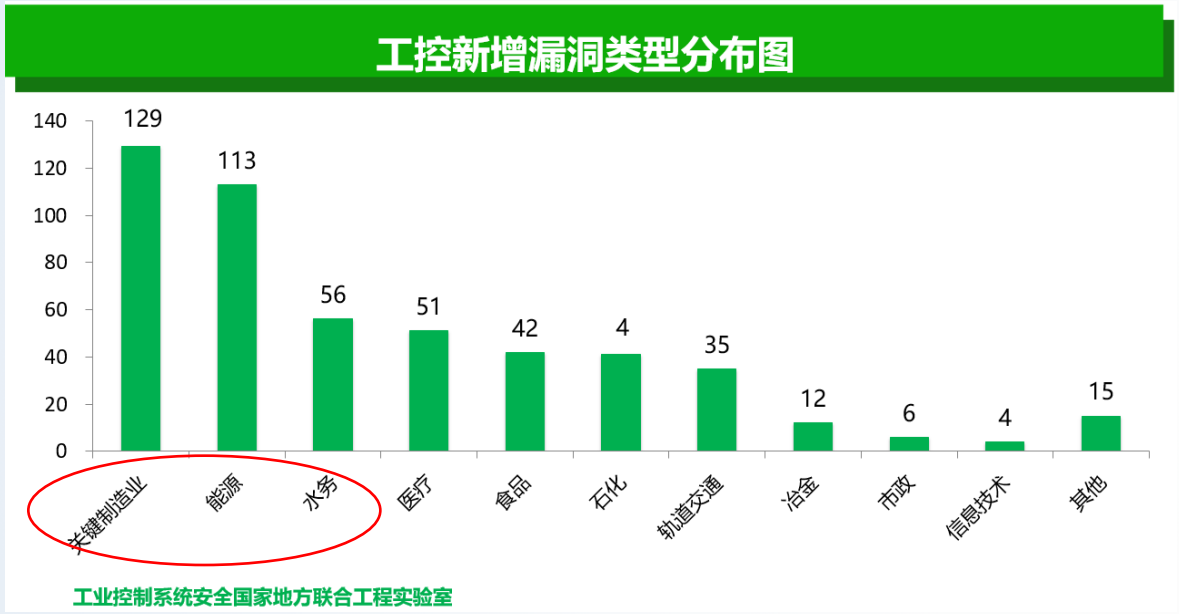
360 企业安全 安全第一™

态势一：风险突出 Vulnerabilities involve a wide range of industries

工业互联网产业联盟 Alliance of Industrial Internet

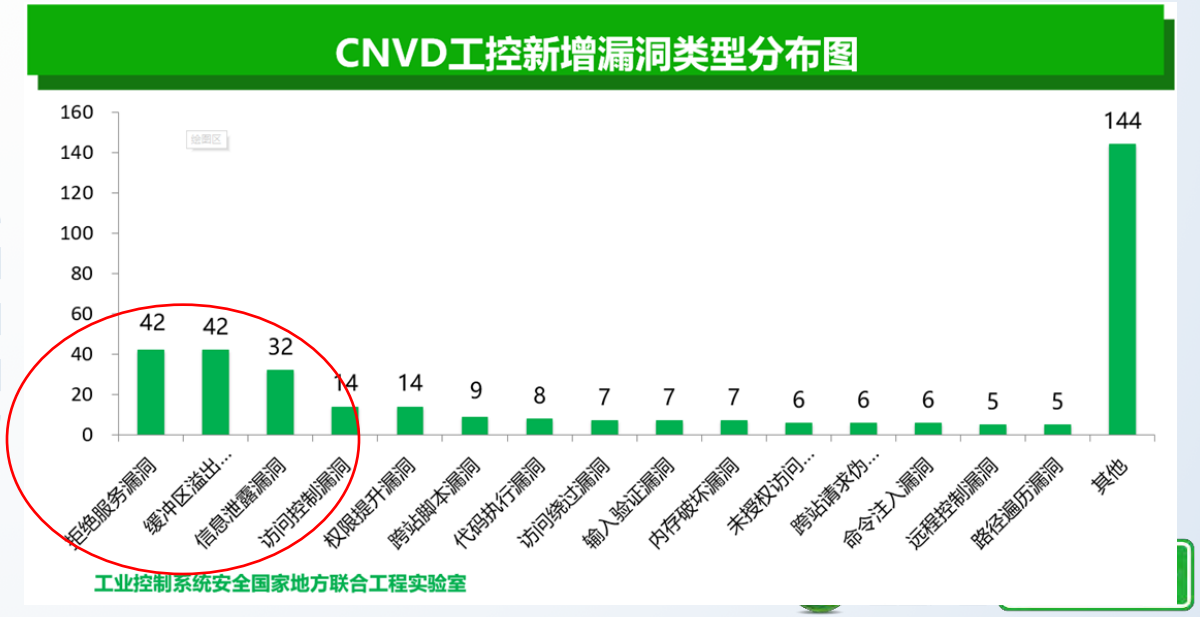
漏洞涉及行业广泛，且类型多样化特性明显

Vulnerabilities involve a wide range of industries, and the types of characteristics are obvious



- From January to September 2018, Vulnerabilities disclosed by CNVD were widely distributed in **Manufacturing, energy, water, medical** and other key industries
- the key **manufacturing industry** has more Vulnerabilities this year.

- Among industrial control vulnerabilities, Dos, Buffer overflow and Information leakage still account for a high proportion.



