ICS 25.040
N 10

# 中华人民共和国国家标准

GB/T 33863.2—2017/IEC/TR 62541-2:2010

# OPC 统一架构　第 2 部分:安全模型

**OPC unified architecture—Part 2: Security model**

(IEC/TR 62541-2:2010,IDT)

2017-07-12 发布　　2018-02-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

# 目　　次

前言 …… Ⅲ
引言 …… Ⅳ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语、定义、缩略语和约定 …… 1
3.1　术语和定义 …… 1
3.2　缩略语 …… 4
3.3　关于安全模型图的约定 …… 5
4　OPC UA 安全结构 …… 5
4.1　OPC UA 安全环境 …… 5
4.2　安全目标 …… 6
4.2.1　概述 …… 6
4.2.2　鉴别 …… 6
4.2.3　授权 …… 6
4.2.4　机密性 …… 6
4.2.5　完整性 …… 6
4.2.6　可审核性 …… 6
4.2.7　可用性 …… 6
4.3　对 OPC UA 系统的安全威胁 …… 6
4.3.1　概述 …… 6
4.3.2　消息洪泛 …… 6
4.3.3　窃听 …… 7
4.3.4　消息欺骗 …… 7
4.3.5　消息改变 …… 7
4.3.6　消息重放 …… 7
4.3.7　畸形消息 …… 7
4.3.8　服务器剖析(profiling) …… 8
4.3.9　会话劫持 …… 8
4.3.10　欺诈服务器 …… 8
4.3.11　用户凭证泄密 …… 8
4.4　OPC UA 与站点安全的关系 …… 8
4.5　OPC UA 安全架构 …… 9
4.6　安全策略 …… 10
4.7　安全行规 …… 10
4.8　用户授权 …… 11
4.9　用户鉴别 …… 11
4.10　应用鉴别 …… 11

4.11 OPC UA 安全相关服务 …… 11
4.12 审核 …… 11
4.12.1 概述 …… 11
4.12.2 单个客户端和服务器 …… 12
4.12.3 聚合服务器 …… 12
4.12.4 通过非审核服务器聚合 …… 13
4.12.5 具有服务分发的聚合服务器 …… 14
5 安全协调 …… 15
5.1 针对威胁的 OPC UA 安全机制 …… 15
5.1.1 概述 …… 15
5.1.2 消息洪泛 …… 15
5.1.3 窃听 …… 16
5.1.4 消息欺骗 …… 16
5.1.5 消息变化 …… 16
5.1.6 消息重放 …… 16
5.1.7 畸形消息 …… 16
5.1.8 服务器剖析(Server profiling) …… 16
5.1.9 会话劫持 …… 16
5.1.10 欺诈服务器 …… 17
5.1.11 用户凭证泄密 …… 17
5.2 面向实现目标的 OPC UA 安全机制 …… 17
5.2.1 概述 …… 17
5.2.2 鉴别 …… 17
5.2.2.1 概述 …… 17
5.2.2.2 应用鉴别 …… 17
5.2.2.3 用户鉴别 …… 17
5.2.3 授权 …… 17
5.2.4 机密性 …… 18
5.2.5 完整性 …… 18
5.2.6 可审核性(Auditability) …… 18
5.2.7 可用性 …… 18
6 实现考虑 …… 18
6.1 概述 …… 18
6.2 适当的超时 …… 18
6.3 严格消息处理 …… 18
6.4 随机数生成 …… 19
6.5 特定和保留数据包 …… 19
6.6 速率限制和流量控制 …… 19
参考文献 …… 20

# 前　言

GB/T 33863《OPC 统一架构》由以下各部分组成：

——第 1 部分：概述和概念；

——第 2 部分：安全模型；

——第 3 部分：地址空间模型；

——第 4 部分：服务；

——第 5 部分：信息模型；

——第 6 部分：映射；

——第 7 部分：规约；

——第 8 部分：数据访问；

——第 9 部分：报警和条件；

——第 10 部分：程序；

——第 11 部分：历史访问；

——第 12 部分：发现；

——第 13 部分：聚合。

本部分是 GB/T 33863 的第 2 部分。

本部分按照 GB/T 1.1—2009 给出的规则起草。

本部分使用翻译法等同采用 IEC/TR 62541-2:2010《OPC 统一架构　第 2 部分：安全模型》。

本部分做了下列编辑性修改：

——删除与规范性引用文件重复的参考文献。

本部分由中国机械工业联合会提出。

本部分由全国工业过程测量控制和自动化标准化技术委员会(SAC/TC 124)归口。

本部分起草单位：机械工业仪器仪表综合技术经济研究所、北京三维力控科技有限公司、上海自动化仪表有限公司、重庆川仪自动化股份有限公司、西南大学、中国工程物理研究院动力部。

本部分主要起草人：王麟琨、王春喜、李云、丁露、王玉敏、丁研、张庆军、姚杰、刘枫、郑秋平。

# 引　言

本部分为GB/T 33863规定的OPC统一架构提供了安全模型。本标准给出了为开发标准接口而进行分析和设计的过程，该标准接口可加快由多个供应商完成的应用开发，并实现内部操作的无缝连接。

# OPC 统一架构　第 2 部分:安全模型

## 1　范围

GB/T 33863 的本部分给出了 OPC 统一架构(UA)安全模型,描述了 OPC UA 预期要运行的物理、硬件和软件环境中的安全威胁,以及 OPC UA 如何利用其他标准实现安全。本部分给出了在 OPC UA 其他规范中规定的安全特性的概述。本部分引用了在本标准其他部分做了规范性规定的服务、映射和行规。

注:在开发应用时,需解决安全性的许多其他方面。鉴于 OPC UA 规定了一个通信协议,所以本部分关注于保护应用间数据交换的安全。

这并不意味着应用开发者可以忽略其他方面的安全,如保护永久性数据免遭篡改。开发者应观察所有安全内容,并确定在应用中如何处理。

本部分用于指导开发 OPC UA 客户端或服务器应用,或实现 OPC UA 服务层。

本部分假定读者熟悉 Web 服务和 XML/SOAP。关于这些技术的信息,可参考 SOAP 第 1 部分和第 2 部分。

## 2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

IEC 62541 (所有部分)　OPC 统一架构(OPC unified architecture)

IEC/TR 62541-1　OPC 统一架构　第 1 部分:概述和概念(OPC unified architecture—Part 1: Overview and concepts)

## 3　术语、定义、缩略语和约定

### 3.1　术语和定义

IEC/TR 62541-1 界定的以及下列术语和定义适用于本文件。

3.1.1

**应用实例　Application Instance**

在一台计算机上运行的一个单独安装的程序。

注:同一应用的几个应用实例可以同时在一台或多台计算机上运行。

3.1.2

**应用实例证书　Application Instance Certificate**

已安装在单个主机中的单个应用实例的数字证书。

注:一个软件产品的不同安装应有不同的应用实例证书。

3.1.3

**非对称密码术　Asymmetric Cryptography**

使用一对密钥的加密方法。一个密钥指定为私有密钥,不公开;另一个密钥称为公开密钥,通常可获得。