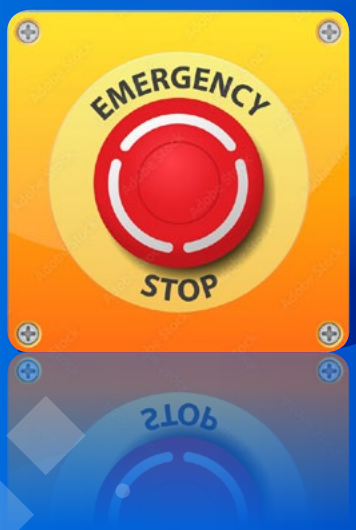
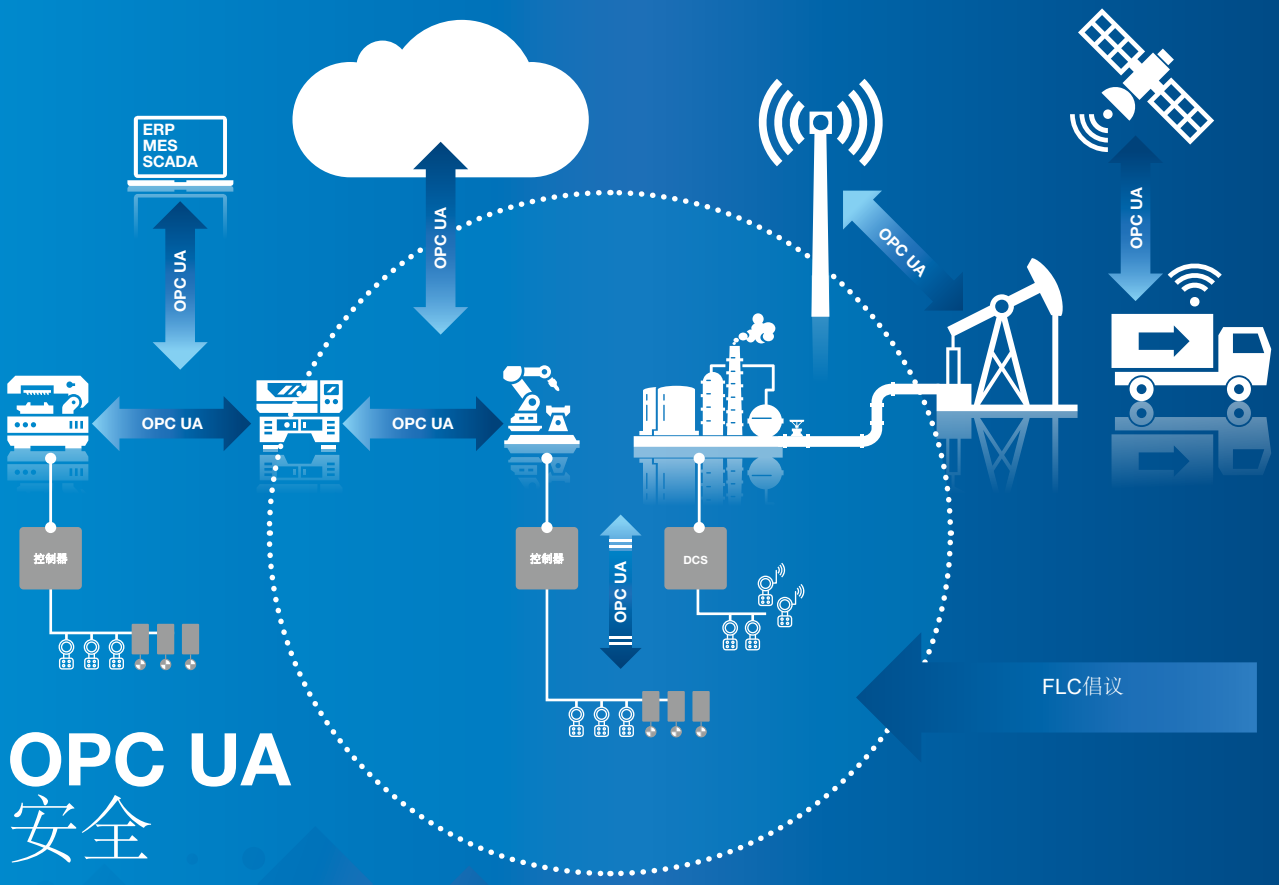
OPC UA 安全:
通过OPC UA实现功能安全通信

版本 1 // 2022年9月



技术手册

OPC UA实现功能
安全通信



OPC UA
安全

目录

OPC UA安全: OPC UA实现功能安全通信

模块化机器和动态系统的安全通信

OPC UA安全 （OPC 10000-15 统一架构 第15部分）定义了一个功能安全层，用于工业控制器之间通过标准化、独立于供应商接口的通信。它在应用层支持单播和多播通信，以及长度可达1500字节的任意结构的安全数据。

这些安全措施符合所有相关的安全标准。OPC UA安全使得构建模块化机器成为可能，其中安全功能可适应机器的实际配置。甚至可以实现那些在运行时需要更换通信对象的安全功能，例如在使用OPC UA 安全的自主移动机器人场景。

