西肯麦 secomea

可私有化部署的非VPN工业远程通信方案

设备制造商 | 系统集成项目 | 工厂 | 硬件设备商

远程调试 | 移动监控 | 数据采集 | 跨网络架构 | 数据上云 | 软件网关

了解西肯麦

secomea

- 简介
- 应用场景与案例
- 选择西肯麦远程技术

西肯麦 – 让安全通信更简单

SECOMEA – SECURE COMMUNICATION MADE EASY

Secure 安全 Communication 通信 Made 变得 Easy 简单

SECOMEA A/S expert on Industrial Remote Technology for 18 years

西肯麦专注于工业远程通信19年

七大基础功能

基于这些功能，结合应用需求，打造多种解决方案

secomea

远程调试

-杜绝低效出差

远程在线调试、程序上下载；
支持PLC、HMI，以太网、串口、USB设备

移动监控

-随时实地监控设备

手机或平板实时监控触摸屏、工控机、摄像头；
支持Web、VNC、RDP访问

远程SCADA

-现场情况，了如指掌

可采集数据到本地SCADA；
远端设备IP可完全相同，无需公网IP。

数据上云

-一套方案即可实现

MQTT上传；支持RS232/485串口、以太网、CAN接口；
支持上百种协议和边缘计算，支持设备远程调试。

远程安全

-消灭最薄弱的人为错误环节

三因素权鉴登陆；
联网端与设备端物理隔离；
主动式安全设计，端口自动开放与关闭。

权限管理

-OT与IT职责清晰，OT可精细化管理设备

权限可精细到单个设备级别；
操作记录永久追溯；
OT可轻松掌握。

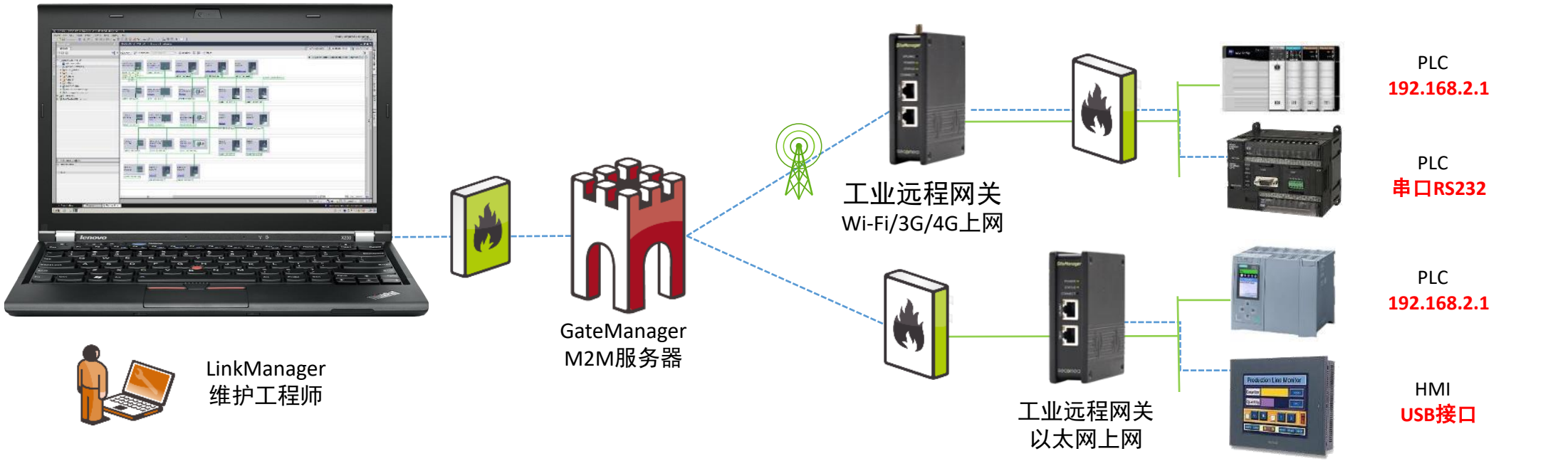
软件网关

-激活已有硬件，少走弯路

支持多种系统及CPU架构；
已有硬件，安装软件即可具备硬件网关大部分功能；
可嵌入工控机、触摸屏等等。

基础功能 - 远程调试

无论身处何地，轻松调试全球各地现场，不再低效出差



备注：不同远端现场的设备IP可相同

操作步骤
- 安装LinkManager软件
- 电脑接入因特网
- 导入数字证书
- 选择需要连接的设备

USB

以太网

RS232/422/485

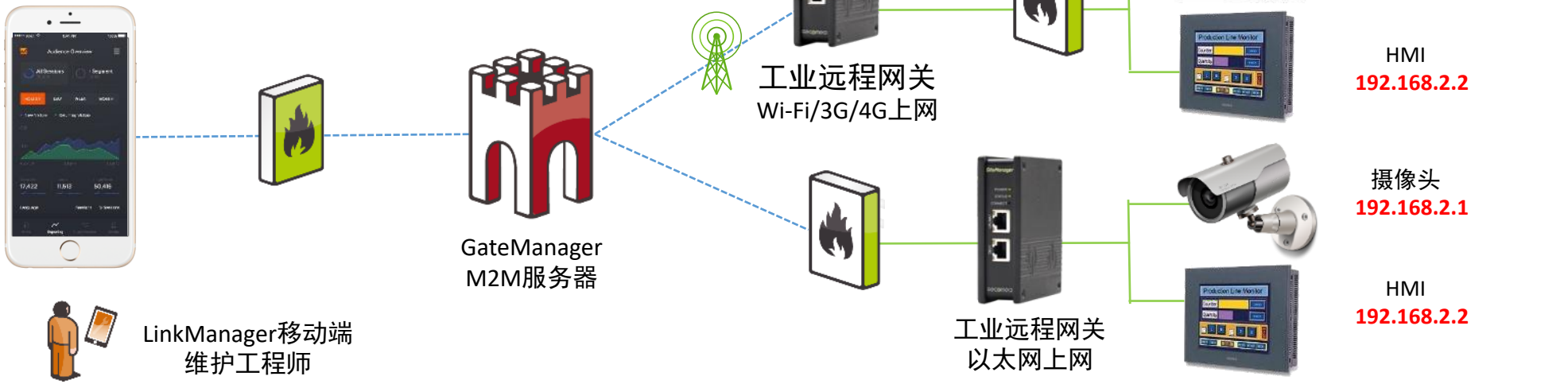
支持对几乎各品牌的PLC/HMI远程编程

支持的物理接口
- 以太网
- USB
- 串口

基础功能 - 移动监控

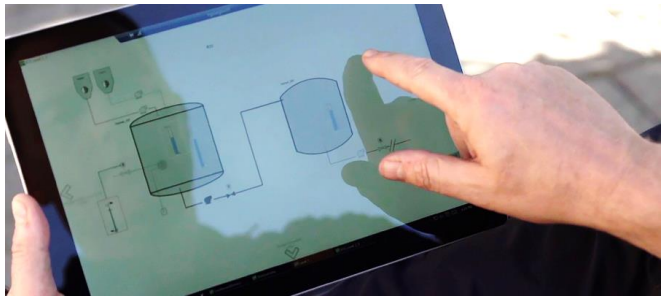
带着手机，就像带了一个办公室

手机无需APP，直接通过浏览器即可
可连接TCP/IP设备，可监控并控制



