http://www.aii-alliance.org/statics/images/logo.png

工业互联网

典型安全解决方案案例汇编

v1.0.0

2018年xx月

工业互联网产业联盟 发布

目 录

[**1**．**工业互联网安全概述** 4](#_Toc507425341)

[2．XXXX行业典型安全解决方案 5](#_Toc507425342)

[2.1案例一:xxxx安全解决方案 5](#_Toc507425343)

[2.1.1概述 5](#_Toc507425344)

[2.1.2典型安全问题 5](#_Toc507425345)

[2.1.3安全解决方案 5](#_Toc507425346)

[2.1.4小结 5](#_Toc507425347)

[2.2案例二：xxxx安全解决方案 5](#_Toc507425348)

[3．xxxx行业典型安全解决方案 6](#_Toc507425349)

[8．结束语 6](#_Toc507425350)

[附录：2017年汇编中的某案例，供参考。 7](#_Toc507425351)

[某石油石化企业安全解决方案 7](#_Toc507425352)

[概述 7](#_Toc507425353)

[典型安全风险 7](#_Toc507425354)

[解决方案 7](#_Toc507425355)

[典型部署 8](#_Toc507425356)

[小结 9](#_Toc507425357)

前 言

为落实《中国制造2025》规划……

□□□□□□□□□□□□□□

工业互联网产业联盟 安全组

二〇一八年xx月

1．工业互联网安全概述

工业……

□□□□□□□□□□□□□□。

# 2．□□□□行业典型安全解决方案

□□□□□□□□□□□□□□

【编者注】

建议2018年的典型案例在2017年案例汇编V1.0的基础上，可适当侧重于工业互联安全（设备、控制、网络等安全）、工业云平台安全、工业大数据安全、工业应用安全等领域，具体内容包括但不限于安全防护、安全等级保护、安全检测、安全态势感知、威胁情报与风险预警、响应与处置等。

## 2.1案例一：□□□□安全解决方案

### 2.1.1方案概述

□□□□□□□□□□□□□□

【编者注：】

本领域/应用的产业现状及前景、技术现状、发展趋势及挑战

本领域/行业/应用的产业现状、发展前景，技术现状、发展趋势、安全风险及挑战。

### 2.1.2典型安全问题

□□□□□□□□□□□□□□

【编者注】

本方案主要解决的问题、价值体现

### 2.1.3安全解决方案

□□□□□□□□□□□□□□

【编者注】

本方案的技术架构、部署架构、组网方式、……

本方案的关键组件、核心功能、技术指标、……

本方案的创新点、先进性、实用性、效益、……

本方案的适用场景、对平台/软硬件的要求

此部分为重点内容，其篇幅应占全案例的3/4~4/5。

### 2.1.4小结

□□□□□□□□□□□□□□

【编者注】

本方案的特点、优劣势；

选择本方案的理由。

案例提供方：□□□□公司

每个典型案例文档篇幅在4~8页（按当前文档模板的字体大小、行间距、段间距等）

### 2.1.5单位基本信息

□□□□□□□□□□□□□□

【编者注】

本方案贡献单位的基本信息，限500字以内。

## **2.2案例二：**□□□□**安全解决方案**

□□□□□□□□□□□□□□

# 3．xxxx行业典型安全解决方案

□□□□□□□□□□□□□□

# 8．结束语

□□□□□□□□□□□□□□

## 附录：2017年汇编中的某案例，供参考。

## 某石油石化企业安全解决方案

### 概述

通过分析石油企业在各生产环节中所面临的信息安全问题，提出了保障生产信息网络安全的防护解决方案，同时具体提出了企业应采取的安全策略和解决措施，阐明了全面构筑工控信息安全体系，消除网络安全隐患，做到防患于未然。

### 典型安全风险

1. 油田网络容易遭受病毒等恶意代码的侵袭；
2. 缺乏监测及防御人为恶意或者无意的违规操作行为的技术手段；
3. 对外部、内部的网络攻击行为缺乏防御手段；
4. 安全事件发生后不能迅速定位找出问题根源。

### 解决方案

1. 针对油田各生产环节的网络边界和各网络内部区域之间的采取安全隔离和访问控制措施，防止用户的越权访问和非法入侵行为；
2. 对工控网络中的场站服务器、实时数据库、生产调度系统等主机进行加固，保障主机及其运行数据的安全；
3. 提供安全数据交换介质，杜绝移动存储介质“滥用”的安全隐患，保障工控主机间数据交换安全；
4. 提供工控网络操作行为监测审计功能，帮助企业建立网络监测审计机制；
5. 对油田各层级网络中的安全设备或系统进行集中管理，实现全局配置、集中监控、统一管理，提高管理人员的工作效率，降低企业的人员投入成本。