里程碑

→ 2018年2月： “基于 OPC UA 的 PROFIsafe”联合工作组举行启动会议，该工作组由 OPC 基金会与 PI组织（Profibus & Profinet International）共同组建。

→ 2019年4月: OPC 基金会的现场级通信（FLC）倡议决定将其用于安全数据交换，工作组也被纳入该倡议。

→ 2019年7月: 规范更名为“OPC UA 第 15 部分：安全”，并成为 OPC 核心规范集的一部分。

→ 2019年10月: 发布规范 1.04 版本（IEC 61784 - 3标准 ，TÜV Süd评估。）

→ 2019年10月: FLC倡议资助开发 OPC UA 安全测试工具

→ 2020年3月: FLC倡议资助开发协议栈，并邀请其他公司参与。

→ 2020年7月: 发布版本1.04

→ 2021年11月: 发布版本1.05

引言

功能安全通信的现有技术在IEC61508 [1]、IEC 62280 [2] 和 IEC 61784-3 [3] 等标准中已有相关描述。这些标准阐述了如何通过一个标准的（非安全）通信通道传输与安全相关的消息。只有当接收器能够以与安全相关的方式，以有保证的检测概率检测到所有传输错误时，才能实现这种传输。如今，几乎所有的现场总线协议都提供了用于安全通信的相关配置文件。这使得安全相关的控制器能够通过标准通信通道与属于安全功能的传感器和执行器进行通信，不再需要为功能安全相关的数据交换设置单独的通信通道。然而，机器之间的通信需要支持控制器到控制器通信的安全协议，因为每台机器甚至每个机器模块通常都由一个控制器来代表。但到目前为止，还没有独立于制造商的开放标准适用于此类安全通信。现在，OPC UA 安全规范正在填补这一空白。机器之间（或机器模块之间）的功能性安全通信在多种不同场景中都具有重要意义。典型的例子包括传输线、电动单轨系统以及带有模块化装卸系统的机床。其他场景还包括能够停靠在机器上并执行安全功能的自主移动机器人（AMR）。例如，当按下靠在机器上的AMR紧急停止按钮时，则机器运行也相应需要停止，这就是一个常见的安全功能。

OPC UA 安全规范正是针对此类场景设计的。具体而言，它具备以下特性和功能:

- → 在应用层支持单向、双向通信以及多播
- → 适用于任何网络拓扑结构，如星形、线形、环形、网格形等.
- → 可传输多达 1500 字节的安全用户数据
- → 支持在运行时动态建立连接.

从功能安全角度来看，OPC UA安全规范基于广泛使用的PROFIsafe协议[4]。由于它基于OPC UA构建，因此继承了以下特性:

- → 单传输通道上同时进行安全相关通信和标准通信
- → 支持任意数据速率
- → 对网络中非安全相关节点没有任何与安全相关的要求
- → 对网络组件（如交换机）没有与安全相关的要求
- → 无需进行安全时钟同步

OPC UA安全规范的一些独特优势:

- → 支持多供应商之间的控制器到控制器（C2C）、控制器到设备（C2D）以及设备到设备（D2D）的互操作性通信
- → 高度灵活——适用于运输、过程与工厂自动化、运动控制等领域
- → 可扩展性强——从SIL1 到 SIL4 均可支持
- → 支持动态应用场景——能够对机器和工厂进行动态重新配置。
- → 数据有效负载大——可从简单应用扩展到复杂的大量应用
- → 能够穿越路由器——可从单台机器扩展到全厂范围的操作
- → 在资源受限的终端节点上易于部署（商业协议栈的可用性进一步增强了这一优势）

手册首先对OPC UA安全规范进行概述（第1章），然后描述其架构（第2章），最后总结验证协议安全性的基本原理（第3章）.

1. 概述

1.1 服务

OPC UA 安全规范进行安全数据交换的基本原理是在安全数据发布端（SafetyProvider，数据源）和安全数据接收端（SafetyConsumer，数据接收器）端点之间建立直接的点对点连接。根据其各自的作用，安全数据源从本地安全应用程序接收用户数据，并通过 OPC UA 服务将其提供出来。数据接收器使用 OPC UA 服务检索用户数据，并将其提供给本地安全应用程序。因此，这是一个请求/响应过程，如图 1 所示。