备注：不同远端现场的设备IP可相同

操作步骤
- 打开浏览器
- 输入GateManager网址
- 输入用户名密码
- 选择需要连接的设备

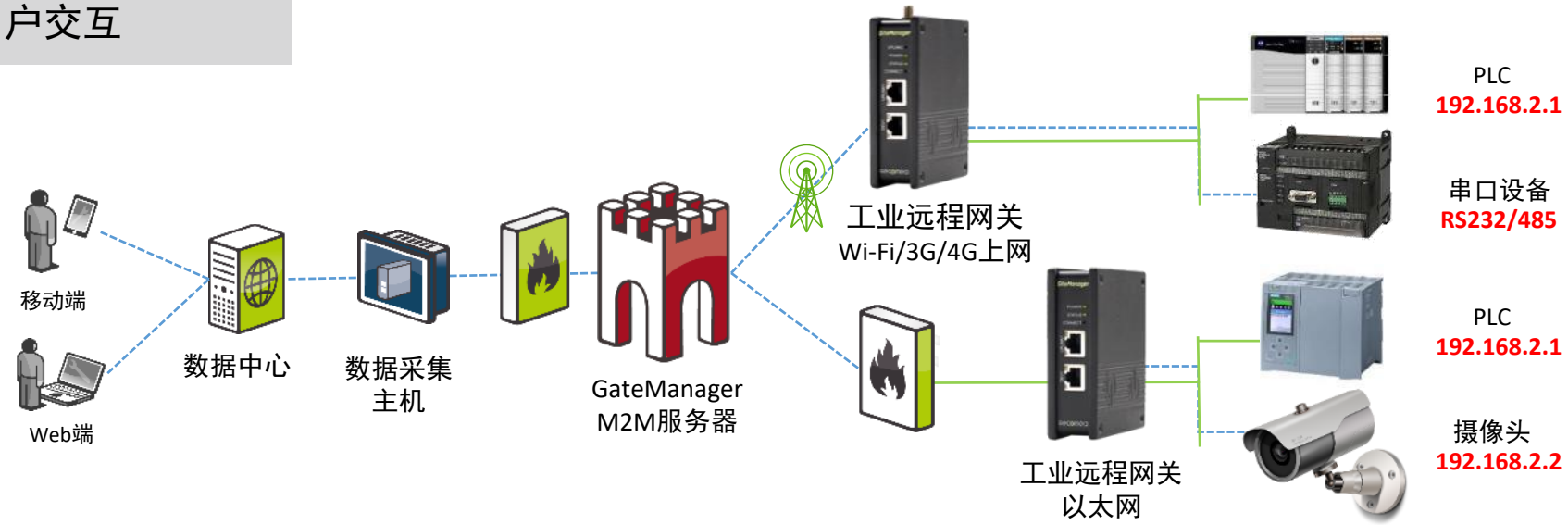


目前支持的访问方式
- WWW：Web网页
- VNC：虚拟桌面
- RDP：远程桌面

基础功能 – 远程SCADA

全球任何地方的数据，为你所用

将远端现场数据从采集上来，数据中心由多种软件与系统构成，最终通过Web、移动客户端与用户交互



您可自主开发软件

也可用监控软件

Wonderware by Schneider Electric　iFIX　FactoryTalk

支持OPC

Kepware　MatrikonOPC

支持各种数据库

Microsoft SQL Server　ORACLE DATABASE

基础功能 - 数据上云

将新、老设备数据上传至自建服务器，亦可上传至公有服务器

DCM为数据采集模块，支持Modbus与OPC协议

云端数据平台

分析 | 大数据存储 | 云端协议

API | 设置 | JSON MQTT

数据可视化 | 设置界面 | 安全模块

断点续传

MQTT

JSON

OPC UA

GateManager

工厂

DCM

Modbus TCP

工业远程网关

Modbus RTU

工厂

DCM

OPC UA

工业远程网关

OPC UA

工厂

DCM

OPC UA

软件网关

OPC服务器

更多协议将持续支持

云端数据平台管理员

设备维护工程师

LinkManager客户端

基础功能 – 远程安全

不更改防火墙，跨内网、因特网，实现安全、精准、可追溯的设备级访问

secomea

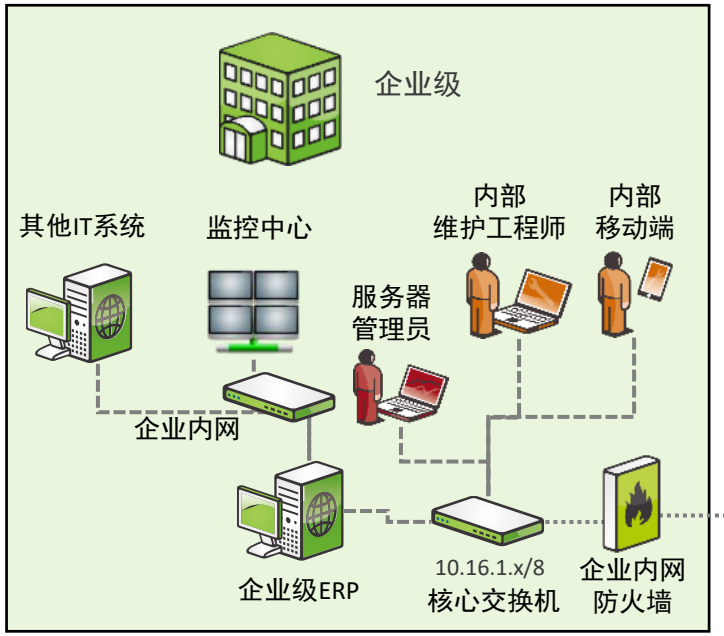
问题4：联网后权限过大，无法简单控制，所以不能轻易开放

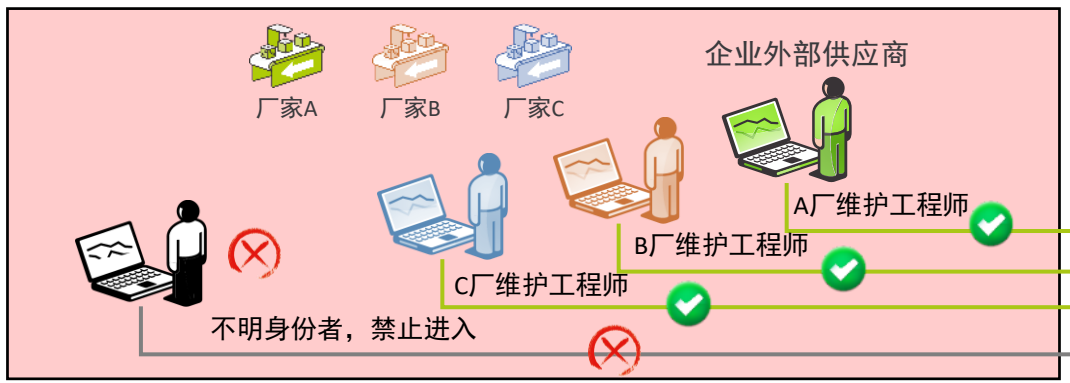
问题2：能看到问题，但排障还需要去现场

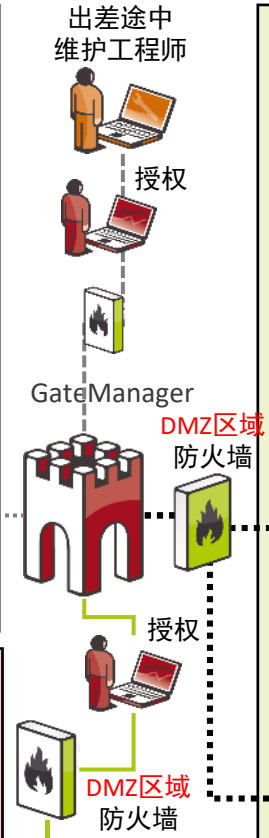
问题1：种种原因，机器级设备无法访问

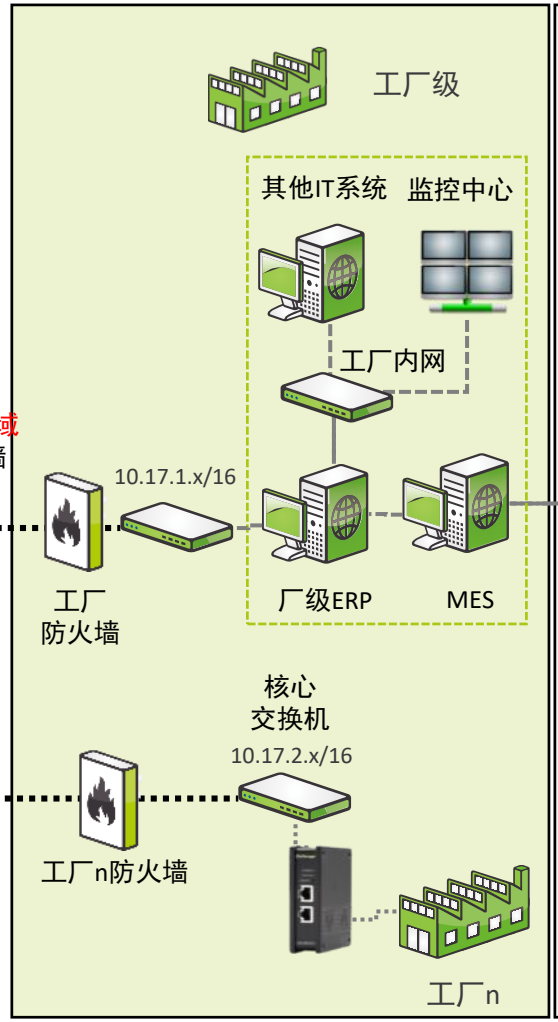
应用价值

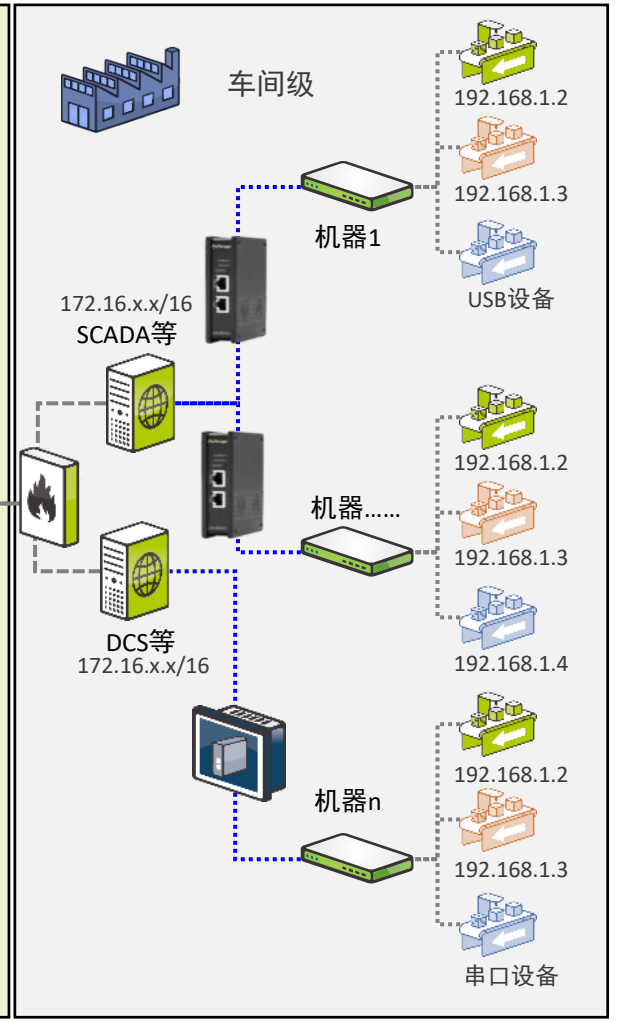
1. 工厂内信息已通过已有的MES/SCADA方式集中归集
2. 各级网络间通过防火墙进行隔离
3. 车间设备故障时，需人到现场解决
4. 外部工程师通过VPN远程排障，无追溯记录，权限无法限制为单台设备，风险大
5. 技术专家出差时，远程排障的困难多
6. 子网冲突解决麻烦