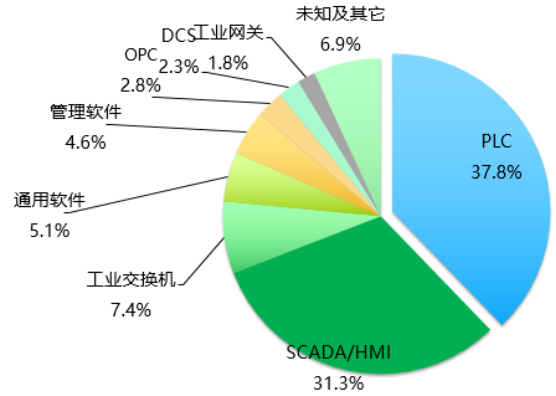
Source：360 ICS Lab’ s research report

态势一：风险突出 Vulnerabilities mainly come from international vendors

Vulnerabilities have the most PLC-related vulnerabilities, involving manufacturers based on international vendors （漏洞以PLC相关漏洞最多，涉及厂商以国际厂商为主）

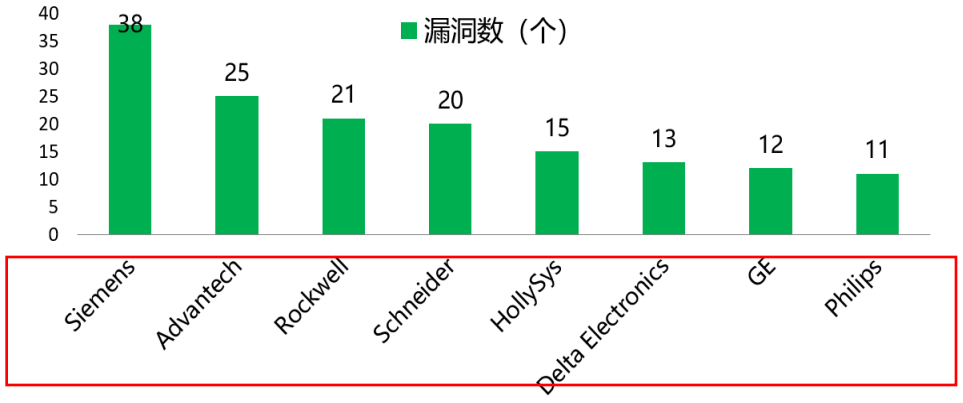
- 37.8% vulnerabilities is PLC- related
- 31.3% vulnerabilities is HMI/SCADA-related

工控漏洞设备类型分布图



工业控制系统安全国家地方联合工程实验室

CNVD工控漏洞所涉及的前八厂商



工业控制系统安全国家地方联合工程实验室

- From January 2018 to September, CNVD open industrial vulnerabilities

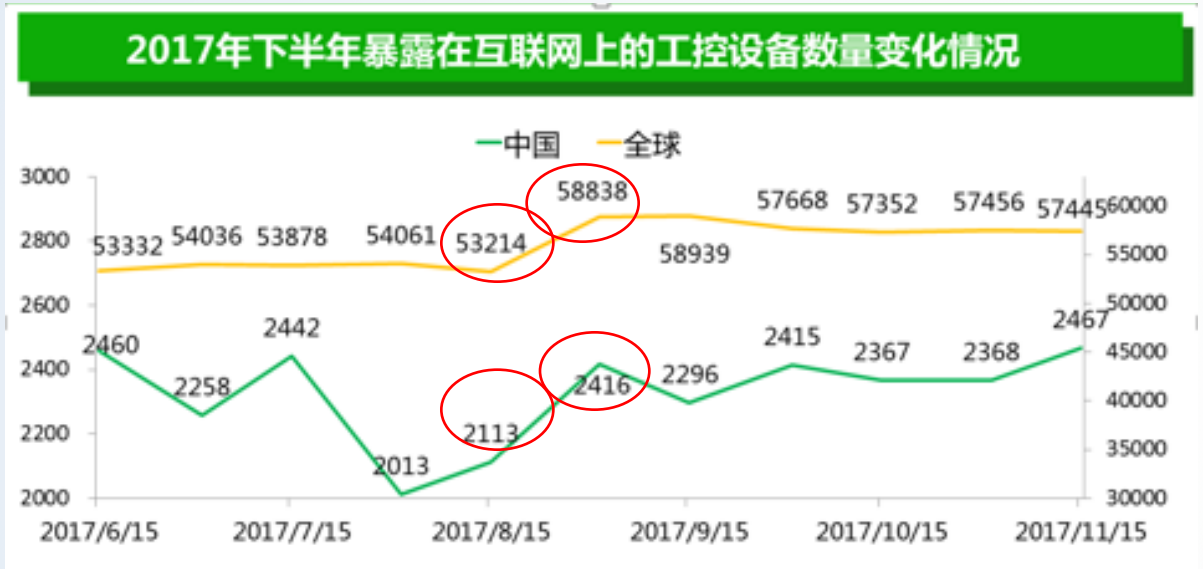
- The Top8 companies with Vulnerabilities are mainly international industrial control companies

