



启明星辰



1	1
1.1	1
1.2	1
1.3	3
1.4	4
2	6
2.1	6
2.2	7
2.2.1	7
2.2.2	8
2.2.3	9
3	11
3.1	11
3.2	12
3.3	12
4	13
4.1	13
4.2	15
4.3	15
4.3.1	16

4.3.2		19
4.3.3		25
5		27
5.1		27
5.1.1		27
5.1.2		34
5.1.3		38
5.2		42
5.2.1	I1OT	42
5.2.2	I1OT	45
5.2.3	I1OT	46
6		50

1

1.1

Industrial Internet Consortium (IIC) AllSeen Alliance Open Interconnect  
Consortium (OIC) 6  
Accenture

1.3

" " " "

2013 2 5

2017 1 17

" "

2016 2020

2016 2020

1.4

2015 2 27

IP

2016 10 21 11:10 UTC( 19:10 ) Mirai  
Dyn DDOS

--

2007 •

2008 14 V

# Arg

2011

2011

RQ-170"

"

2013

.

"

"

SkyJack

"

"

2014

Tesla Model S

## 1 WannaCry

WannaCry

Windows

(PC)

(IoT)

IoT Institute

## RFID

2.2

2.2.1

a)

b)

c)

d) /

e)

f)

g)

1 1

2.2.2

a)

b)

c)

2.2.3

a

b

c

d

e

3

3.1

a)

f)

g)

3.2

a)

b)

3.3

a)

b)

c)

d)

e)

f)

g)

h)

i)