问题5：通过VPN或远程桌面方式，权限过大且无追溯记录，权宜之计

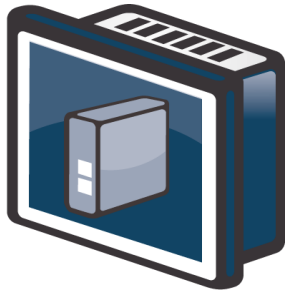
问题3：为了确保网络安全，架设多层防火墙，可能会纠枉过正

基础功能 – 软件网关

软件网关，使能硬件安全地接入数据上云

工业设备

SiteManager软件网关



具备物联网功能的工业设备

操作系统	CPU架构	硬件类型
Linux	x86	工业电脑
Windows	ARM	PLC
VxWorks	Power PC	人机界面
Android	MIPS	智能硬件
……	……	……

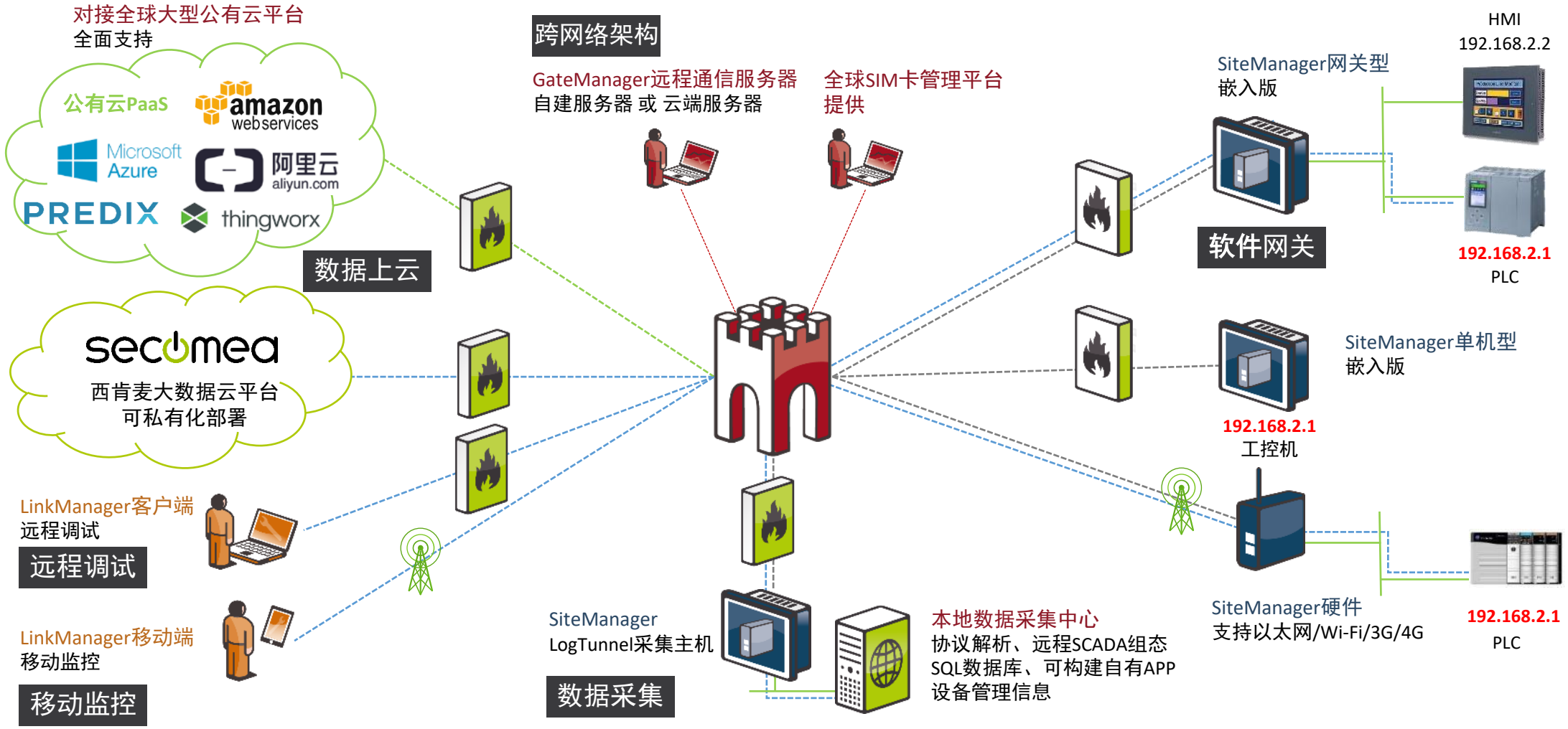
标准版	定制版
Linux与Windows操作系统直接安装	精简版操作系统可订制开发

基本型	网关型
只能访问设备本身无法访问同网段的其他设备	除设备本身外可访问其他网络界面的IP设备

确认您的硬件是否能够成为物联网硬件：操作系统 + CPU

西肯麦工业远程通信方案

安全、稳定、易用



secomea

- 简介
- 应用场景与案例
- 选择西肯麦远程技术

远程专家中心

Remote Expert Center

欢迎进入远程专家中心

远程专家中心

轻松建立您的远程专家中心

传统维护 VS 远程维护

轻松建立您的远程专家中心

专家坐镇，30分钟内响应，年轻工程师也可解决复杂问题

应用场景：应急性维护

远程专家中心搭建指南

1. 为每台机器配置SiteManager
2. 专人GateManager管理员，
3. 创建账号，分配权限，监控操作记录
4. 总部规划专用电脑用于远程维护用途
5. PLC告警设置通过SiteManager发出
6. 工程师登陆，并对设备进行维护
7. 出差的工程师可分配数字证书，允许连入网络中对设备进行维护