Source：360 ICS Lab’ s research report

态势一：风险突出 Industrial Internet security risks prominent

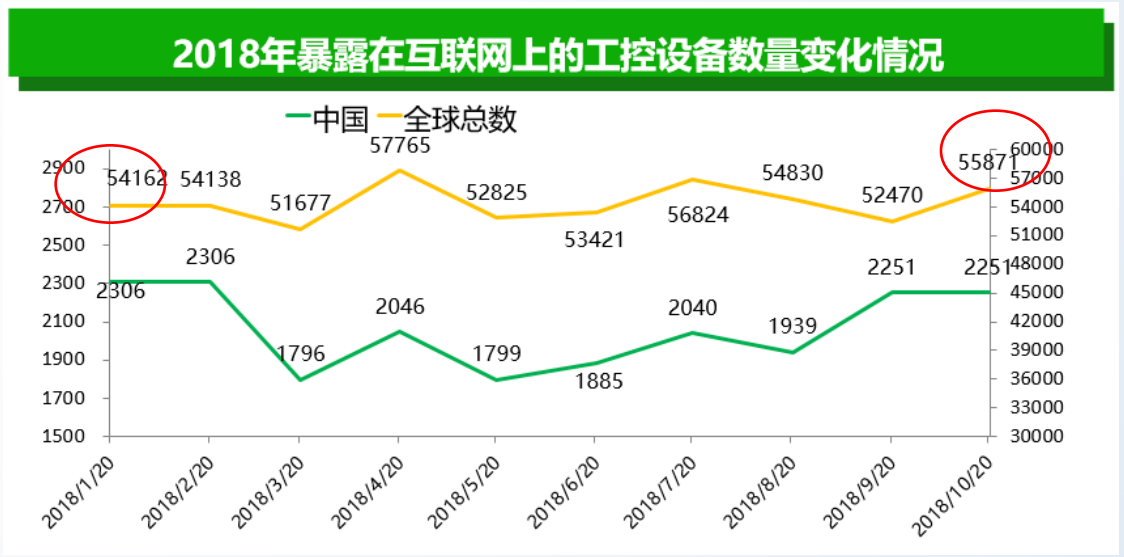
工业互联网产业联盟 Alliance of Industrial Internet

The number of ICS connected to Internet still huge and keep increasing
工控系统联网数量仍然庞大,并持续增长



- During August and mid-September 2017, there was a significant **upward trend** in the number of industrial control equipment exposed domestically and globally.

- From January to October 2018, the number of industrial control devices exposed to the Internet fluctuated and the overall form **increased**



Source：360 ICS Lab’ s research report

360 企业安全 安全第一™

态势二：事件频发 Wannacry attack on an Automobile company

工业互联网产业联盟 Alliance of Industrial Internet

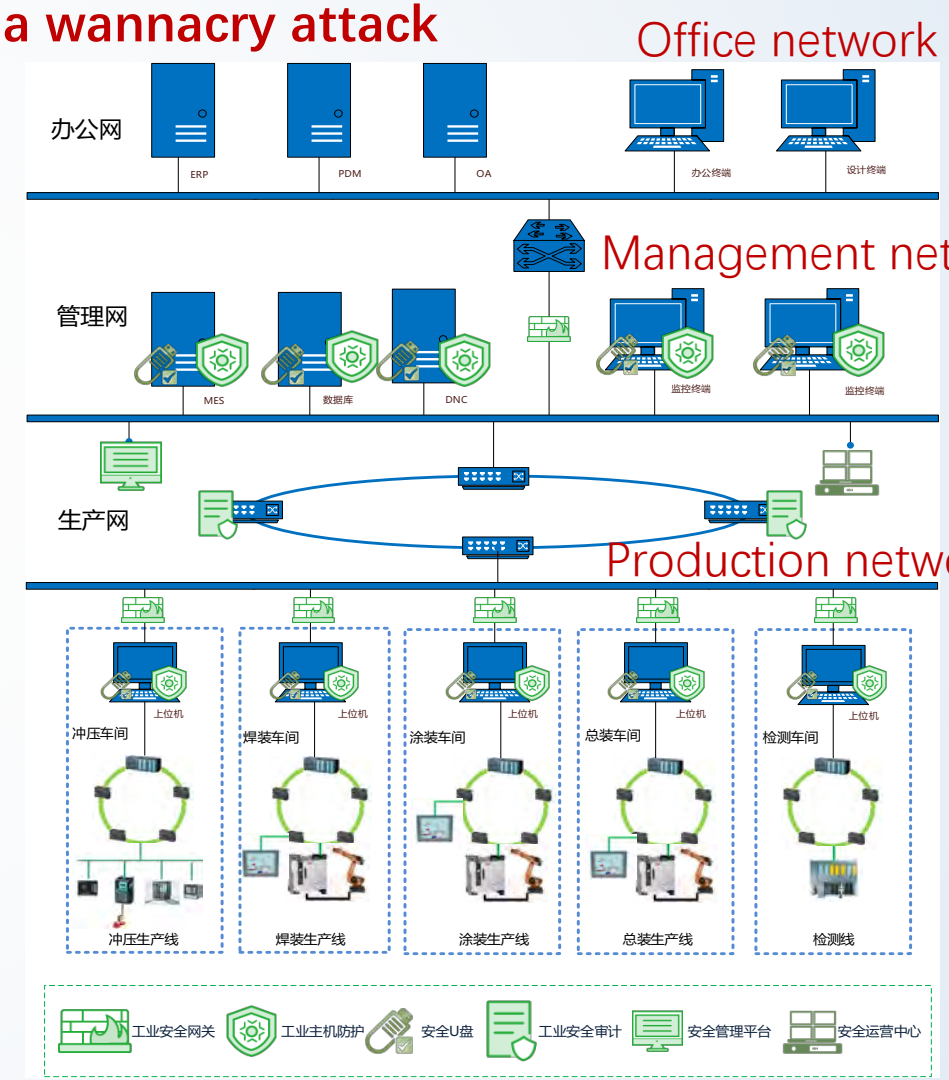
Case1：某汽车制造企业遭受病毒侵袭
An automobile manufacturing company suffers from a wannacry attack

Problem research

- Some industrial PC in the production lines frequently were halted in blue screen, and quickly spread to the entire production park, which forced the production line to stop production.
- Daily production value of more than 1 million, and the direct loss is serious.
- Production network（OT） is connected with the office network （IT）, without any security protection measures