4

4.1



3

## 4.2

GB/T 35317-2017

GB/T 35318-2017

GB/T 35592-2017

GB/T 25070

YD/T 2437-2012

YDB 101-2012

2011

2016 CAICT

2017

## 4.3



4.3.1

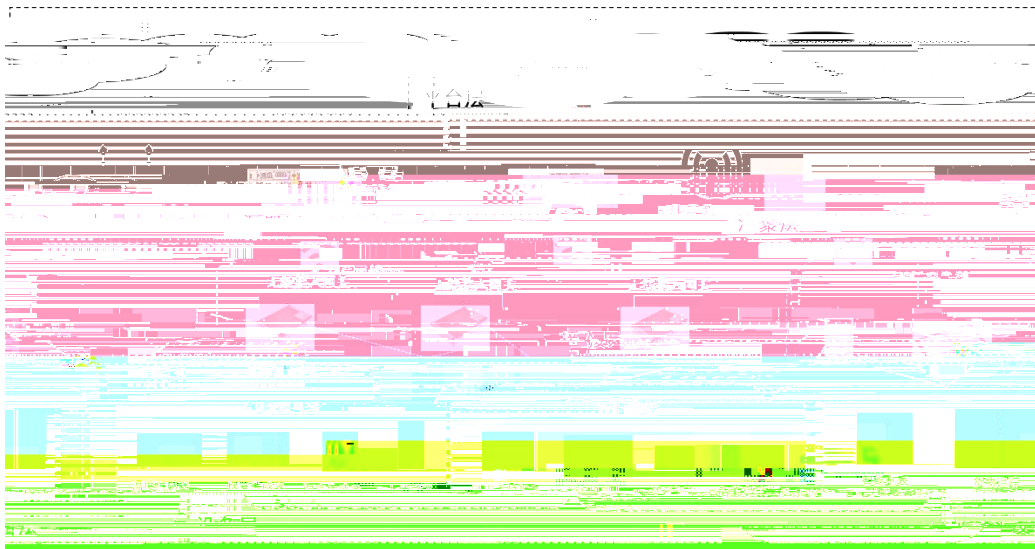


4

4.3.1.1

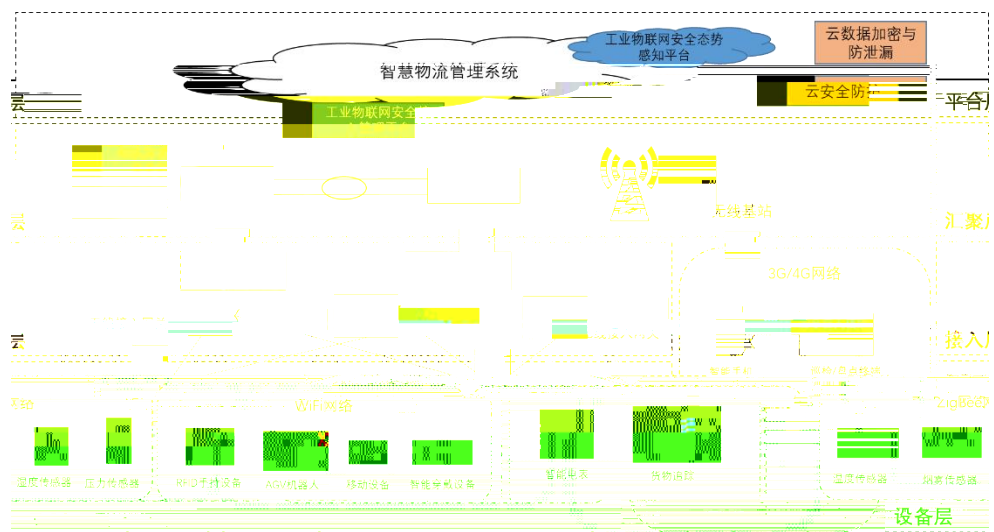
WiFi

ZigBee 4G-LTE

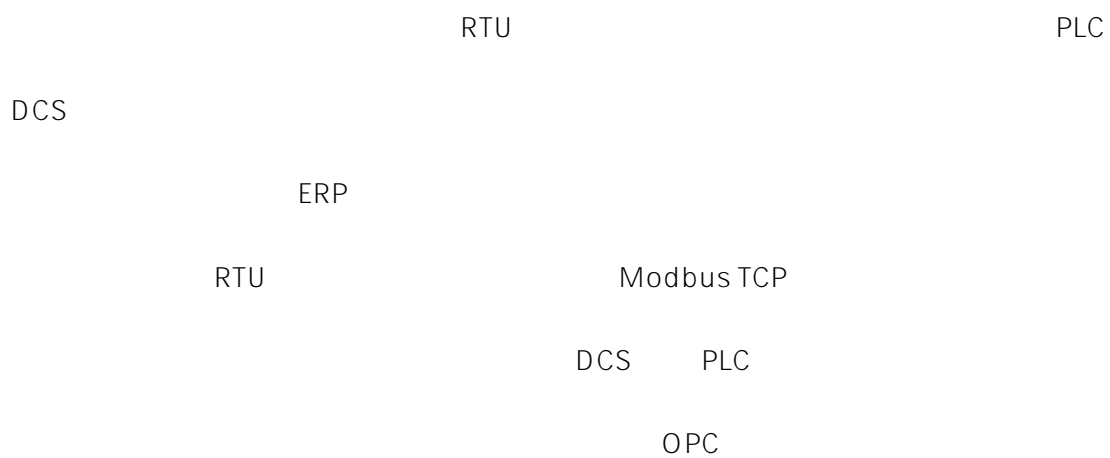


5

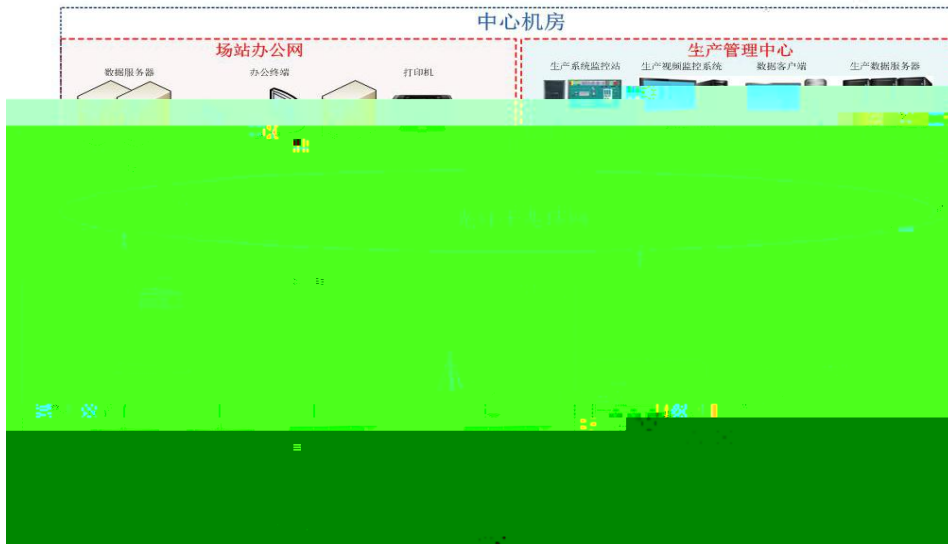
#### 4.3.1.2



#### 4.3.2



4.3.2.1



7

a) RTU

RTU

Modbus

IP MAC

RTU

b)