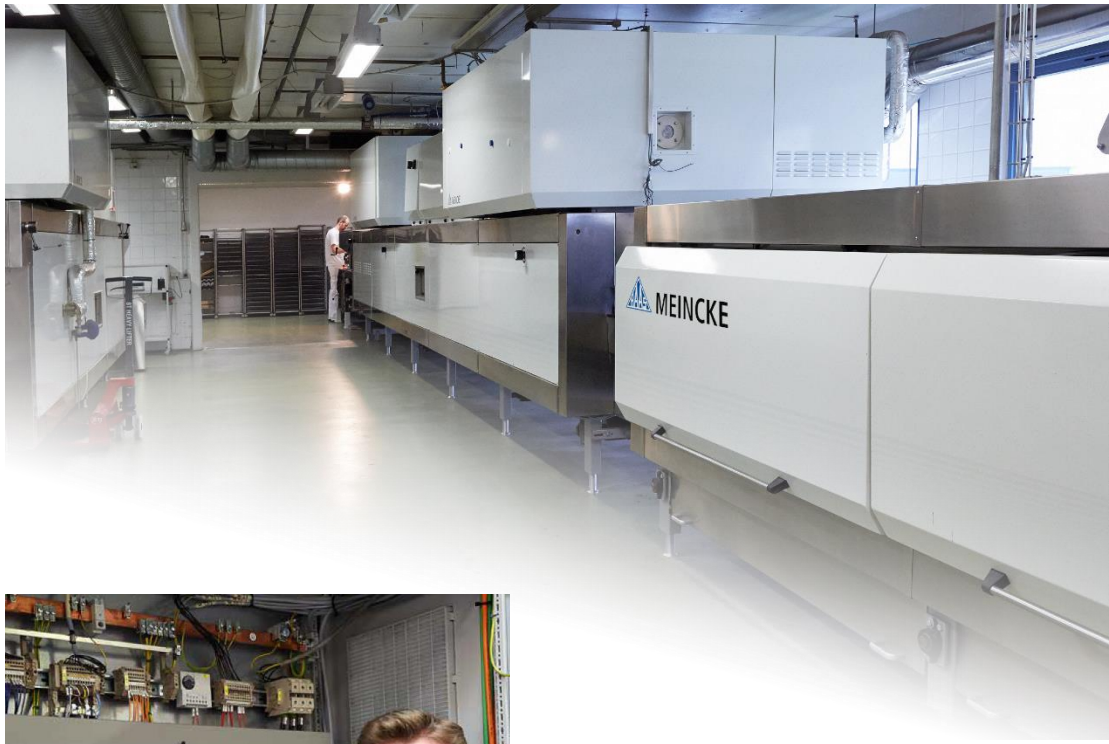
案例：烘焙设备制造商Haas Meincke的全球维护专家中心

公司位于丹麦，设备销往全球各地，在丹麦远程专家中心进行统一维护

secomea

背景与需求

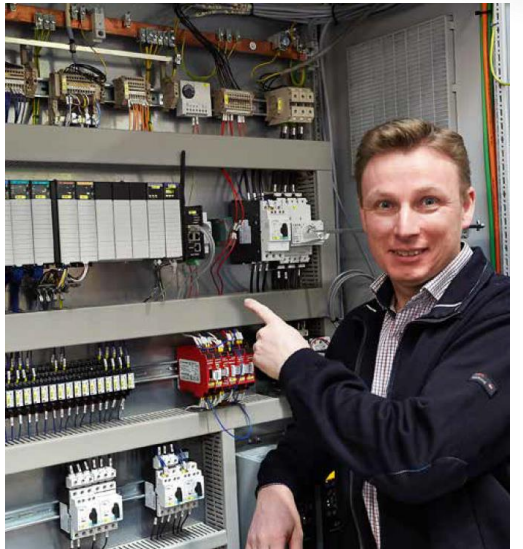
- 控制人员成本
- 减少出差
- 提高响应速度
- 提高普通工程师解决问题的能力



解决方案

初次使用 2008年

- 4台设备出口南美
- 配置SiteManager 3G 型号
- 装配由南美的装配工完成
- 丹麦工程师全部远程调试与维护
- 没出差一天，并提前完成任务



应用结果

全部机器标准配置 2009年

- 所有设备标准配置SiteManager
- 丹麦建立远程专家中心
- 应用扩展至集团的荷兰、奥地利子公司

HAAS MEINCKE

设备状态监控系统

Device Monitoring System

轻松建立您的远程设备状态监控系统

传统VPN方式 VS 西肯麦方式

发现问题还得派人去

大部分问题远程解决掉

成本居高不下

几乎不用出差了

操作无追溯

任何操作都可以追溯

对人员IT水平要求高

简单培训即可上岗

跨国联网不稳定

稳定性更强

IP冲突有困难

支持所有现场IP相同

普通工程师搞不定

普通工程师可解决大部分问题

设备状态监控系统

采集数据并可视化展示，根据初级告警及时介入，排除故障

预防性维护：组态软件采集水源井的状态数据

无人值守

支持PLC间通讯

无需光纤
4G跨区域采集
偏远水源井的数据
上位机采用SCADA软件

水源井1

水源井2

水源井3

水源井4

服务器管理员(杭州)

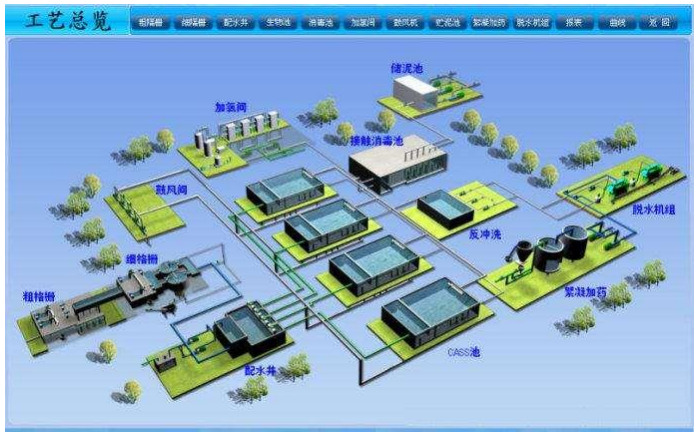
电气技术专家(杭州)

数据中心

WinCC

4G信号
无需光纤

设备状态监控系统



设备状态监控系统搭建指南

1. 为每台机器安装SiteManager
2. 专人GateManager管理员，
3. 创建账号，分配权限，监控操作记录
4. 总部规划专用电脑用于设备状态监控用途
5. 通过组态软件、自主开发软件、私有数据中心对各地收集回来的数据进行展示
6. 与业务逻辑对接，定义告警级别与对策
7. 远程将问题解决掉

案例： AKCENTRALEN的HVAC设备实时状态监控系统

承接丹麦超过1600家超市的HVAC设备状态监控与优化

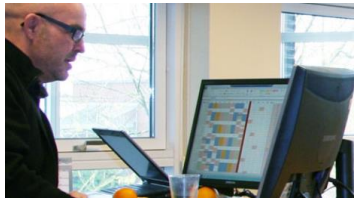
背景与需求

- 降低维护成本
- 减少去现场服务的次数
- 确保食物的温度处于合规水平
- 优化制冷效率
- 降低能源消耗

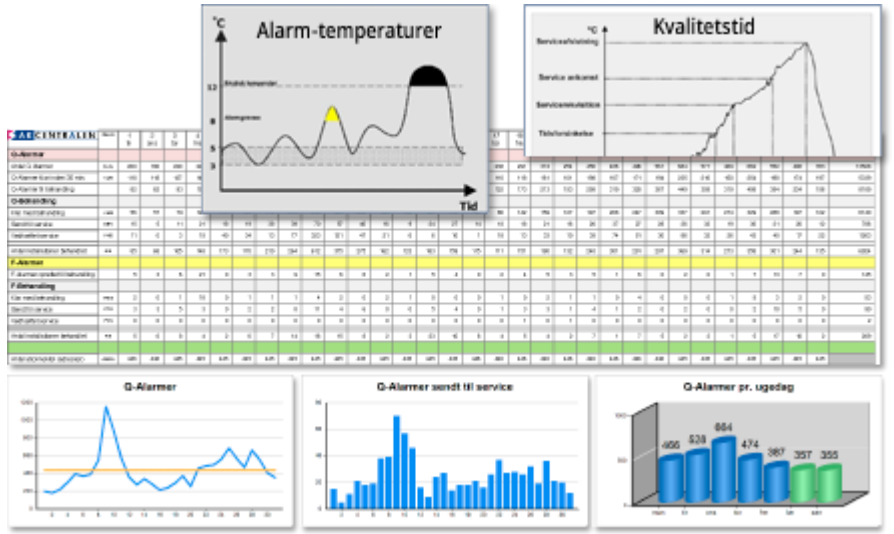
解决方案

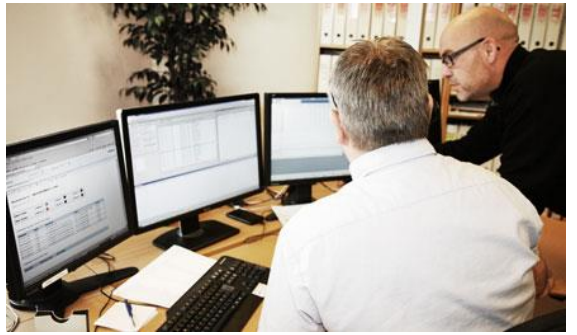
- 使用远程调试、数据采集功能
- 专用HVAC控制器安装SiteManager
- 数据采集回来存在SQL数据库
- 软件工程师完成数据可视化
- 无效告警消除、电话支持、在线调试
- 有效告警派出维护工程师现场作业

应用结果



- 监控20万传感器、18万个通风电机等
- 处理25万个告警，过滤94%的无效告警
- 6%的有效告警，1%需要现场支援
- 节约26MW用电，食物损耗率降低8%





案例：FLSmidth 全球设备状态监控系统

对全球各地的项目进行监控，基于数据为客户提供有偿的优化报告

背景与需求

- 预防性维护
- 对现场数据进行历史数据存储
- 提高现场解决问题的能力
- 为客户提供增值报告服务
- 解决IP冲突的问题

解决方案

- 替代已有的IPSec VPN解决方案
- 减少此前VPN系统维护人员数量
- 监控系统使用现有软件
- 所有项目现场安装SiteManager
- 多余的工程师转为项目维护工程师
- 快速替换，上线