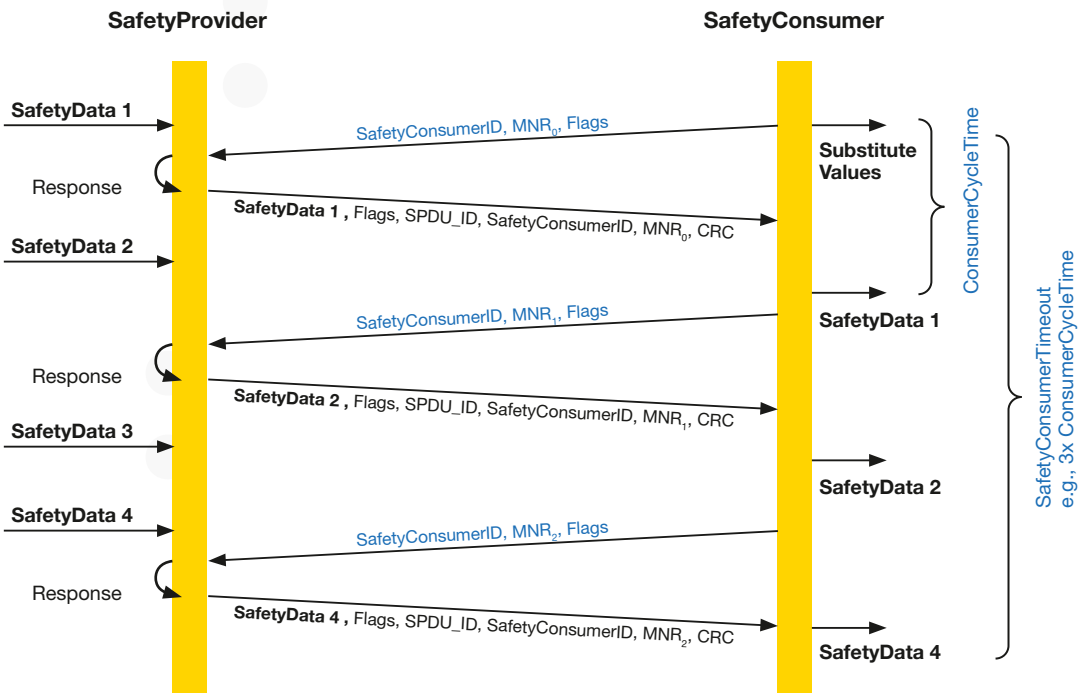


图 1: 请求/响应流程的 OPC UA 安全连接序列图

1.2 安全措施

为了检测传输错误，会在与安全相关的请求和响应消息中添加相关的附加信息。本质上，这涉及到用于检查各个数据源的全系统唯一标识符（ID）、用于检查正确顺序的监控编号（MNR）以及用于检测数据损坏的 CRC 签名。无需发送时间戳，因为安全数据接收器仅使用其本地时钟就可以检查响应安全协议数据单元（ResponseSPDU）的及时性。这意味着无需同步安全数据源和数据接收器的时钟。

1.3 唯一标识符（ID）

OPC UA 安全规范使用不同的 ID 来检测寻址错误。每个安全数据源都被分配一个唯一的发布端 ID（ProviderID），该 ID 首先会告知安全数据接收端。与其他信息（例如，显示所发送用户数据结构的签名）一起，根据发布端 ID 计算出一个安全协议数据单元 ID（SPDU_ID），该 ID 包含在每个响应安全协议数据单元（ResponseSPDU）中。基于 SPDU_ID，安全数据接收端可以检查接收到的安全协议数据单元是否来自预期的安全数据源。在大型系统中，分配唯一 ID 可能需要大量的管理工作。如果工厂的不同部分由不同的厂商建造，情况尤其如此。最初使用多台相同类型的机器以及相关自动化项目的克隆也会导致相同 ID 并存，然后必须手动更改这些 ID 以排除其重复出现的情况。

为了减少管理 ID 所需的工作量，每个安全数据源还包含一个基础 ID（BaseID），该 ID 也包含在 SPDU_ID 中并由安全数据接收端进行检查。并非每个安全数据源都需要唯一的基础ID；相反，这些基础 ID 是为整个工厂车间或机器共同分配的。例如，如果两个集成商正在参与一个工厂的建设，每个集成商将使用不同的基础 ID，那么每个集成商分配的发布端 ID 保持唯一就足够了。在批量生产的机器克隆项目时，为每台机器重新生成一个单独的基础 ID 就足够了。由于发布端 ID 不会改变，因此项目克隆后无需检查所有 ID 的唯一性。基础 ID 是一个由随机数生成器生成的128 位的值。例如，在实际应用中，可以在此处生成通用唯一标识符（UUID，[8]），而且有足够的概率证明不会出现两个相同的基础 ID。因此，无需明确检查所有工厂部件是否具有不同的基础 ID。在某些应用中，告知安全数据源当前与其通信的安全数据接收端可能是有意义的。为此，安全数据接收端也会获得一个相关的接收端ID（ConsumerID）。然而，由于仅检查安全数据源的身份就足以进行安全响应，因此接收端 ID 与安全无关。

1.4 通信模式

在实际应用中，除了直接的点对点连接外，安全应用程序中还会出现双向连接和点对多点连接（多播）。在 OPC UA 安全规范中，这是通过使用多个安全数据源/安全数据接收端对来实现的，如图 2 所示。

由于安全数据源需要进行多次实例化，与使用下层现有多播机制的解决方案相比，多播会产生一定的开销。然而，OPC UA 安全规范有相关规定，使得安全数据源在内存和计算能力方面都能以高效的方式实现。