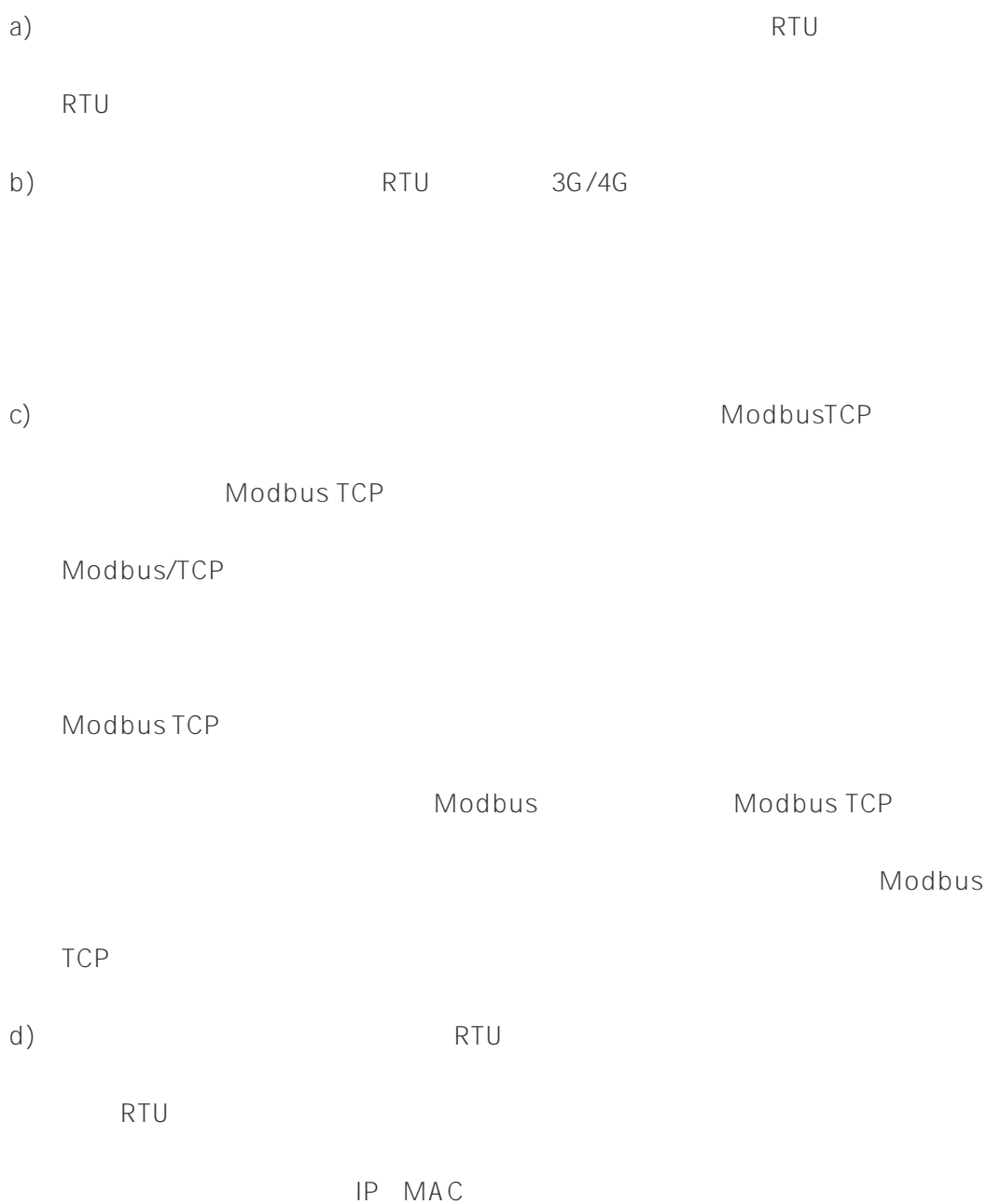
RTU

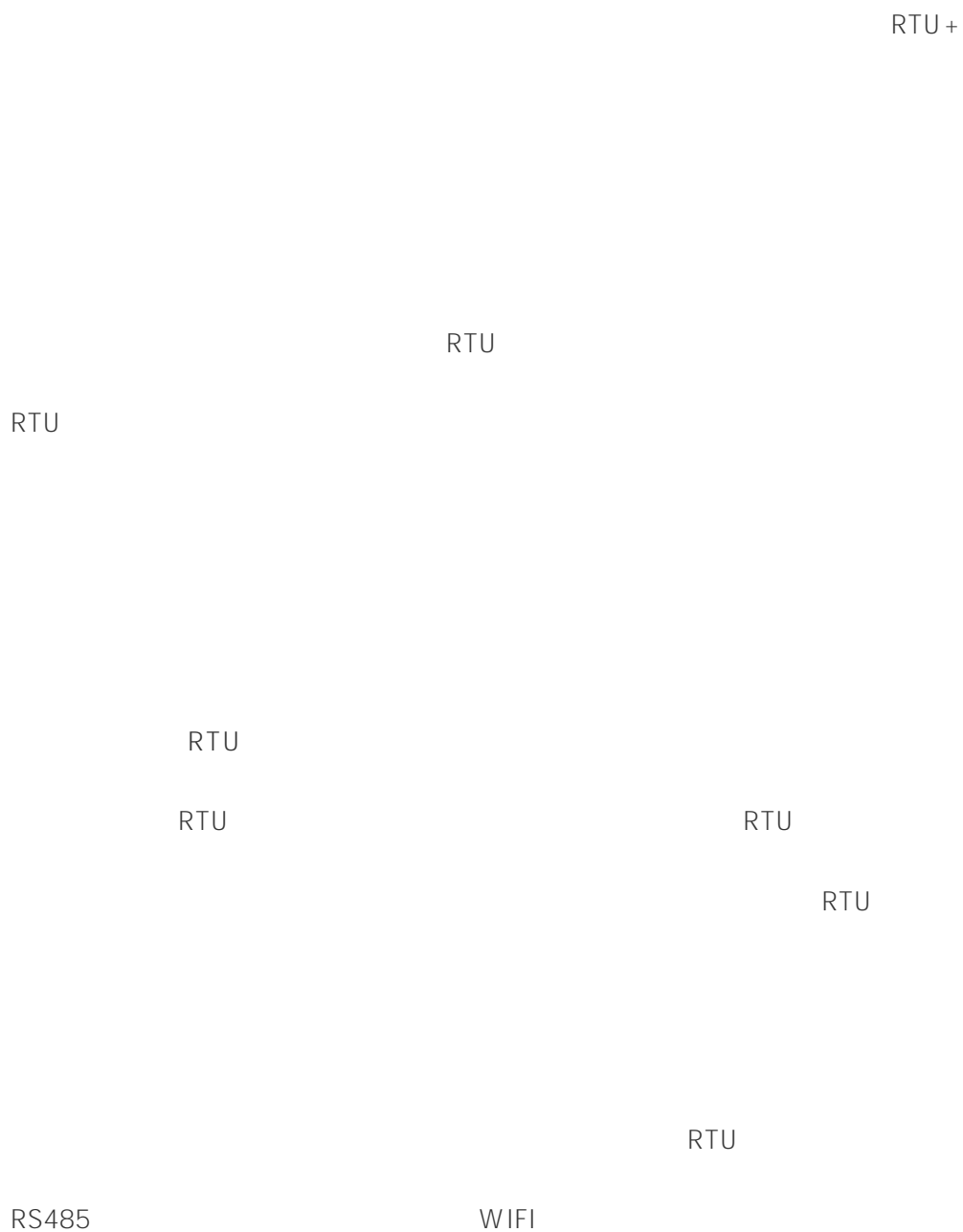
Modbus

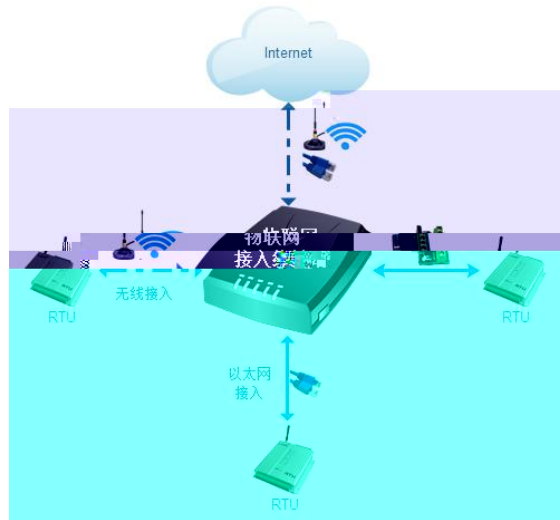
c)