应用结果

- 6个月内完成全球部署
- 总部可获取全球各地项目的实时数据
- 客户收到优化报告，延长设施利用年限
- 减少因故障停机，专家出差频繁的问题

大数据云平台

Data Cloud

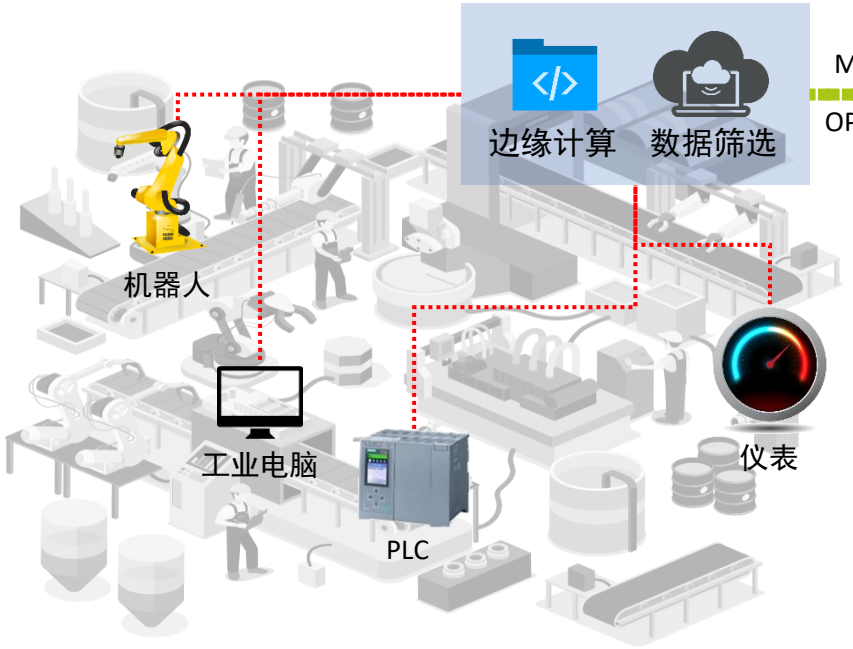
工业物联网 –西肯麦混合云架构

为公有云传输数据，轻松对接私有云，远程调试、监控均支持

secomea

远端现场

链路、协议与边缘



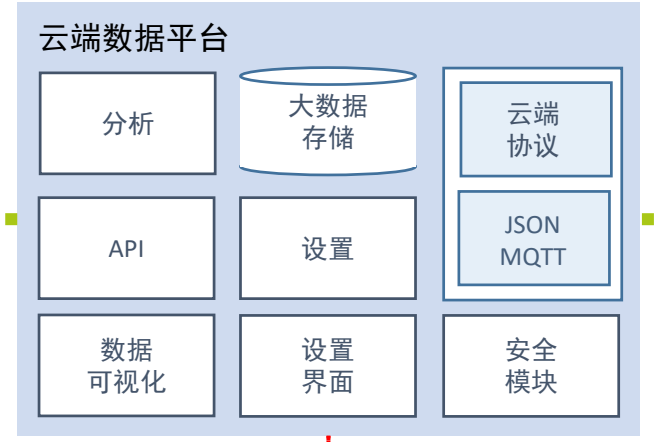
支持通过MODBUS **RTU/TCP, OPC UA**采集数据

MQTT
OPC UA
SSL
JSON
SSL
JSON

secomea

私有/云 服务器

数据存储与挖掘、安全、应用、交互



外部云PaaS　企业IT系统　其他信息系统

Windows Azure
amazon web services
ERP

SSL

客户端

可视化、管理、流程、用户体验

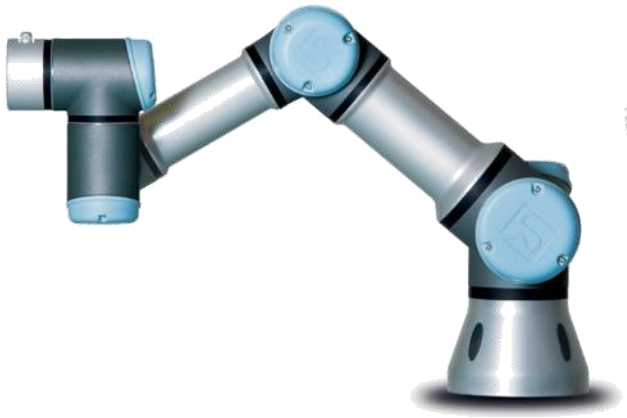
数据展示台

远程调试　移动监控　管理决策

案例：Universal Robots 优傲机器人

ACRS嵌入机器人后，获得移动示教仪、远程调试、机器人数据云的功能

LinkManager PC与移动版



联网硬件

IIoT enabled Hardware

激活您已有的“物联网”硬件 – 对接西肯麦的功能

适合于几乎所有主流的具备CPU与操作系统的硬件

secomea

工控机

基于PC的PLC

智能硬件核心板

路由器/交换机

CNC控制器

机器人

人机界面

安卓工控机/手机

已有应用案例

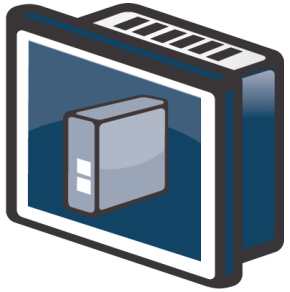
得到众多全球知名品牌的青睐

技术演示：Windows上的软件网关

激活您已有的“物联网”硬件 – 对接西肯麦的功能

Windows系统电脑

+



SiteManager软件网关

=

具备远程通信功能的电脑

操作步骤

1. 从西肯麦处获得服务器测试账号信息与相关授权
2. 前往http://www.xikenmai.com/support处下载SiteManager软件网关的程序，在Windows电脑上完成安装
3. 打开浏览器，输入http://127.0.0.1:11444并回车进入SiteManager设置页面
4. 根据软件网关入门手册，设置GateManager信息，连接至服务器，添加同网段设备即可

软件网关的安装方式

立即拥有西肯麦的所有功能

标准安装

Windows XP/7/8/10

Linux 标准发行版本

安卓

UNIVERSAL ROBOTS

订制开发

Windows CE

Linux 裁剪版本

VxWorks

secomea

- 简介
- 应用场景与案例
- 选择西肯麦远程技术

您熟悉远程通信吗？

易用、安全、稳定的远程链路，并不简单

操作追溯

登陆安全

使用便利性

192.168.2.4

企业防火墙

网络爬虫/机器人随机攻击

信息安全

中间人恶意攻击

自建服务器

大数据应用

服务器管理员

精准权限管理

工厂防火墙

设备与品牌兼容性

通信网络支持

移动/电信/联通 2/3/4G， Wi-Fi，以太网

IP冲突

如果现场IP都相同？

192.168.1.2

操作安全

远程操作时的现场人员安全

中国总部

高延时稳定性

巴西工厂

西肯麦方案亮点

不仅给您提供链路，更提供信心

secomea

誉满全球

- 19年专注工业远程
- 全球知名工控厂商背书
- 全球著名客户案例
- 销售网络遍布全球
- ……

远程安全

- 三因素权鉴登录
- 双网口物理隔离
- 国际权威机构认证
- 网络安全始终是核心关注
- ……

权限管理

- 无需IT技能即可管理
- 访问权限精确到单台设备
- 账号可禁用和解除
- 访问、操作记录可追溯
- ……

非VPN技术

- 突破VPN技术难点，将繁杂操作变简单
- 更加安全可靠，不为工业设备联网留下任何隐患
- ……

软件网关

- 已有工控硬件可嵌入软件实现联网
- 支持标准安装、定制开发
- 全球著名工控品牌嵌入案例
- ……

移动监控

- 手机即可监控设备
- 无需APP，浏览器即可实现
- 查看HMI/工控机/WEB界面
- 提供APP的API接口
- ……

可扩展性强

- 固件持续优化更新
- 新功能持续开发，新旧型号产品兼容
- 服务器部署灵活，支持一键迁移
- ……

灵活简单易用

- 联网方式：以太网/4G/WiFi
- 丰富的设备接口：RJ45/RS232/USB
- 无需专业的IT技能，零基础快速掌握
- ……

选择远程通信方案的参考

secomea

可私有化部署

整套方案可部署在企业内部
服务器可私有/公有
云平台私有化

总拥有成本

一套方案多种应用
百万级规模应用，成本透明
产品固件持续免费更新
优质的售后服务
专业而全面的技术文档中心
kb.xikenmai.com

可扩展性

产品固件定期更新
提供软件网关，部署灵活
网关可免费升级为DCM

secomea

- 西肯麦远程技术安全性介绍

secomea

西肯麦主动式安全-认证篇

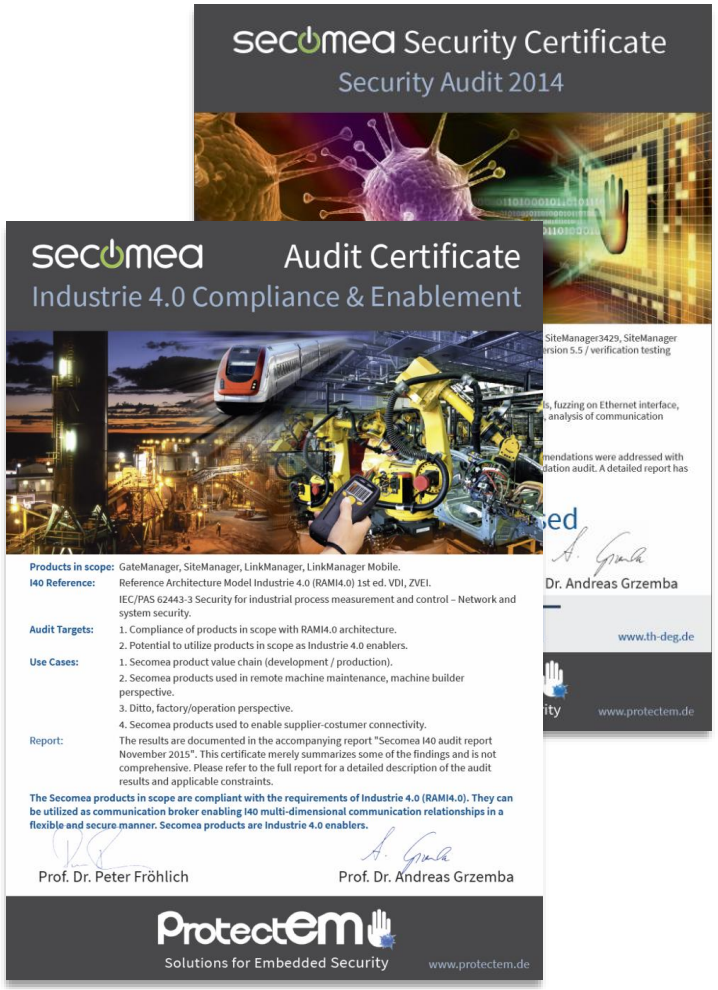
符合权威的的工控网络及信息安全标准

安全，合规，有章可循

主动式安全则是立业之本，稳定地提供通信链路是我们永恒的追求

- **通过德国第三方安全认证**
  - *ISA/IEC 62443 (前SA 99)*
    - *工控网络与系统信息安全标准*
  - *NIST (National Institute of Standards and Technology)*
    - *美国标准与技术研究院*
  - *BSI (German federal office for information security)*
    - *德国联邦信息安全办公室标准*
  - *ISECOM (Institute for Security and Open Methodologies)*
    - *国际安全与公开技术研究院*