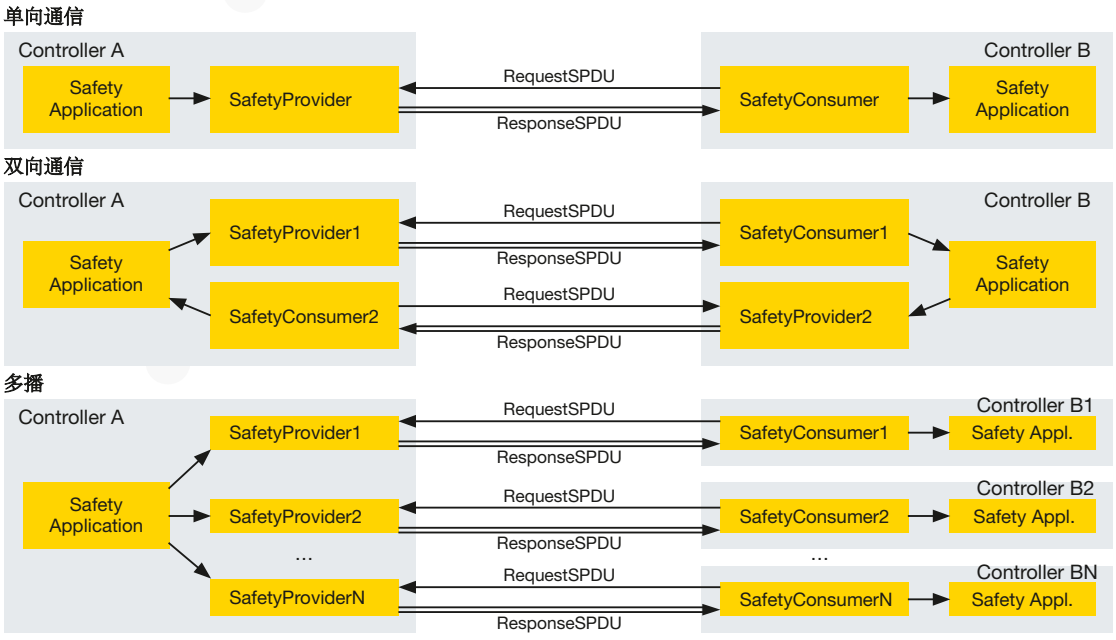


图2: 通信模式: 单向和双向单播以及多播通信

2. 架构

2.1 概述与接口

OPC UA 安全遵循 IEC 61784 - 3（现场总线功能安全，[2]）中推荐的方法，如图 3 所示。OPC UA 安全这一层是插入在安全应用程序和作为标准（非安全）通信通道实现的底层网络层之间。OPC UA 安全堆栈层的功能是检查在标准通道上传输的所有安全消息的完整性，并在此基础上检测通信错误，最后将正确的用户数据传递给安全应用程序。这提供了控制所有通信错误的能力，但不包括终端节点本身的错误。因此，OPC UA 安全（安全数据源与接收端）必须按照 IEC 61508 [1] 来实现。具体而言，一方面涉及克服随机硬件错误的措施，另一方面涉及克服系统性硬件和软件错误的措施。

为了更方便地适应不同的底层通信服务，通过OPC UA 映射器实现与 OPC UA 堆栈的连接。由于该映射器不属于安全相关通信层，因此无需对实现 OPC UA 安全进行任何重新的评估。目前，OPC UA 映射器支持远程方法调用（OPC UA 客户端/服务器）以及 OPC UA 发布 - 订阅模式。安全应用程序接口（SAPI）也特定于应用程序，因为不同的应用程序会交换不同的数据。然而，与 OPC UA 中的惯例一样，该接口也可以通过配套规范在独立于制造商的基础上定义（例如特定行业）。除了 SAPI 和通过 OPC UA 映射器与 OPC UA 连接之外，安全数据源和接收端各自还有一个安全参数接口（SPI）和一个诊断接口。安全协议数据单元（SPDU）在安全数据源和接收端之间交换，一方面由请求 SPDU 和响应 SPDU 这一结构定义，另一方面由发布端和接收端状态机定义。