Modbus TCP







9

2

RJ45

RTU

RS485

RS485

RS485

RS485

WIFI

RTU

RTU

### 4.3.3

#### 4.3.3.1

“

”

a)

b)

c)

d)

Mirai

DNS

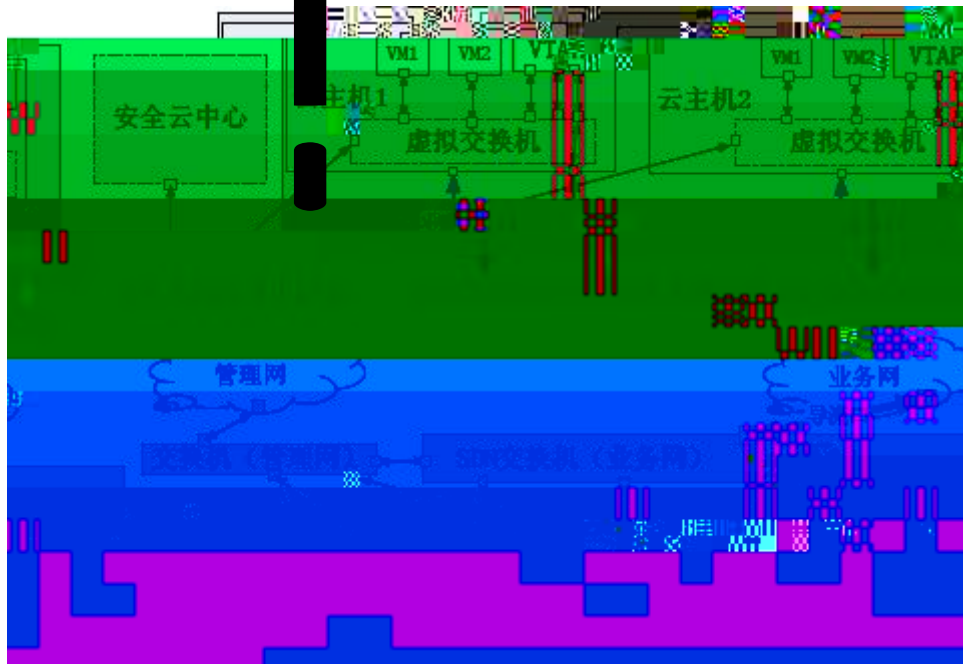
DYN

DDOS









12

1-N

1~2

CPU

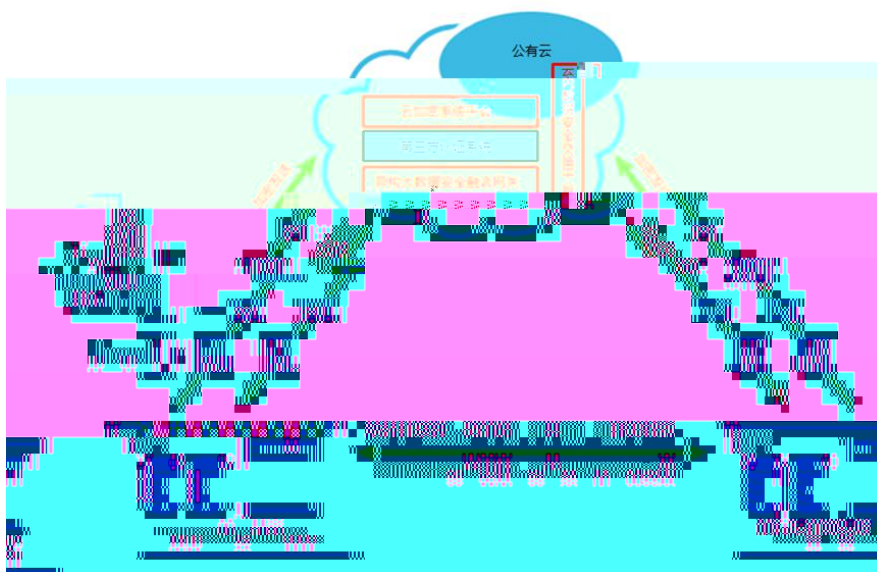
CPU

CPU

5.1.1.2

VPN

DCAP



13

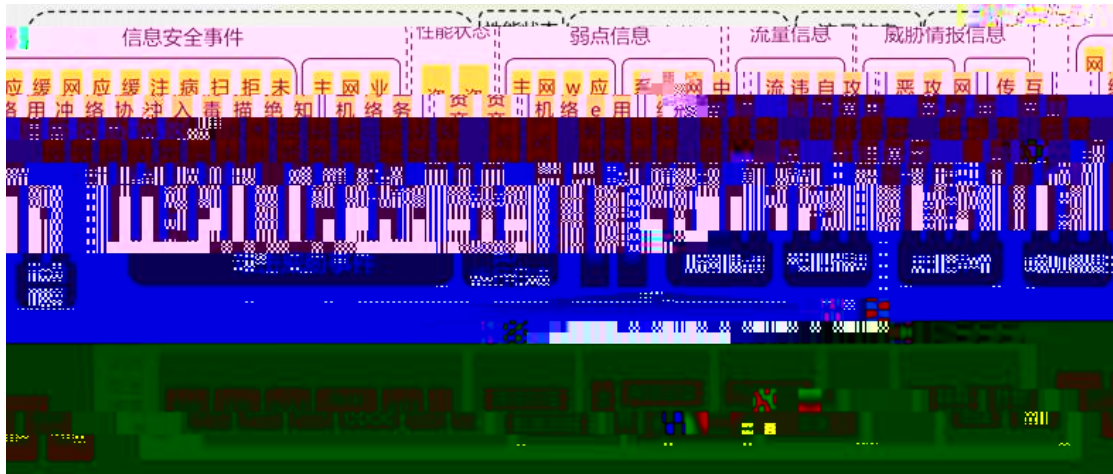
DBA

IP

SQL

### 5.1.1.3

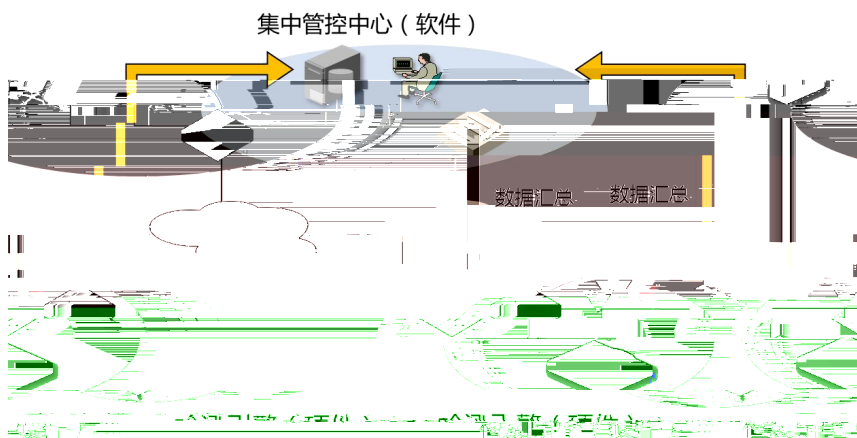
ê



5.1.2

5.1.2.1

DDOS



Web攻击检测				
模糊查询		重置		
序号	规则编号	规则名称	状态	操作
1	5000084	HTTP_可疑行为_恶意的User-agent SAPHagent	已启用	● ☒
2	5000085	HTTP_可疑行为_恶意的User-agent STORMDDOS	已启用	● ☒
3	5000086	HTTP_可疑行为_恶意的User-agent AsyncHTTPAgent	已启用	● ☒