- **通过工业4.0符合性认证**
  - *RAMI4.0 (Reference Architecture Model Industrie)*
    - *工业4.0执行委员会标准*
  - *IEC/PAS 62443-3 (Security for Industrial Process Measurement and control and system security)*
    - *工业过程测量、控制与系统安全的安全标准*

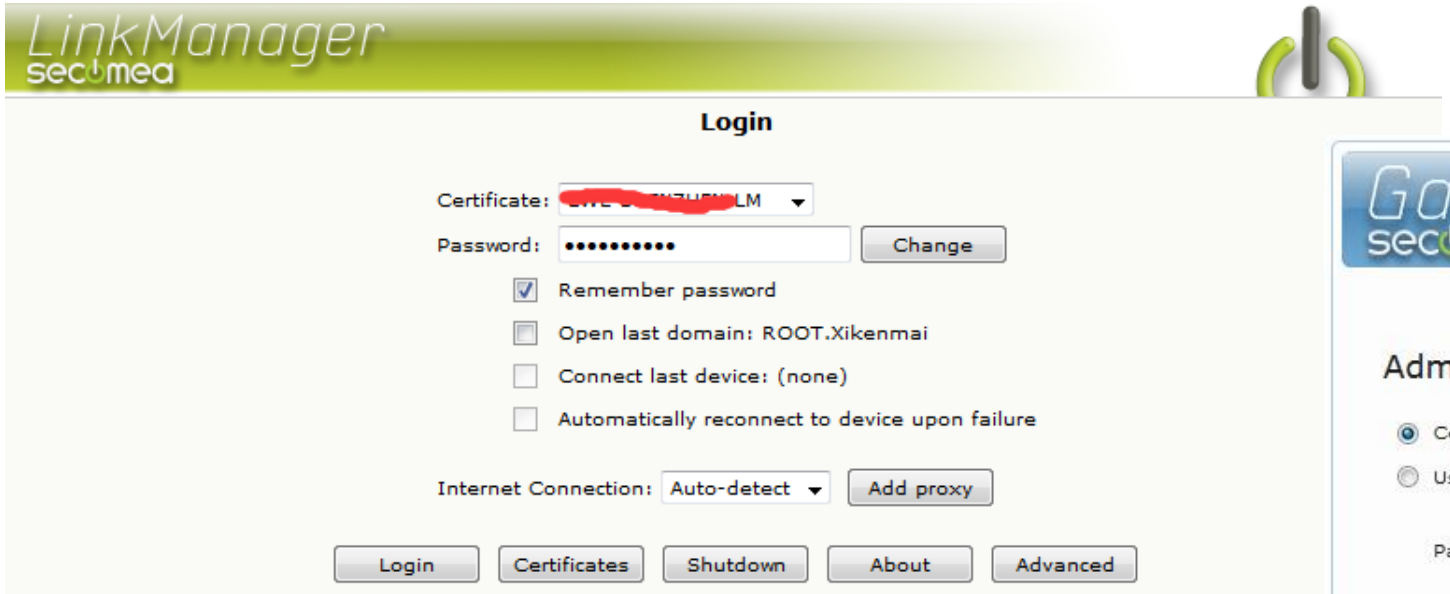


西肯麦主动式安全-技术篇

从登录、连接、管理每个环节主动防御

账号安全：三因子权鉴账号登录

密码、证书、短信三因子验证登录方式，从源头保障登录安全

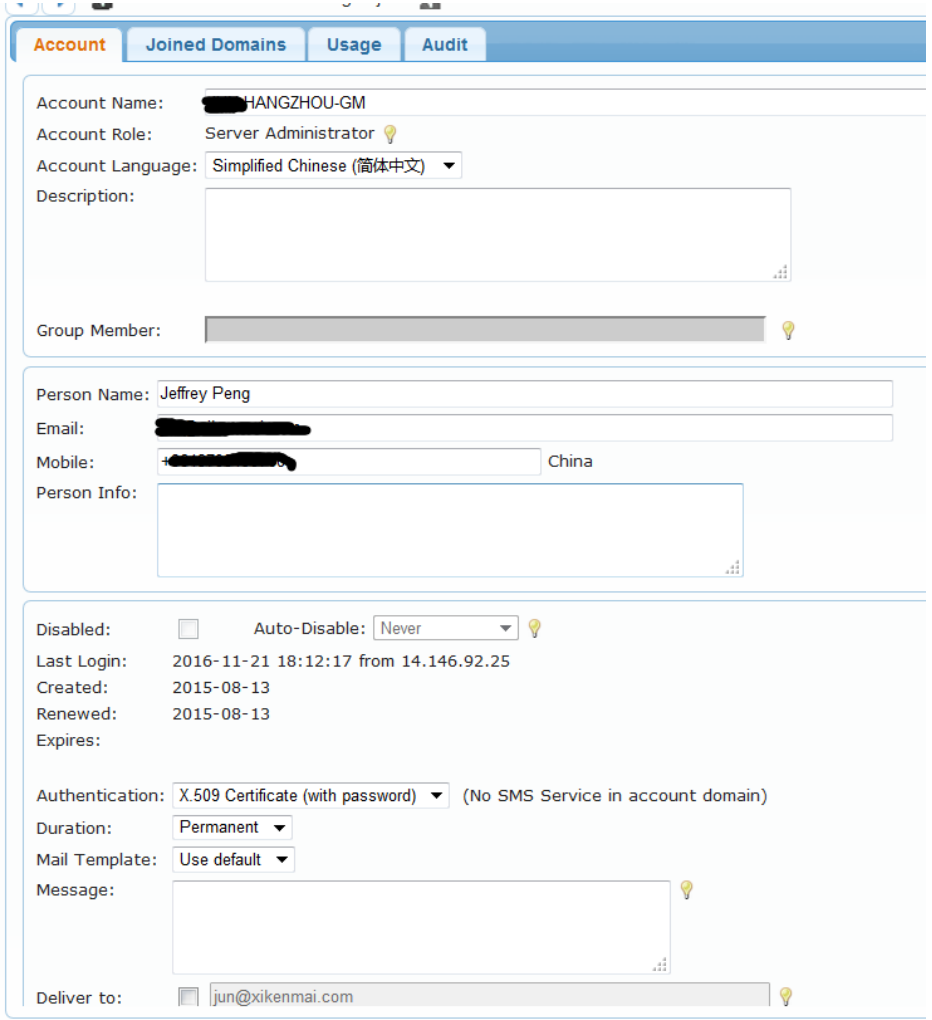


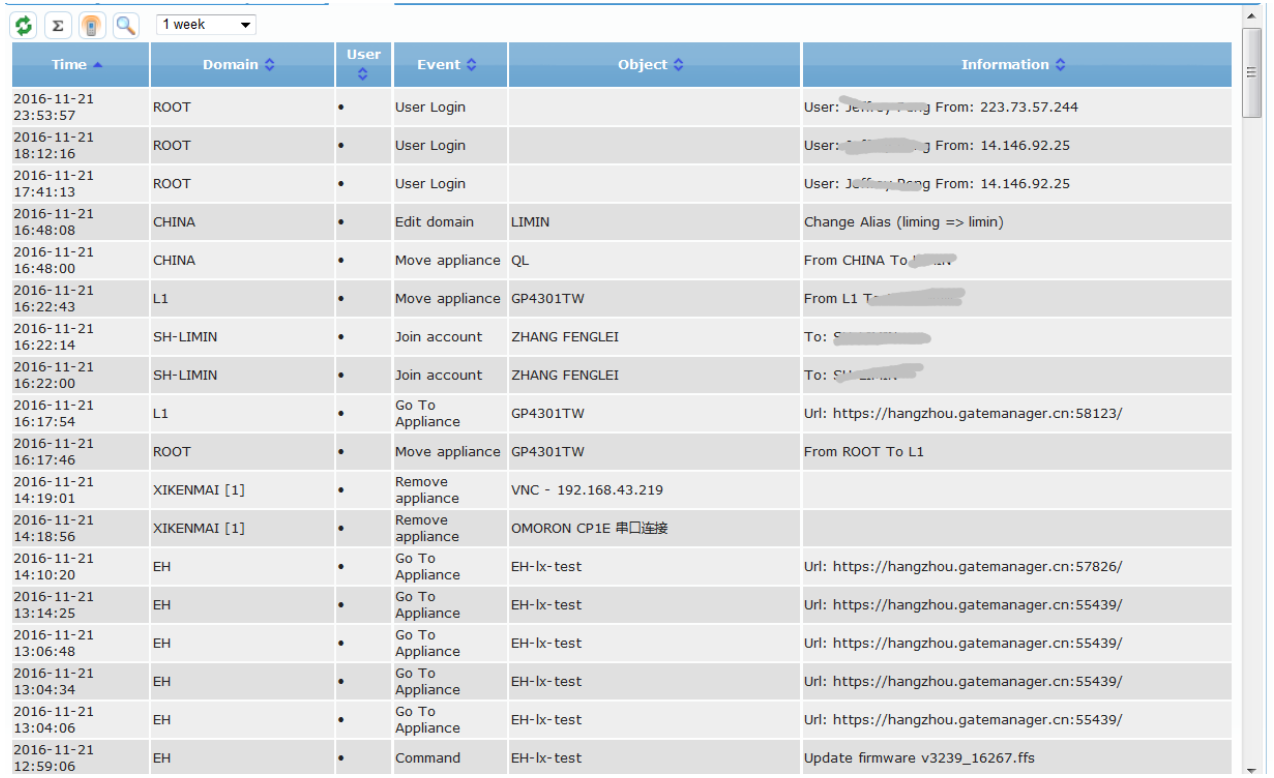
账号登录三因子验证

- 账号登录犹豫进入远程系统的大门，登录验证仅凭密码已经不足够
- 每个账号登陆都经多因素验证，具备高安全等级，保证远程连接每个环节的安全

账号管理：每个人有独立账号，各司其职

操作记录永久追溯，可按时间、登陆次数、立即生效方式禁用账号



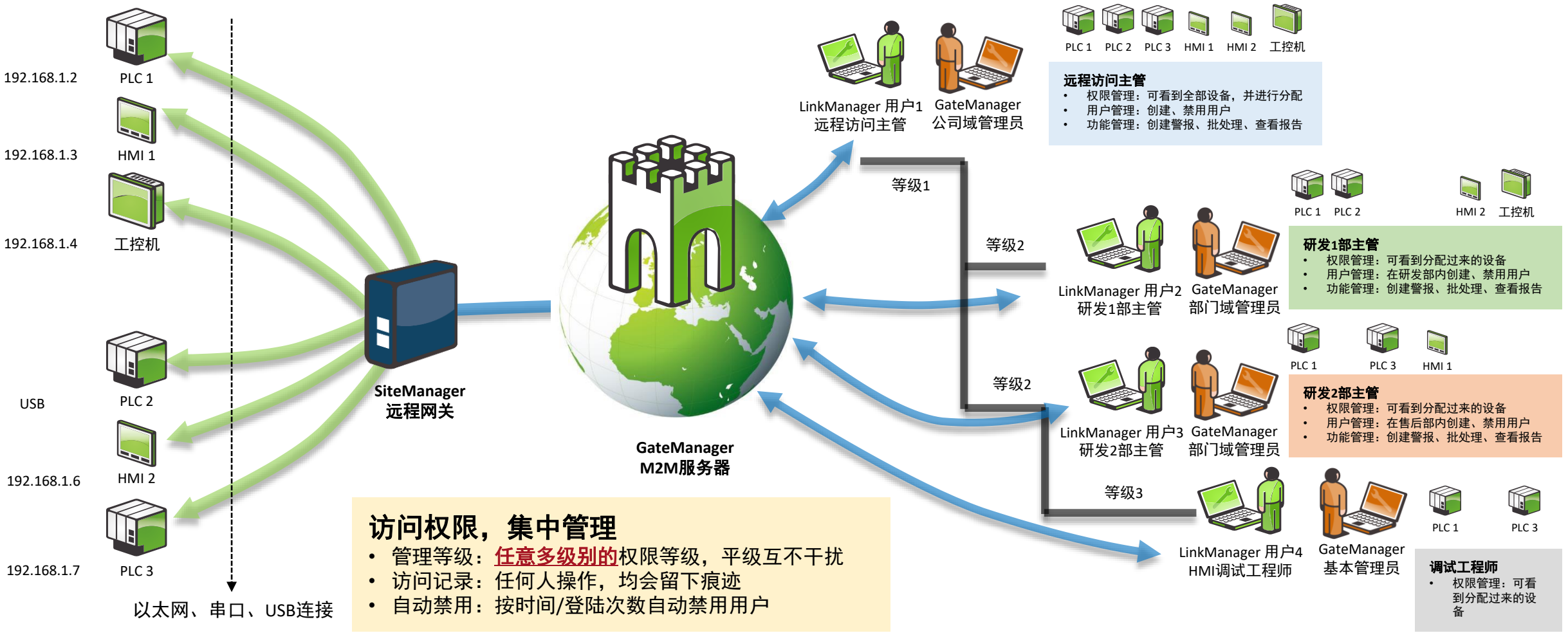


1 week

Time	Domain	User	Event	Object	Information
2016-11-21 23:53:57	ROOT	•	User Login		User: [redacted] From: 223.73.57.244
2016-11-21 18:12:16	ROOT	•	User Login		User: [redacted] From: 14.146.92.25
2016-11-21 17:41:13	ROOT	•	User Login		User: [redacted] From: 14.146.92.25
2016-11-21 16:48:08	CHINA	•	Edit domain	LIMIN	Change Alias (liming => limin)
2016-11-21 16:48:00	CHINA	•	Move appliance	QL	From CHINA To [redacted]
2016-11-21 16:22:43	L1	•	Move appliance	GP4301TW	From L1 T[redacted]
2016-11-21 16:22:14	SH-LIMIN	•	Join account	ZHANG FENGLEI	To: [redacted]
2016-11-21 16:22:00	SH-LIMIN	•	Join account	ZHANG FENGLEI	To: [redacted]
2016-11-21 16:17:54	L1	•	Go To Appliance	GP4301TW	Url: https://hangzhou.gatemanager.cn:58123/
2016-11-21 16:17:46	ROOT	•	Move appliance	GP4301TW	From ROOT To L1
2016-11-21 14:19:01	XIKENMAI [1]	•	Remove appliance	VNC - 192.168.43.219	
2016-11-21 14:18:56	XIKENMAI [1]	•	Remove appliance	OMORON CP1E 串口连接	
2016-11-21 14:10:20	EH	•	Go To Appliance	EH-lx-test	Url: https://hangzhou.gatemanager.cn:57826/