### 典型部署

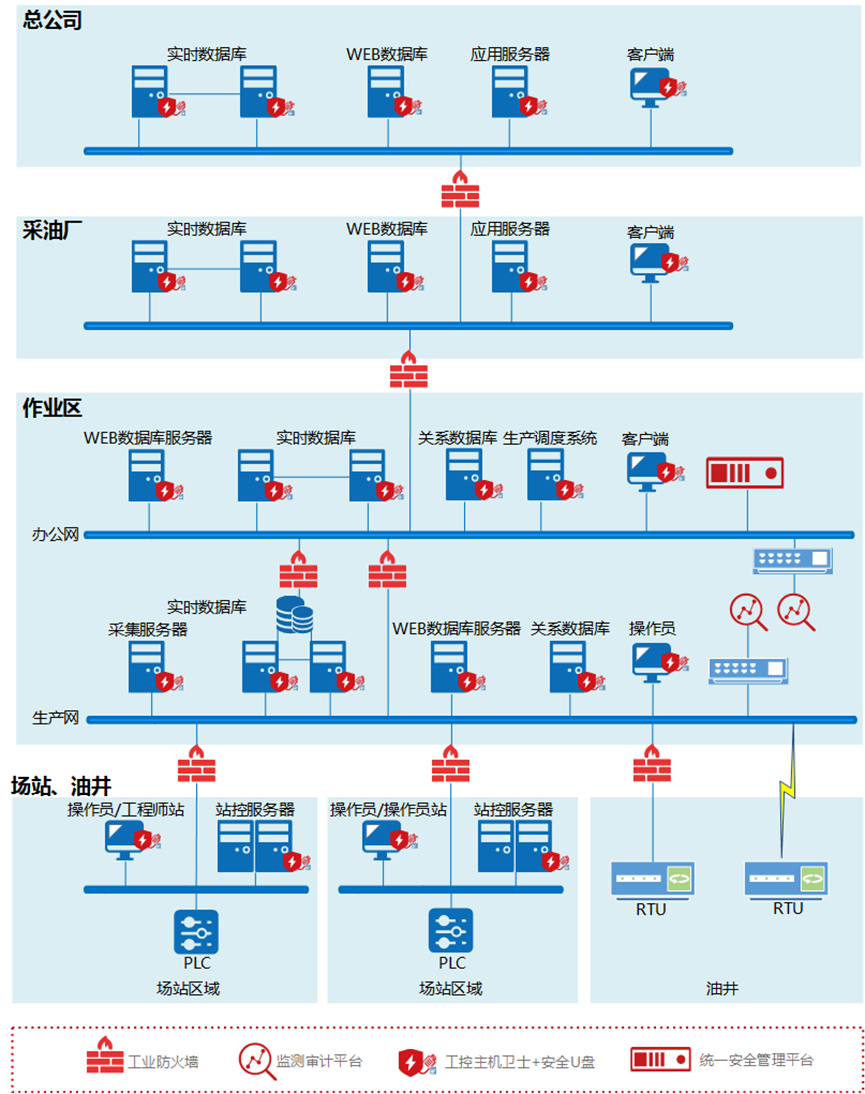


图 19工控安全规划与访问控制拓扑图

1. 边界、区域边界防护

在采油厂、作业区、场站油井边界及作业区区域边界部署工业防火墙，对各层级用户和外来的访问进行控制，保障采油厂、作业区等重要生产区域网络的可用性和安全性。

1. 主机安全防护

在采油厂、作业区、场站油井的实时数据库、关系数据库、生产调度系统等重要主机系统部署工控主机卫士。采用“白名单”防护机制，保证只有安全的软件程序才能够在主机系统中运行，同时对主机操作系统、注册表等进行防护。

1. 数据交换安全

采用安全U盘作为数据交换介质，避免不安全的移动存储介质进入工控网络影响生产网络的正常运行。

1. 网络监测审计

在作业区的办公网和生产网旁路部署监测审计平台，监控和记录用户对数据库、生产调度系统、采集服务器的违规操作、误操作行为，为事后调查取证提供依据。

1. 集中管理

在作业区的办公网中部署统一管理平台，对整个工控网络中的安全设备和系统进行统一策略配置下发、状态集中监控、网络流量分析。实时掌握工业控制网络运行状态，便于出现问题及时溯源定位。

**【编者注：2018年案例汇编中，建议在方案细节部分，多体现一些技术细节、技术先进性、技术实用效果等】**

### 小结

该解决方案具备如下特点：

1. 阻止病毒、蠕虫恶意软件扩散和入侵攻击，保护控制系统安全运行；
2. 阻止非授权软件或进程的安装和运行，防止恶意代码攻击；
3. 防止操作员使用移动介质带入的病毒在生产网中扩散；
4. 实时检测工控网络中的恶意攻击、误操作、违规行为、非法设备接入以及蠕虫、病毒等恶意软件的传播，帮助客户及时采取应对措施，避免发生安全事故。