17

IP空包检测				
模糊查询		重置		
序号	规则编号	规则名称	状态	操作
1	300000	IP报文头错误	已启用	● ☒

18

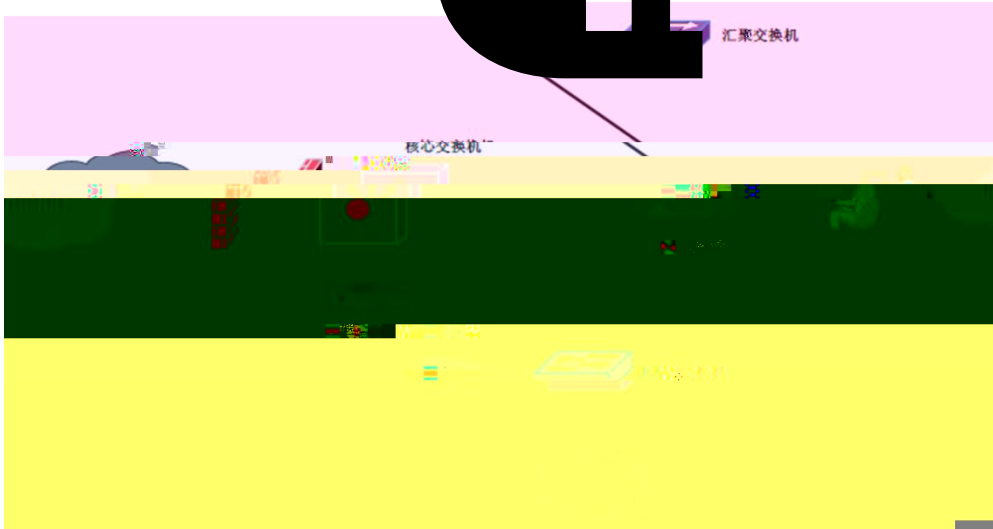
TCP UDP HTTP DNS 60

300



19

### 5.1.2.2

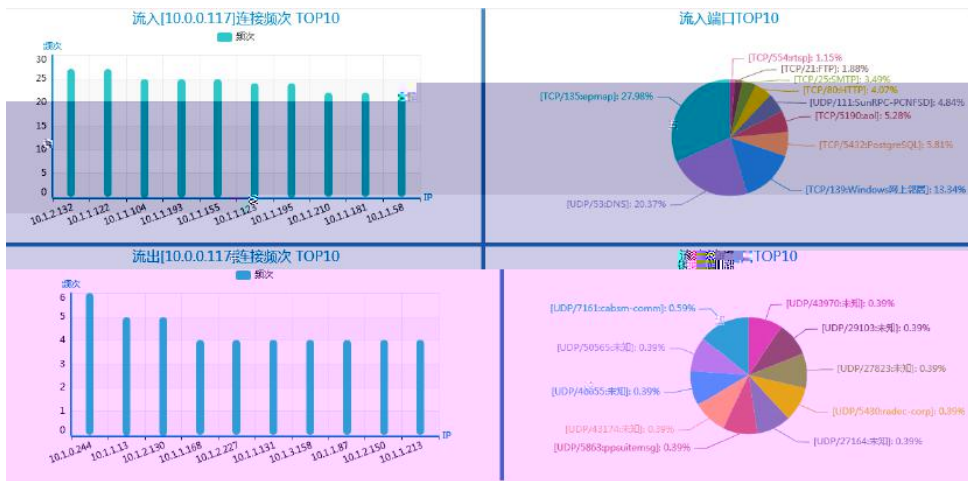


20

y ō

## Top10 IP Top10

### IP



22

ARP

DDoS

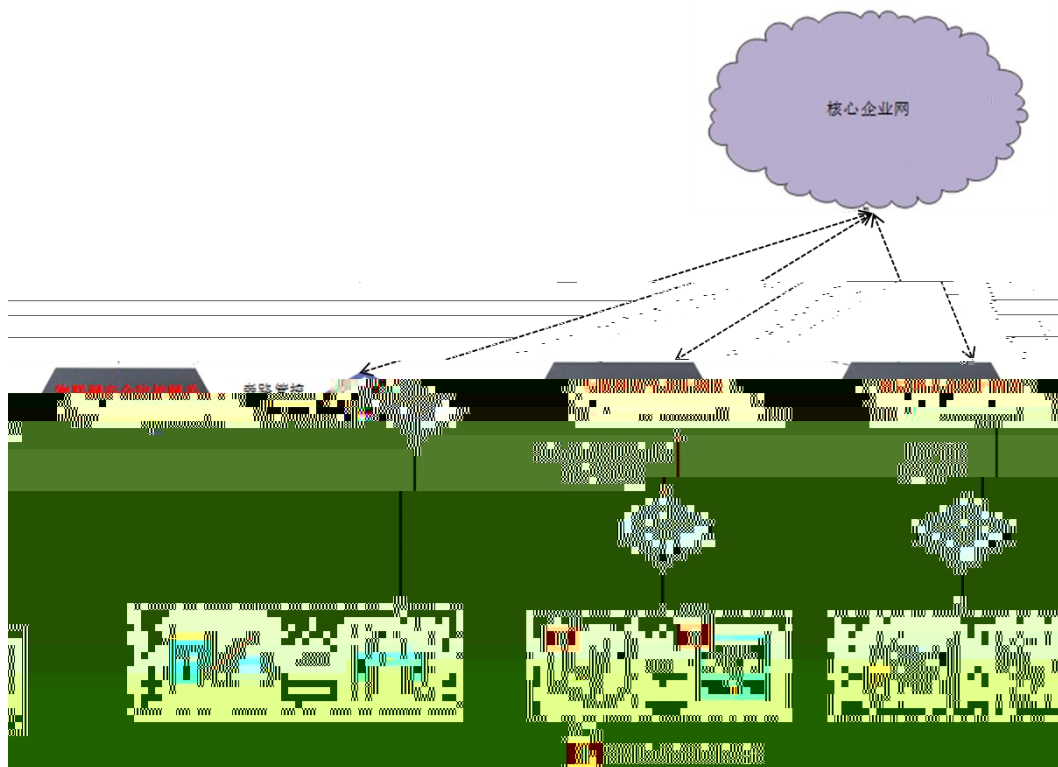
5.1.3