Suggestions and measures

- Asset inventory and Network segmentation
- Deep defense，Endpoint protection is more than 10 thousand points
- IT/OT unified management
- Continuous monitoring response

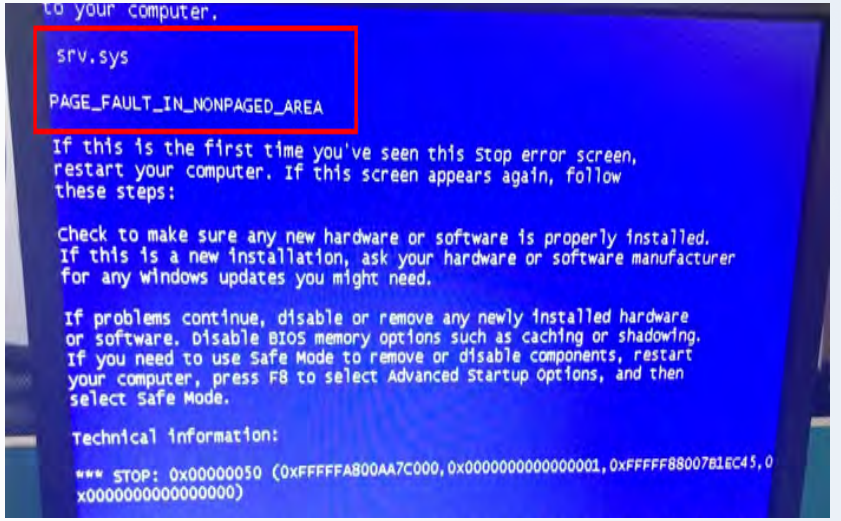


360 企业安全 安全第一™

Wannacry attack on an Automobile steel plate factory

Case2 ：某汽车钢板生产厂遭受永恒之蓝变种攻击

An automobile steel plate manufacturing factory suffers from a Eternal-blue variant attack



IT/OT status

- SCADA system consisting of 170 points including server and host computer. Six production lines consisting of different processes.
- There is no VLAN partition in OT network
- To facilitate maintenance, OT network set up ADSL for SI Servicer without any protection
- USB storage, personal notebook access to OT network without management

Emergency Response

- In September, the production line broke out for wannacry .
- Emergency disposal within 24 hours by 360ESG response team
- Follow up work, risk assessment, rectification

态势二：事件频发 Industrial Application Websystem needs great attention

工业互联网产业联盟 Alliance of Industrial Internet

Industrial Application websystem is defined as: the web system that monitors and/or controls physical devices, processes and management at enterprise, which usually connected to Internet with great many vulnerabilities。

Case 3：Some industrial application Websystem on public networks

360 企业安全 安全第一™

态势二：事件频发 Heating monitoring system can be attacked

工业互联网产业联盟 Alliance of Industrial Internet

■ 某热力集团有限公司（a heat-supply enterprise）

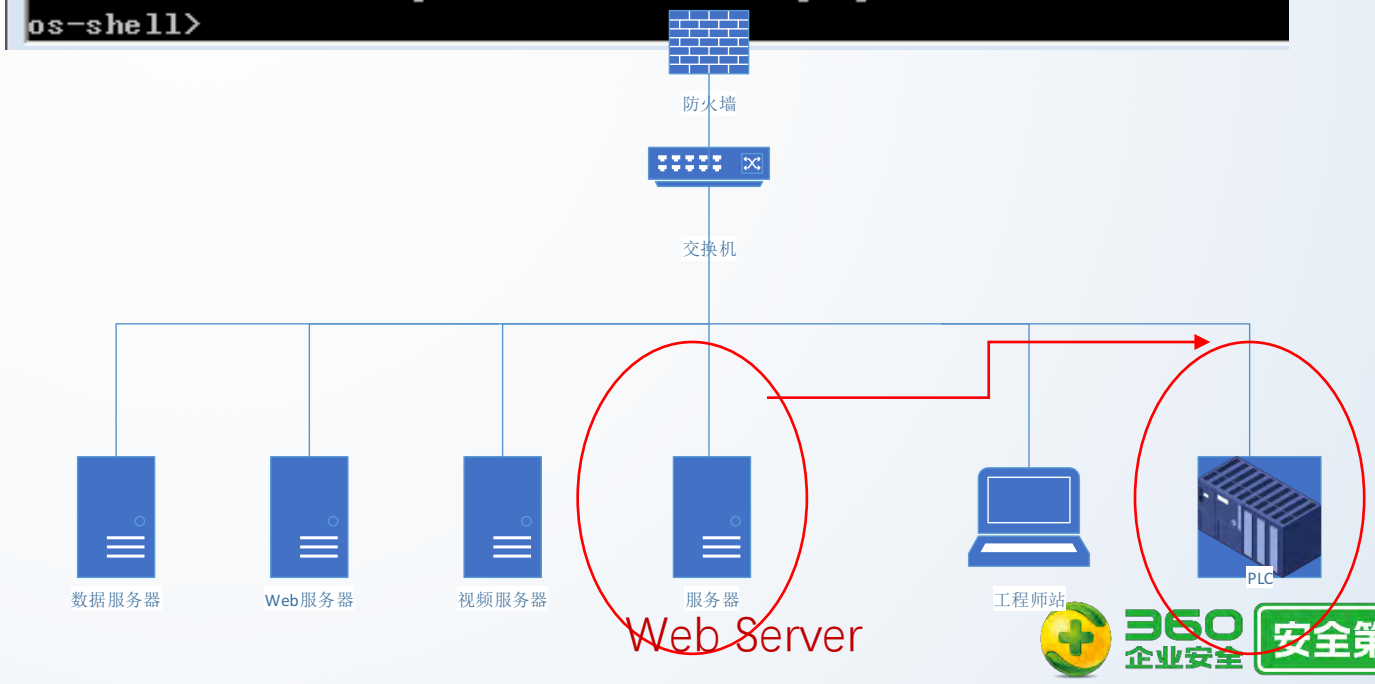
There is a weak password in the monitoring system of the heating network. It can be injected and get the shell.