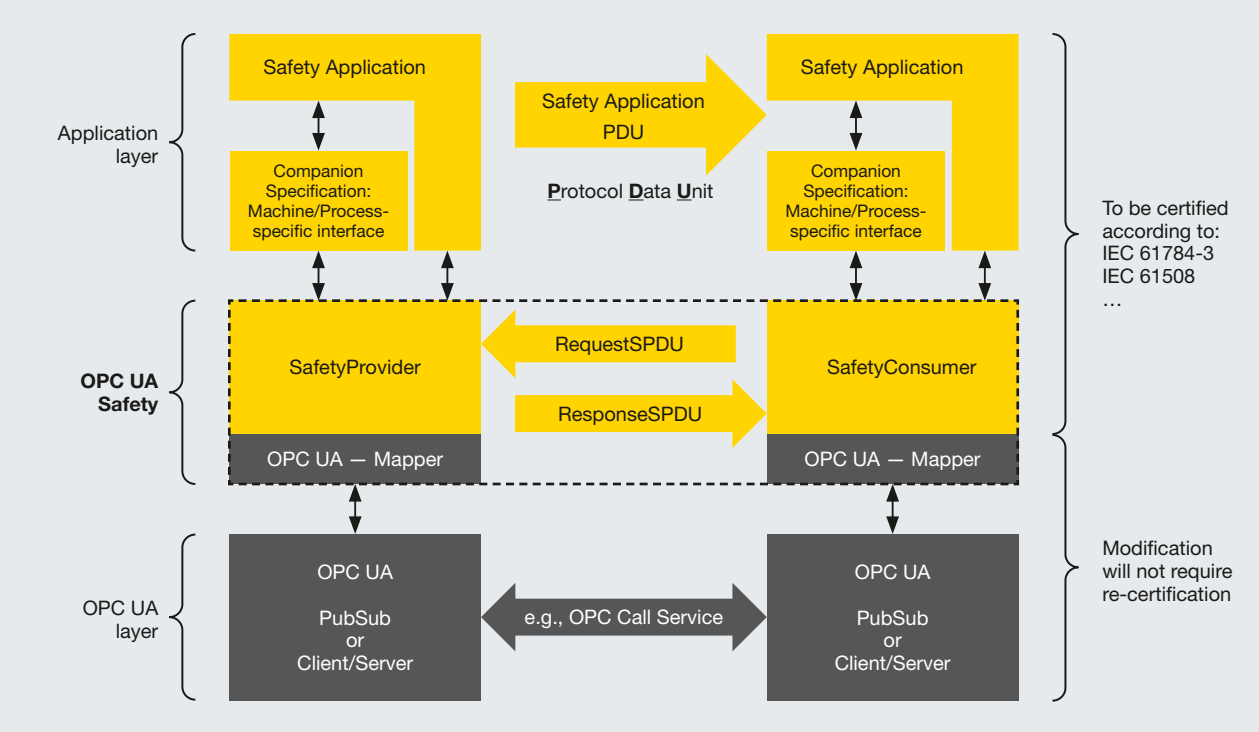


图3：OPC UA 安全架构概述

2.2 安全数据源

安全数据源通过SAPI从安全应用程序接收安全用户数据（安全数据）。此外，也可以以一致的方式发送非安全相关数据（非安全数据）（见图4）。这意味着安全数据源在同一时间采样的安全和非安全数据会一起发送给安全接收器。安全应用程序可以通过控制输入影响安全数据源的行为，进而间接影响安全数据接收器的行为。例如，可以使用激活故障安全值（ActivateFSV）的输入，使安全接收器向其安全应用程序提供安全替代值，而非实际的过程值。安全数据源在调试时通过安全参数接口（SPI）进行参数设置安全基ID和安全数据源ID共同为该数据源实例定义了一个全局唯一的ID。安全结构签名是对所发送的安全用户数据的结构和类型标识符的校验和。安全数据接收端也会检查这个签名。例如，如果编程错误导致安全数据接收端将一个三维向量（类型标识符例如“vec3D”）与一个以三个欧拉角形式提供方向的安全数据源（类型标识符例如“orientation”）连接起来，签名将不匹配，安全数据接收端将不会把这些数据传递给安全应用程序。