5.1.3.1

a

b

c



300

24

5.1.3.2

1700

1700

1700

1700

1700

1700

1700

1700

1700

1700

1700

1700

1700

1700

1700

1700

1700

1700

1700

1700

1700

1700

1700

1700

1700

1700

1700

1700

1700

1700

1700

1700

1700

1700

1700

1700

1700

1700

1700

1700

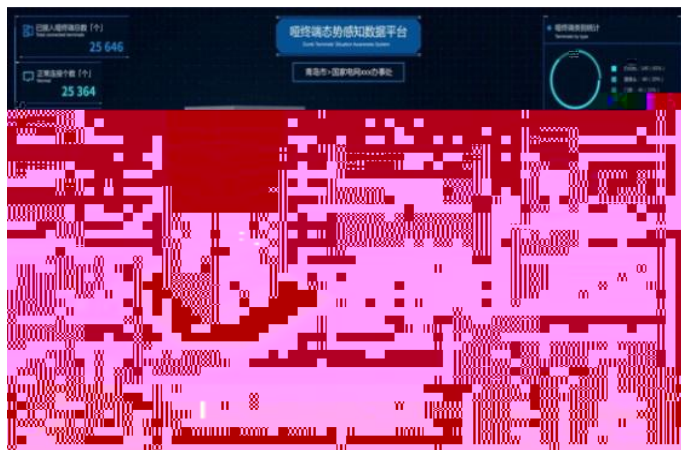