The Hacker can directly control the PLC S7-300 to stop heating.

URL: http://221.*.*.* :9000/Publishing/Login.aspx

```
**********************************************************
IP:192.168.1.230  PORT:102  STATUS:open  SERVICE:S7
BANNER:{
        Copyright: Original Siemens Equipment
        PLC name: S7-300 station_1
        Module type: CPU 314C-2 PN/DP
        Basic Firmware: v.3.3.11
        Basic Hardware: 6ES7 313-6CG04-0AB0
        }
**********************************************************
IP:192.168.1.231  PORT:102  STATUS:open  SERVICE:S7
BANNER:{
        Copyright: Original Siemens Equipment
        PLC name: S7-300 station_2
        Module type: CPU 314C-2 PN/DP
        Basic Firmware: v.3.3.11
        Basic Hardware: 6ES7 313-6CG04-0AB0
        }
**********************************************************
IP:192.168.1.232  PORT:102  STATUS:open  SERVICE:S7
BANNER:{
        Copyright: Original Siemens Equipment
        PLC name: S7-300 station_3
        Module type: CPU 314C-2 PN/DP
        Basic Firmware: v.3.3.11
        Basic Hardware: 6ES7 313-6CG04-0AB0
        }
**********************************************************
IP:192.168.1.234  PORT:102  STATUS:open  SERVICE:S7
BANNER:{
        Copyright: Original Siemens Equipment
        PLC name: S7-300 station_4
        Module type: CPU 314C-2 PN/DP
        Basic Firmware: v.3.3.11
```

```
os-shell> whoami
do you want to retrieve the command standard output? [Y/n/a]
[18:27:46] [INFO] retrieved: 2
[18:27:46] [INFO] retrieved: nt authority\system
[18:28:28] [INFO] retrieved:
command standard output:    'nt authority\system'
os-shell>
```



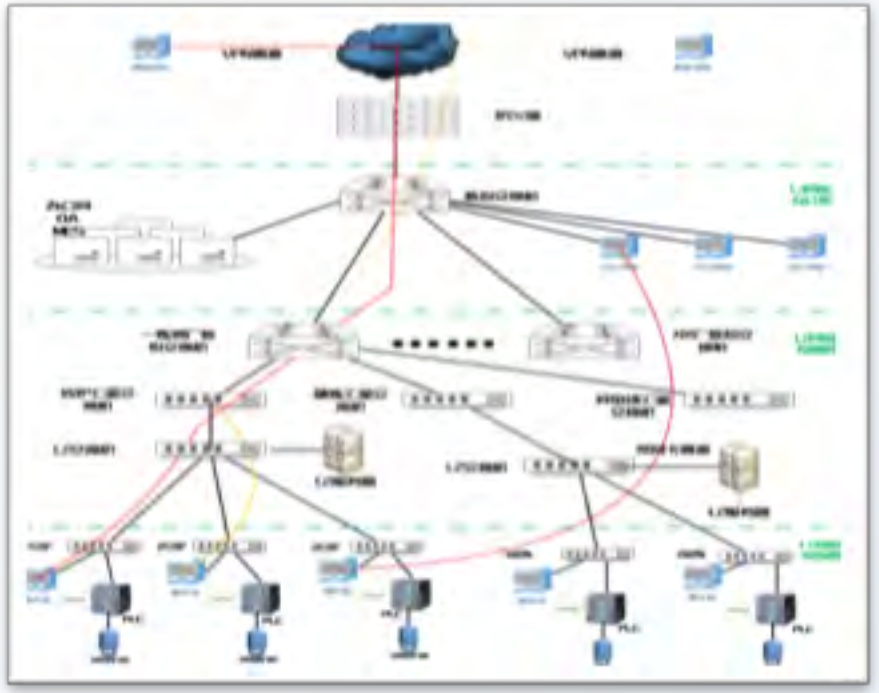
360 企业安全 安全第一

WannaMiner attack on an Large Steel Corp

Case4： 某大型炼钢厂遭受永恒之蓝挖矿病毒攻击

A huge steel plant suffers from a WannaMiner attack

- **About 150 PC of a steelmaking plant, involving different production processes, appeared repeated blue screen or restart phenomenon at 2018.10.31.**
- **After on-site emergency treatment, the production of PC infected with the WannaMiner virus, and the virus is in the trend of large-scale outbreak**