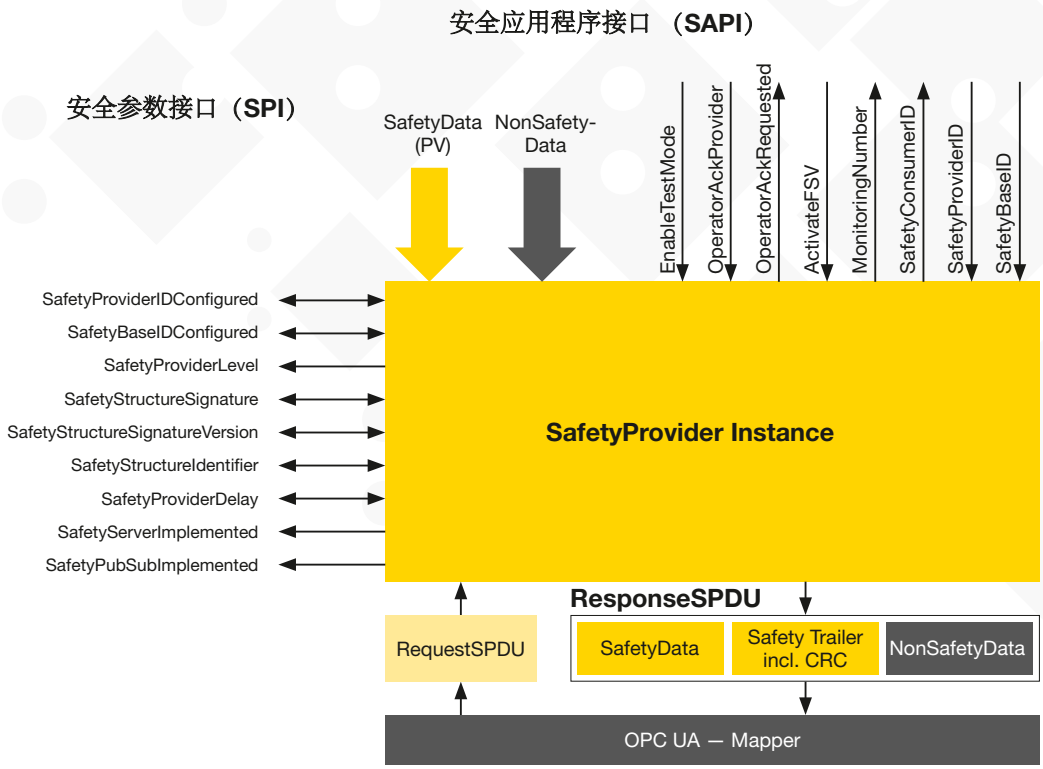


图 4: 安全数据源接口: 安全应用程序编程接口（SAPI）、安全协议接口（SPI）和安全协议数据单元（SPDU）

安全数据源的状态机简单，仅包含两个状态（见图6）。在“WaitForRequest”状态下，数据源等待请求SPDU。在 “PrepareSPDU” 状态下，借助RequestSPDU和当前 SAPI 处的数据生成ResponseSPDU，并将其传输到 OPC UA 映射器。这意味着安全数据源的实现实际上没有任何状态。无需在安全级别建立任何连接，也无需将安全数据接收端的身份告知数据源。

一个安全数据源可以依次为多个安全数据接收端服务。为避免可用性问题，在这种情况下的安全数据接收端必须实施一种防止同时访问同一安全数据源的程序。不过，可以以非安全的方式完成，因为并发访问导致的数据损坏会被安全检测到。

安全数据源的每个实例在 OPC UA 信息模型中由一个安全数据源类型对象表示（见图 5）。此外，每个实现 OPC UA 安全的 OPC UA 服务器都会获得一个固定、已知NodeID 的安全访问控制集（SafetyACSet）节点，该节点组织所有安全数据源对象，使得在调试和运行期间都能轻松访问所有安全数据源。

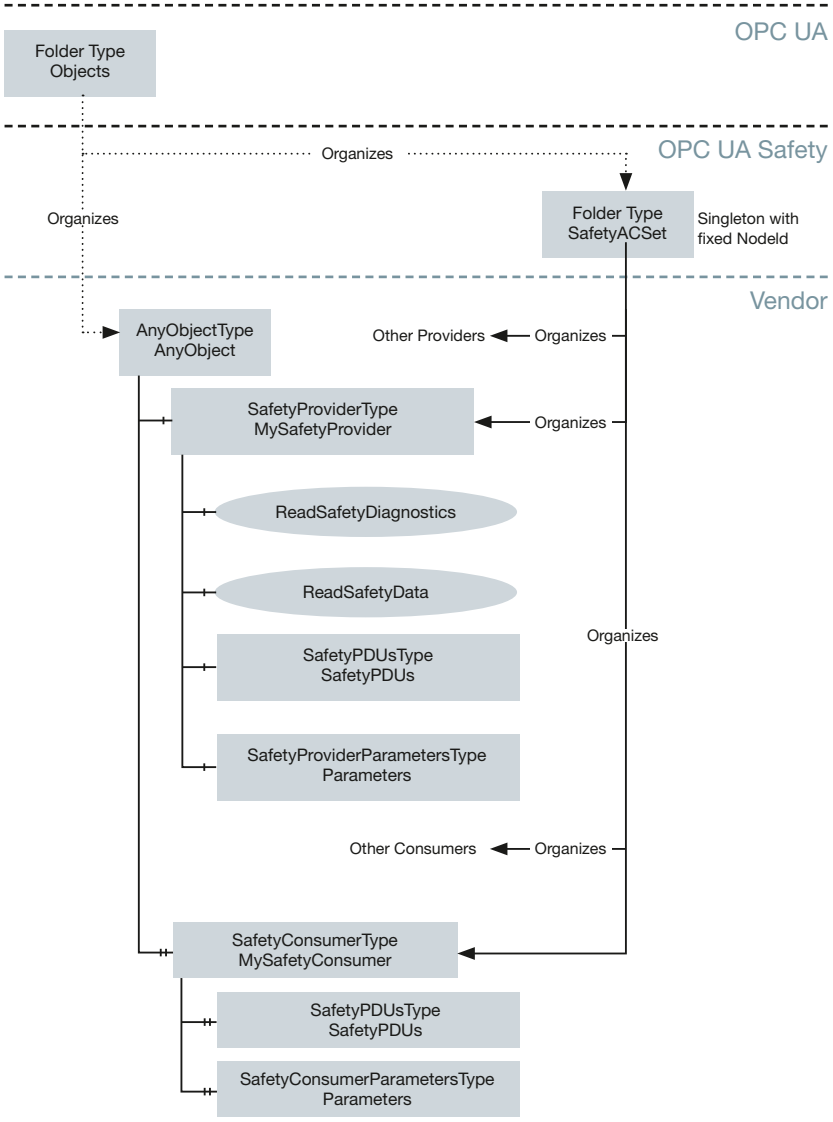


图5：OPC UA信息模型，由节点SafetyACSet（带fxed NodeID）和一个或多个SafetyProvider组成。

2.3 安全数据接收端

在安全数据接收端中，安全用户数据从响应安全协议数据单元（ResponseSPDU）中提取，完成有效性检查后通过SAPI与非安全用户数据一同传递给安全应用程序（见图 7）。此外，安全应用程序通过该接口（FSV_Activated）输出接收有关此数据的有效信息。安全数据接收端通过安全参数接口（SPI）进行参数设置。具体而言，现在已设置预期的安全基础ID和安全数据源ID，并且与安全数据源一样，保存一个能显示安全用户数据结构和ID签名。若发生错误，例如定义一个操作员确认机制，确定安全数据接收端在安全数据源做出响应并触发超时之前需要等待的时间。