1700

1700

1700

1700

1700

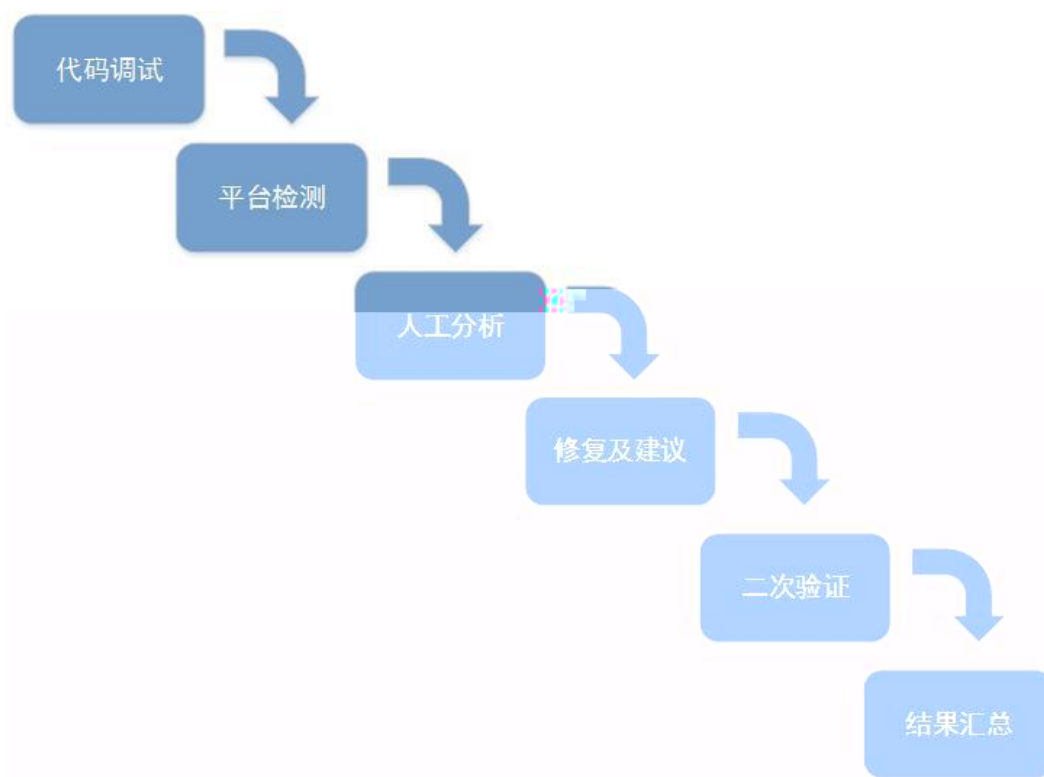


26

## 5.2

### 5.2.1 IIOT

90%





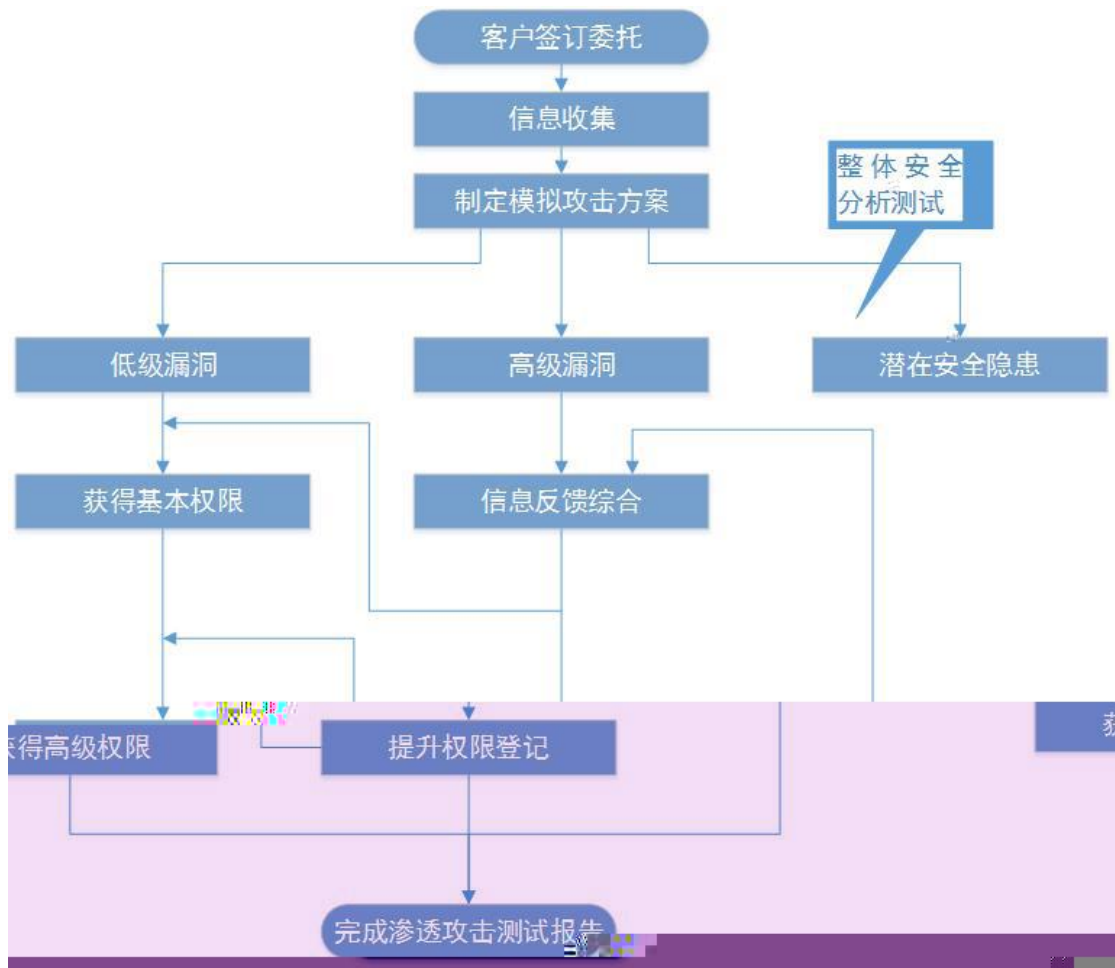
## 5.2.2 IIOT

m

—

### 5.2.3 IIOT

/



28

a

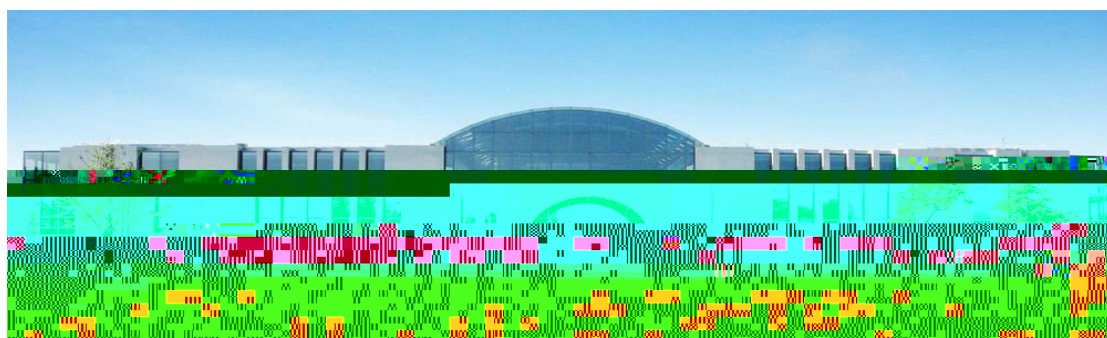
b

c

I







29

200

20

863

"

" "

" "

20 " "