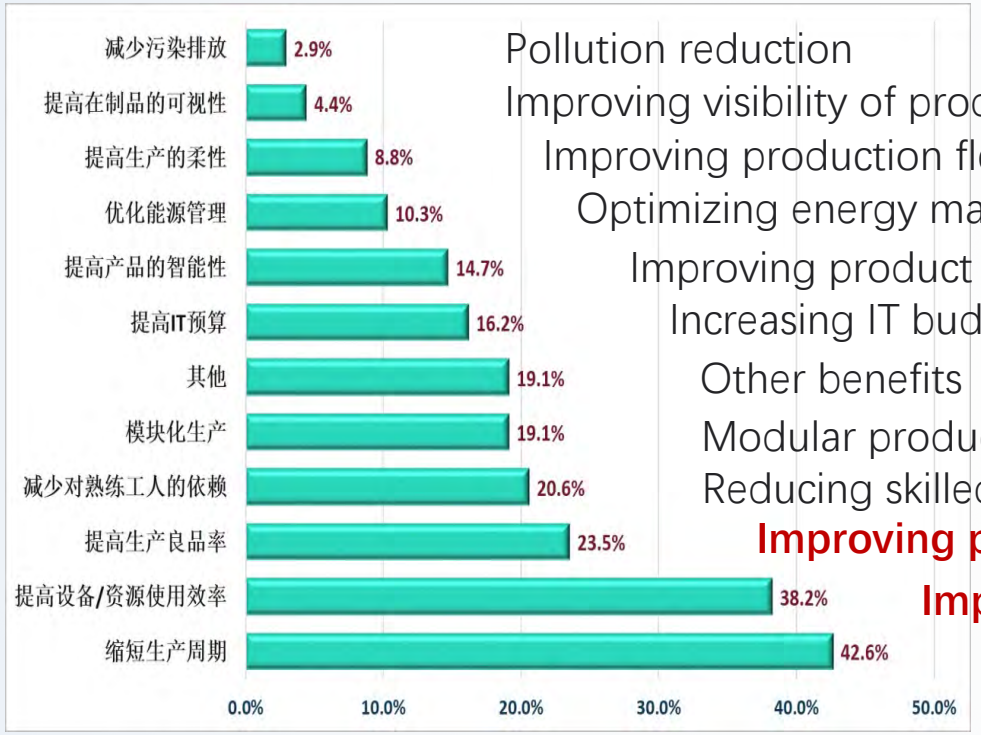


企业态度

How and Why to develop industrial Internet

工业互联网产业联盟
Alliance of Industrial Internet

Expected benefits of enterprises by industrial Internet



Pollution reduction
Improving visibility of production
Improving production flexibility
Optimizing energy management
Improving product intelligence
Increasing IT budget
Other benefits
Modular production
Reducing skilled workers' dependence
Improving production quality
Improving utilization ratio of equipment resources
Shorten production cycle

Key points for improving production and operation in the next 1-2 years

来源：常州市工业调研
Source：Industrial investigation in Changzhou

企业态度

What impedes Industrial Internet?

工业互联网产业联盟
Alliance of Industrial Internet

10 major problems impeding the development of industrial Internet

Lack of path to Industrial Cloud

Lack of management support

Equipment connection difficulty

Other problems

Not the preferred strategy

It's not easy to see the effect

Insufficient policy environment

Lack of IT budget

Worry about Cyber Security

Lack of compound talents

Impeding the implementation of industrial Internet

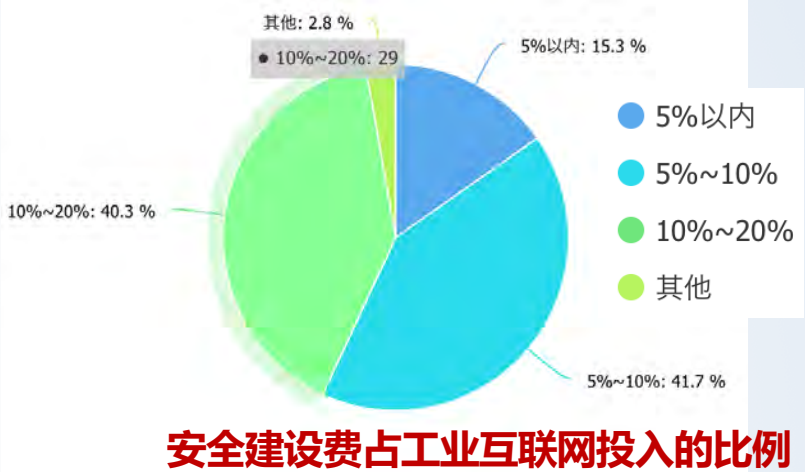
来源：常州市工业调研
Source：Industrial investigation in Changzhou

360 企业安全 安全第一™

The result of survey(100+) :

Self evaluation (optimistic ?) :

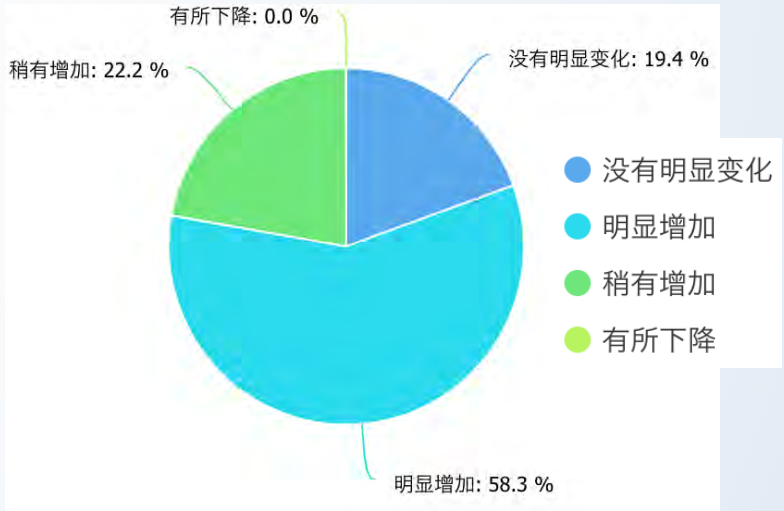
1. A large number of enterprises believe that their network security level is good
2、More than half of companies believe they will not be attacked by the Internet.