2016-11-21 13:14:25	EH	•	Go To Appliance	EH-lx-test	Url: https://hangzhou.gatemanager.cn:55439/
2016-11-21 13:06:48	EH	•	Go To Appliance	EH-lx-test	Url: https://hangzhou.gatemanager.cn:55439/
2016-11-21 13:04:34	EH	•	Go To Appliance	EH-lx-test	Url: https://hangzhou.gatemanager.cn:55439/
2016-11-21 13:04:06	EH	•	Go To Appliance	EH-lx-test	Url: https://hangzhou.gatemanager.cn:55439/
2016-11-21 12:59:06	EH	•	Command	EH-lx-test	Update firmware v3239_16267.ffs

权限管理：一个交换机下的设备如何分配权限

多层次多维度进行权限分配，各司其职，精准追溯



访问权限，集中管理

- 管理等级：任意多级别的权限等级，平级互不干扰
- 访问记录：任何人操作，均会留下痕迹
- 自动禁用：按时间/登陆次数自动禁用用户

物理隔离：现场设备不会直接连到外网

现场与公网连接设置物理隔离，最大限度保证现场设备的安全

1. GateManager:	120.25.2.135	Connected to 120.25.2.135:443 (UPLINK)	Edit
2. Uplink port:	192.168.16.153/24 (DHCP)	Up	Edit
3. Uplink2 (Mobile broadband):		Not Installed	Edit
4. DEV port:	172.24.2.1/16		Edit
5. Device Agents:	6 up, 3 down	2 failed	Fix
6. Chat / Scratchpad:	Empty		Edit
7. Admin Password:		Using default password (MAC address)	Fix

设备接口与联网接口隔离

- 设备与外网并不在同一网段
- 设备与外网接口之间设置物理隔离，现场设备与外网不会直接连接，外网不能入侵到设备网络

端口级安全：如何保护您的信息安全？

每个品牌的端口设定了然于心，每次连接时自动开放和关闭，减少人为参与

ROOT.CHINA.丹麦演示设备

丹麦设备 Siemens S7-300 6GK7-343-1GX21-0XE0 (SiteManager in Denmark) - 172.24.2.129

Agent	Address	Status	Connects		Packets		Bytes	
			ok	fail	tx	rx	tx	rx
丹麦设备 Siemens S7-300 6GK7-343-1GX21-0XE0	172.24.2.129:80,443,102,5002,5188,5800,5900,10001	IDLE	0	0	0	0	0	0
	:2308,5001,50523	IDLE	0	0	0	0	0	0
	:34964	IDLE	0	0	0	0	0	0
	:502	IDLE	0	0	0	0	0	0
	:135	IDLE	0	0	0	0	0	0
	:1099	IDLE	0	0	0	0	0	0
	:34964,50156-50164 (udp)	IDLE	0	0	0	0	0	0
	:1099 (udp)	IDLE	0	0	0	0	0	0