安全消费者的状态机如图 8 所示。在无故障状态下运行时，安全数据接收器会循环经过状态 S13、S14、S15、S16 和 S18。在状态 S13 中，发送 RequestSPDU；在状态 S14 中 ResponseSPDU等待响应。在状态 S15 中，检查响应ResponseSPDU的循环冗余校验（CRC）签名；在状态 S16 中，检查数据的来源和时效性。如果这些检查中有任何一项失败，或者在状态 S14 中出现任何超时的情况，系统都会进入状态 S17，随后会生成一条错误消息用于诊断。

当 OPC UA 安全系统在非安全相关通信层检测到错误时，需要给出安全响应。不过，根据具体情况，OPC UA 安全系统能够容忍此类错误。其中有一种情况是偶发性错误，即后续的RequestSPDU重新发送时没有错误。此外，最近一次发生的错误不能早于安全错误间隔限制。参数（SafetyErrorIntervalLimit）决定了偶发错误之间可容忍的最小间隔，并根据所需的安全完整性等级（SIL）进行设置。当SIL2偶发错误发生的频率低于每 6 分钟一次时，不一定会导致系统过渡到安全状态。尽管如此，下一个正确的RequestSPDU必须在安全接收器超时到期之前发出。可容忍的错误会使请求-响应周期再次运行。需要注意的是，在此过程中新的用户数据不能提供给安全应用程序。