安全建设费占工业互联网投入的比例

Trend :

1. 53% of enterprises believe that the investment of information security will increase significantly.
2.80% of enterprises believe that security investment should account for 5%-20% of industrial Internet investment.
3. over 76.4% think that the decision of top leaders decides the importance of network security.
4. the biggest challenge of industrial network security is lack of security talents



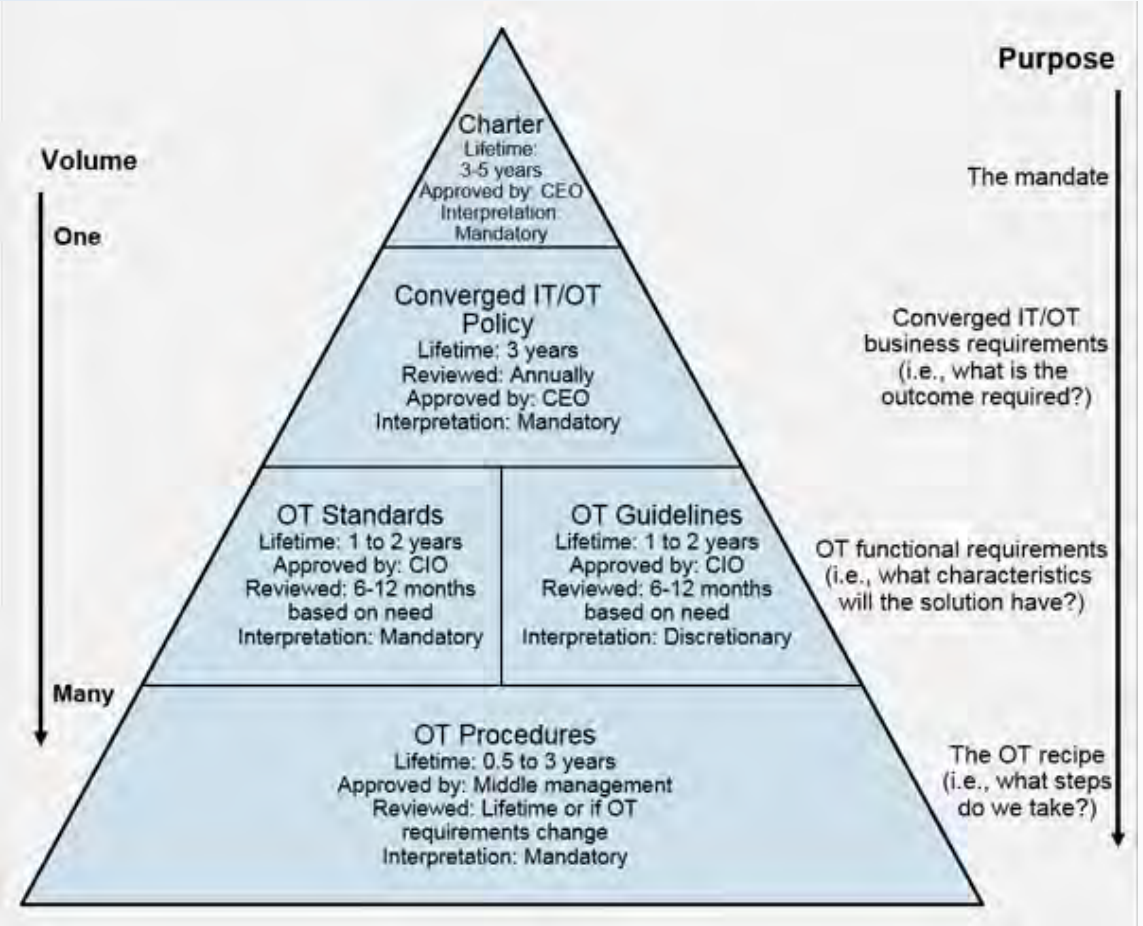
安全费用投入趋势

目 录
CONTENT

一体化安全战略

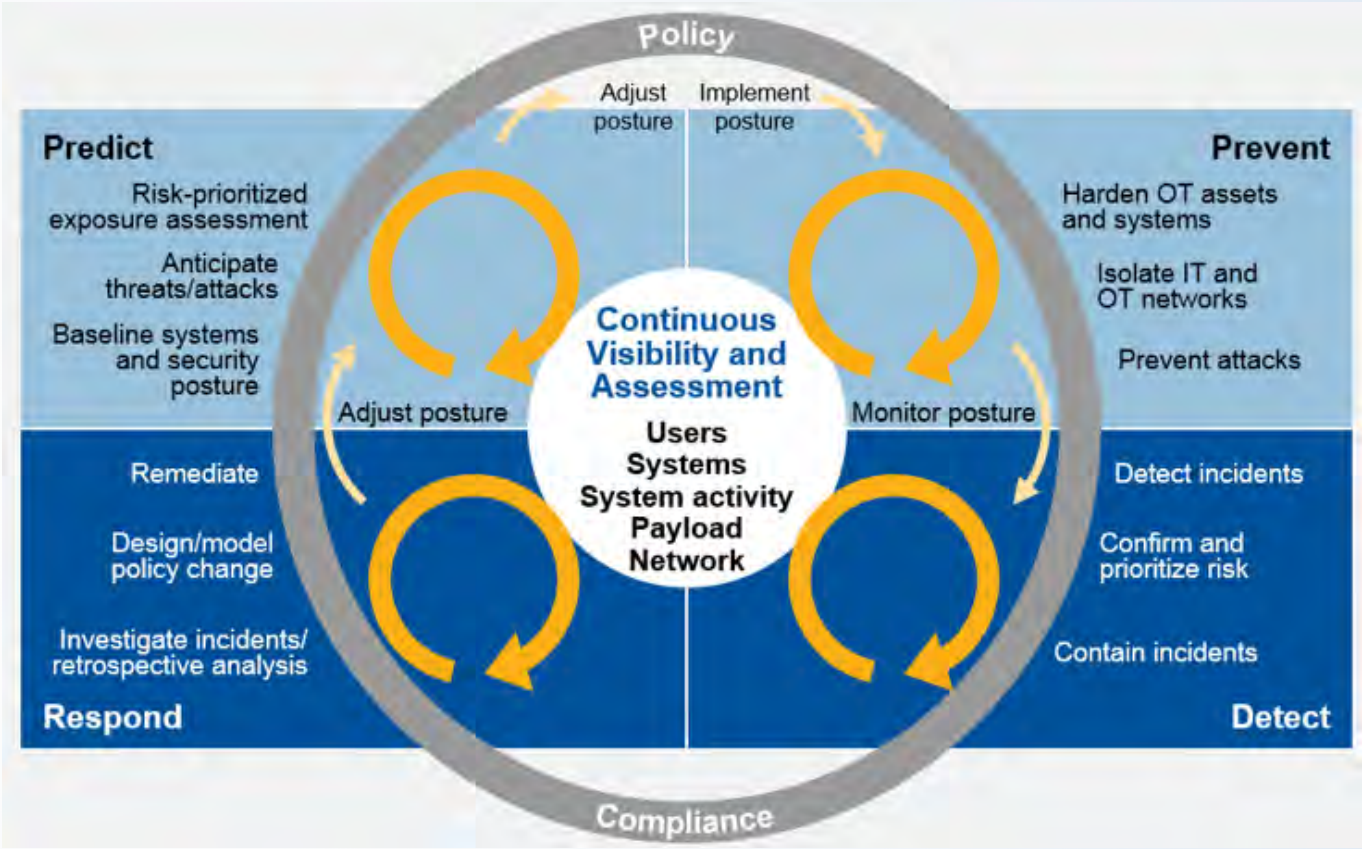
Converged IT/OT Security development route

工业互联网产业联盟 Alliance of Industrial Internet