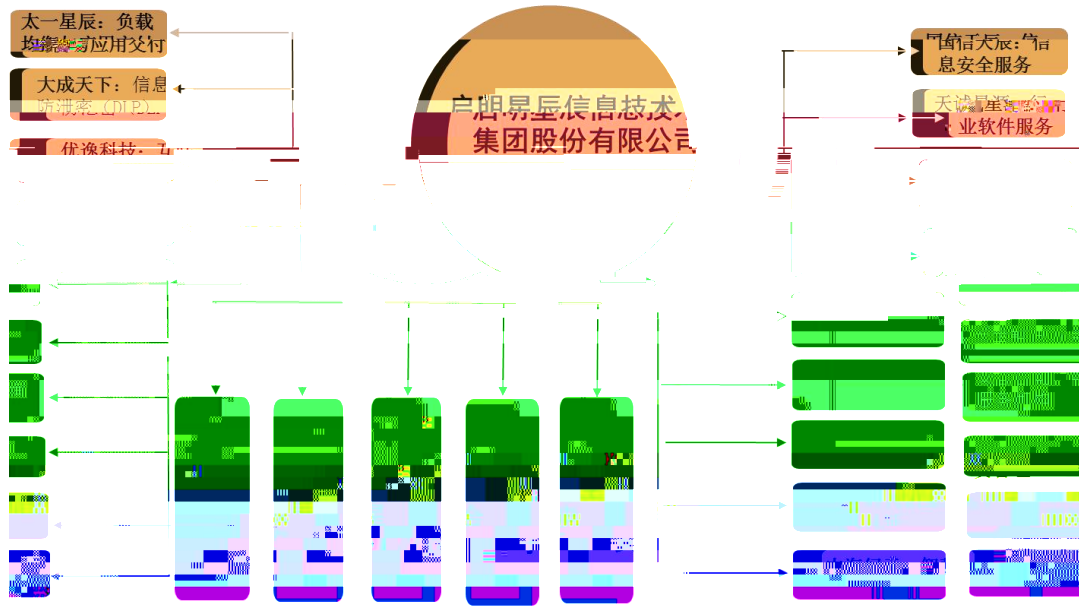
"

3000

/UTM

/

30



30

IT

863

/

"

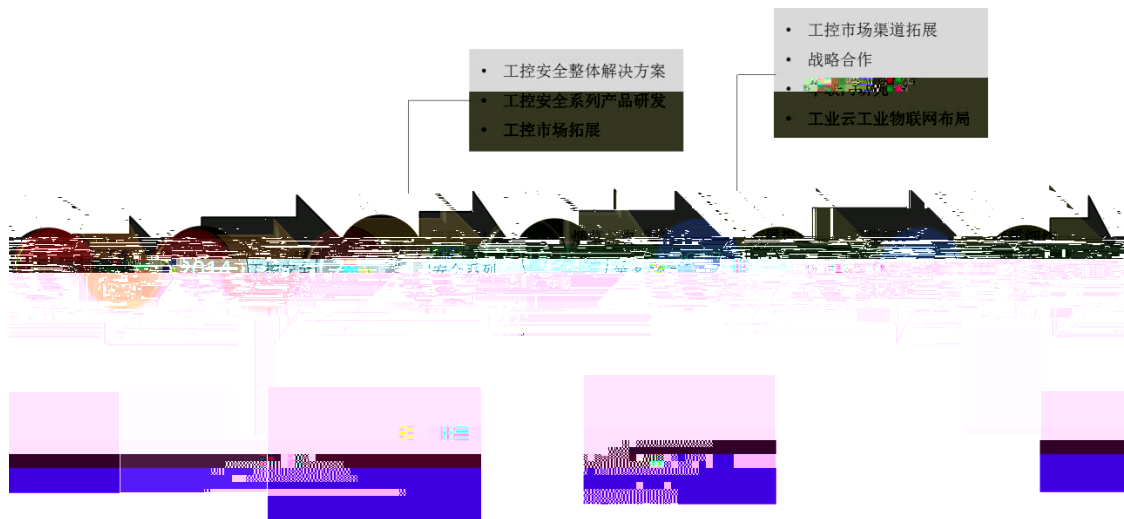
"

"

"

2010

2014



31

36

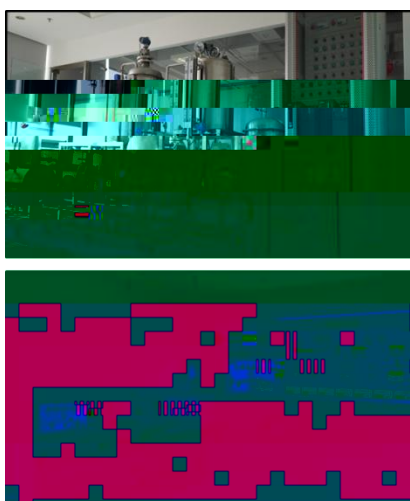
53

PSCAC

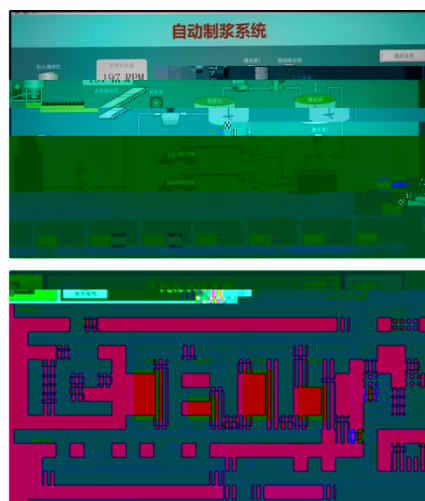
C



32 +



33 +



ADLab

70

ADLab

CVE

Windows Linux Unix

ADlab

+

GPS

Android



34

T-Box

TSP

APP

Authorization

App



:

DCS

PLC