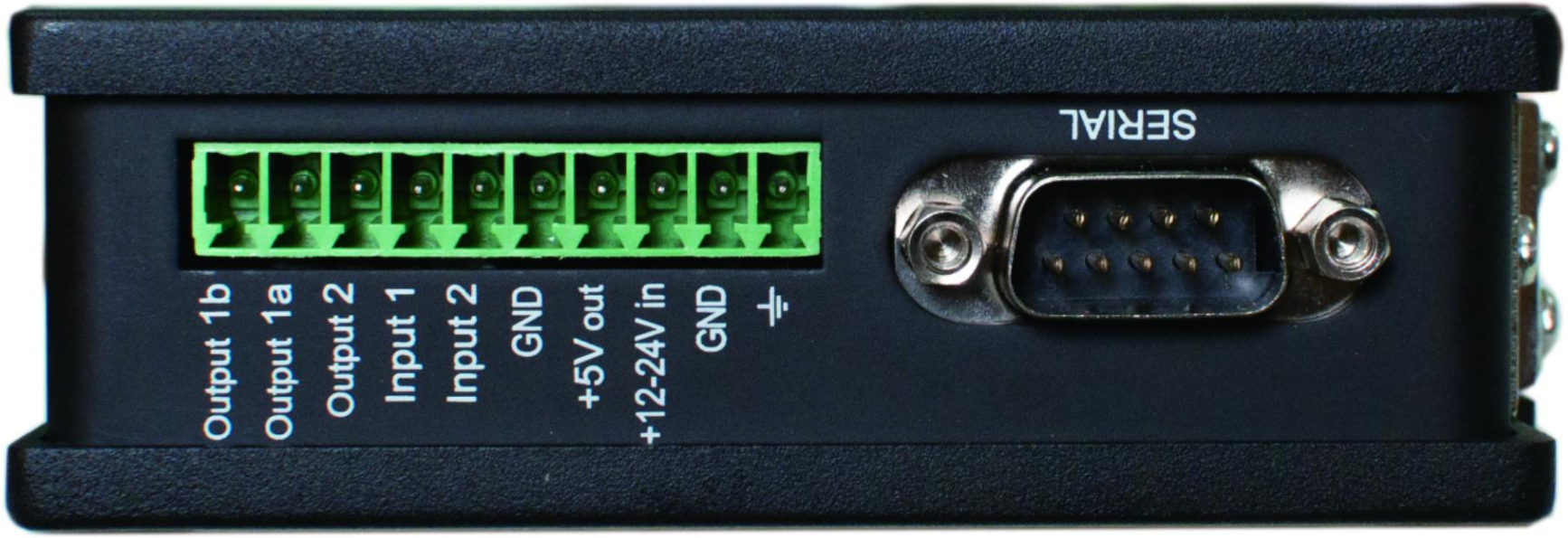
Round-trip time: Min: 422.1 ms, Avg: 562.1 ms, Max: 1011.5 ms **Bandwidth:** 128 KB/s **Auto-tune:**

西肯麦远程技术不仅仅帮您连通两个或多个设备

- 校验：在SiteManager、GateManager和LinkManager操作时，都会对授权进行匹配，防止中间人攻击，DDOS等
- 端口安全：不同于其他方案需人工应用防护策略，一般情况下连通后所有端口都是打开的，存在极大安全隐患，西肯麦端口自动开闭，避免人为设置端口或全开端口的极大风险

远程访问开关：打消最终用户的顾虑

通过I/O控制远程访问的权限

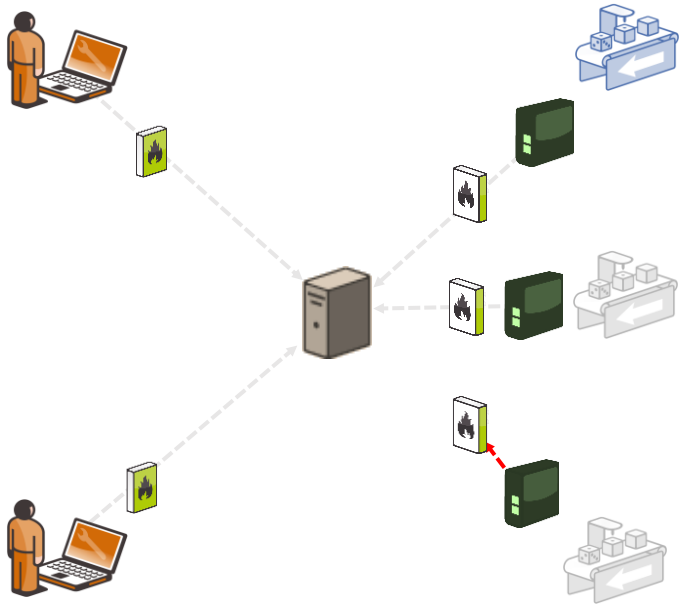


巧用I/O，功能非常强大

- DI 远程访问开关：通过Input1和GND控制两个选项，允许远程和禁止远程，由最终用户来控制。从禁止运程转换到允许远程后，在几秒钟内SiteManager就会上线，比拔网线、拔电线、卡信号都要快捷、稳定和方便
- DI PLC报警：PLC发出的电信号可通过DI转发到GateManager，然后通过电子邮件和短信的方式发给用户
- DO 连接告警：现场工作人员在设备被远程操作时应收到信号，否则有安全隐患，DO1可以接灯塔或者蜂鸣器
- DO 控制PLC断线：DO可对PLC发出信号，控制停机等

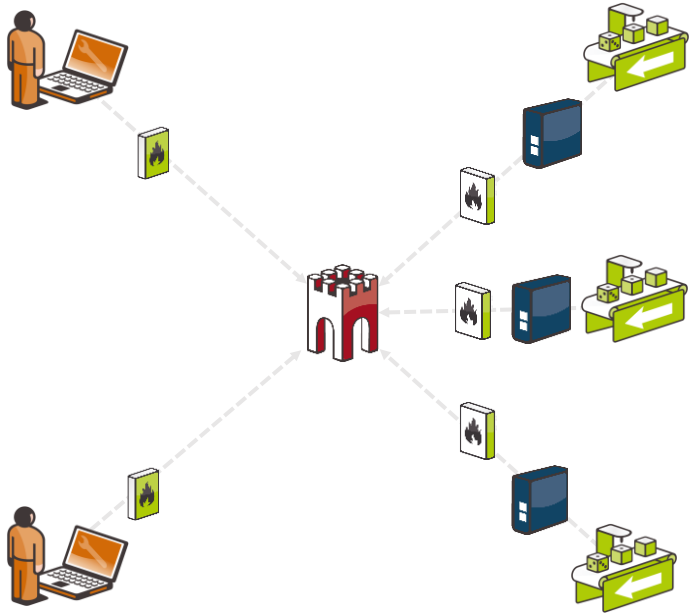
防火墙友好，不更改防火墙策略

安装在企业防火墙内，连接外网对防火墙要求少



Open SSL VPN/M2M

防火墙要求多



Secomea Relay M2M

防火墙要求少

最低要求只需开放80/443/11444端口

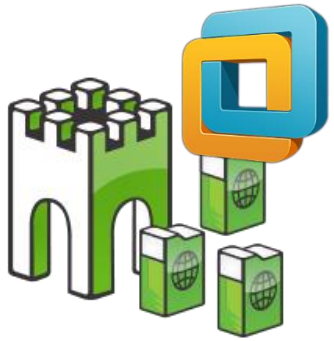
- 只要能浏览网页，就可以连接外网，进行设备连接
- 对企业防火墙要求少，无需开放过多端口或更改防火墙策略，最大限度保证企业信息安全

支持自建服务器：企业内部数据及信息全掌控

建立一套可完全由企业控制的私有化远程通信方案

硬件服务器4260

Linux服务器8250



虚拟机服务器9250

多种服务器类型选择

- 无需依赖云平台，可以建立自主控制的服务器
- 企业数据在自建的系统平台采集及传输，将数据牢牢掌握并保证私密性

工业网络安全必须给予足够重视

远程连接是工业设备必经之路，但安全的连接才是真正的连接

疫苗不安全，那远程安全吗

西肯麦SECOMEA 7月26日

"去年的WannaCry（勒索病毒）攻击事件，我想大家应该还记得吧！超过 150 个国家、10 万家组织或机构、个人超过30 万电脑受到感染，其中汽车制造商本田和雷诺都因为此次事件被迫暂停生产线。"

虽然此次事件没有直接针对工业控制系统，但令我们震惊的是勒索病毒居然能从IT网络扩散到OT网络中。

文章链接：

- https://mp.weixin.qq.com/s/OhSVa0J0WvvH9kKycYNDUA

西肯麦 secomea

可私有化部署的非VPN工业远程通信方案

设备制造商 | 系统集成项目 | 工厂 | 硬件设备商

远程调试 | 移动监控 | 数据采集 | 跨网络架构 | 数据上云 | 软件网关

了解西肯麦