IT/OT一体化安全策略框架

Converged IT/OT Security Policy Framework



IT-OT自适应安全架构

IT-OT Adaptive Security Architecture

Gartner

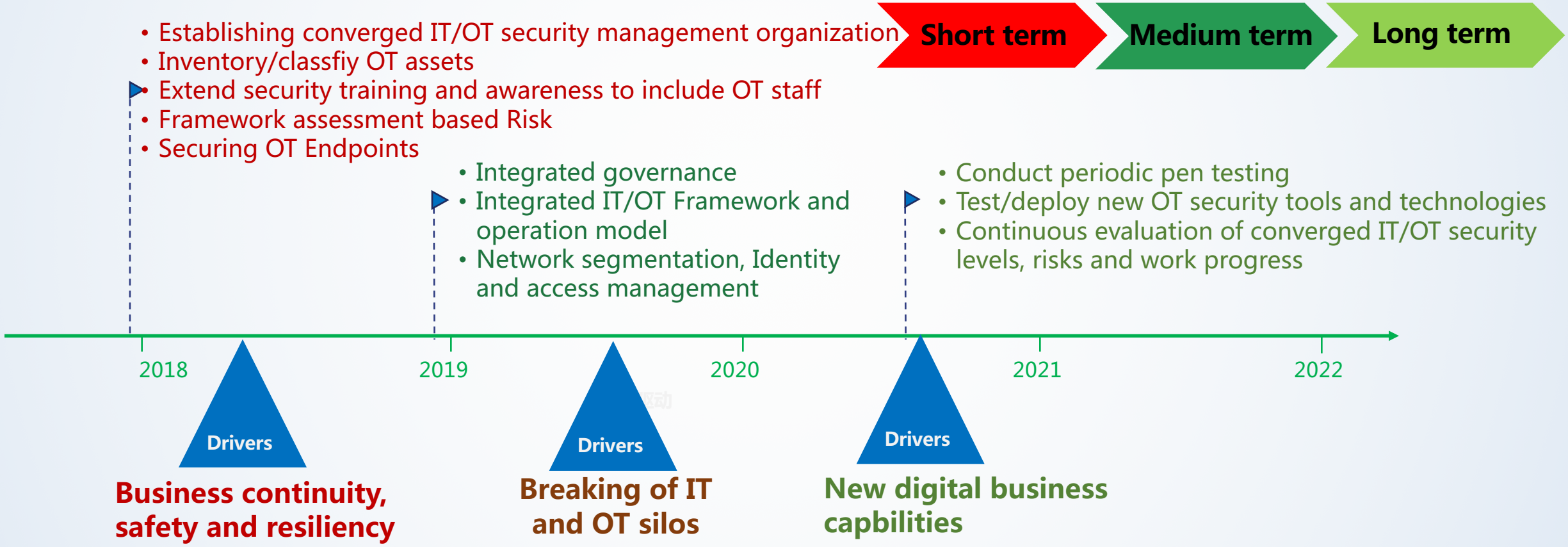
360 企业安全 安全第一™

企业战略推进 Converged IT/OT security strategic advancement

工业互联网产业联盟 Alliance of Industrial Internet

安全治理是长期且复杂的过程，难以一蹴而就，需要循序渐进

Security governance is a long-term and complex process that is difficult to achieve overnight and requires gradual progress



战略路线图时间表

Strategic roadmap timeline

360 企业安全 安全第一

工业互联网产业联盟
Alliance of Industrial Internet

融合·协作·共赢

共同把握工业互联网的历史机遇

联盟公众号：工业互联网产业联盟

联盟网址：http://www.aii-alliance.org/

联盟邮箱：aii@caict.ac.cn