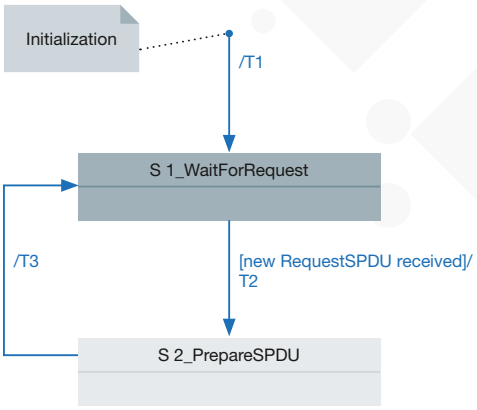


图6: 安全数据源状态图

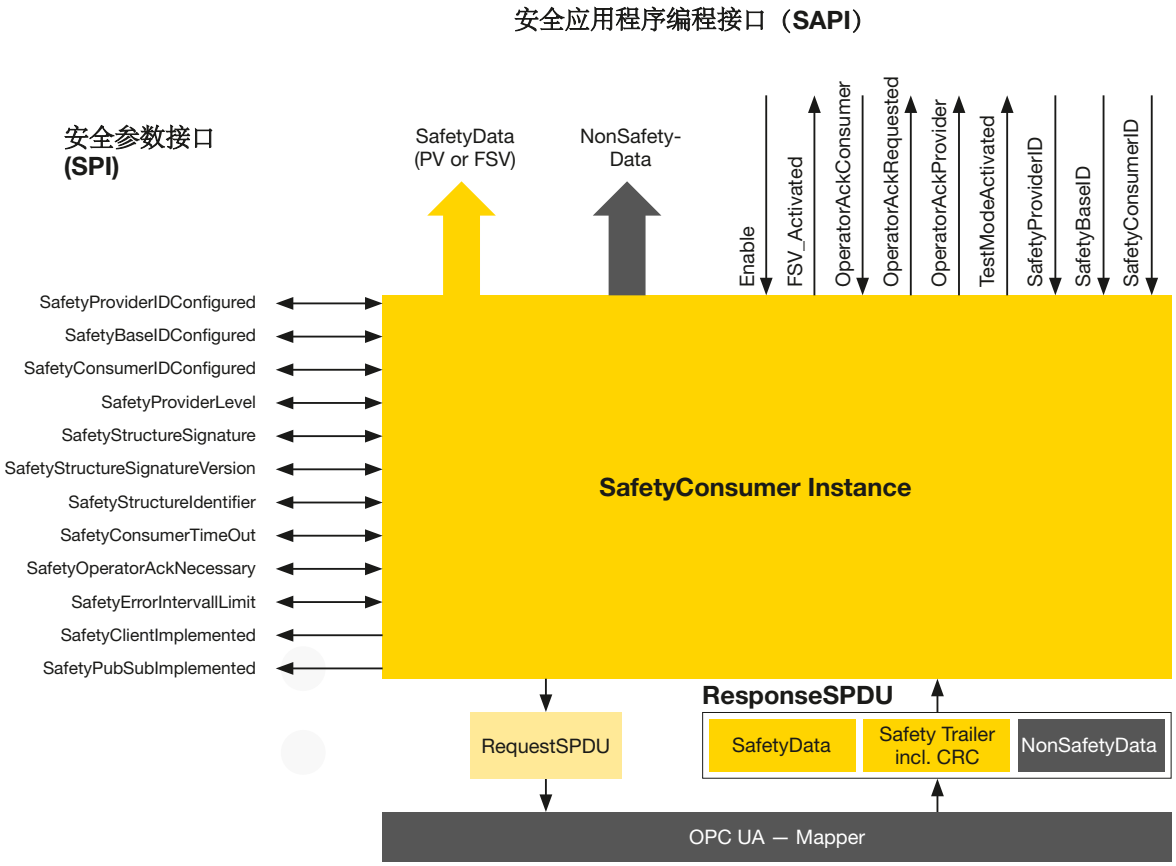


图 7: 安全数据接收端接口：安全应用程序编程接口（SAPI）、安全协议接口（SPI）和安全协议数据单元（SPDUs）

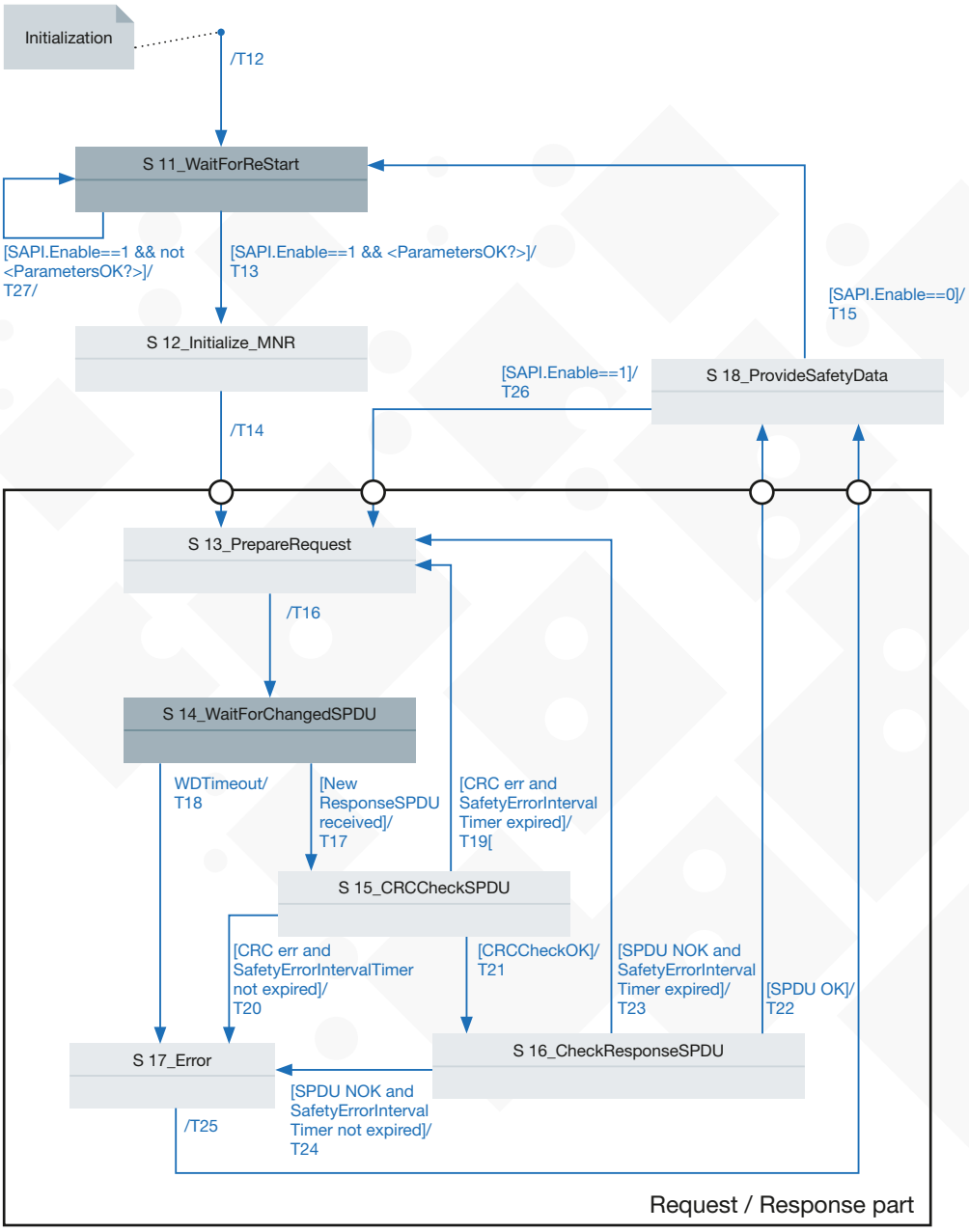


图8: 安全数据接收端状态图

如果错误无法容忍（因为是永久性错误，或者瞬态错误发生过于频繁），则必须给出安全响应。在这种情况下，安全数据接收端使用FSV_Activated变量告知安全应用程序不存在有效过程值。此时，用户数据会逐位设置为零。根据所发生错误的类型，需要操作员确认才能恢复使用真实过程值进行操作。有些应用程序始终要求操作员确认，这可以通过操作员必要参数（OperatorAckNecessary）来实现（见图 9）。一旦错误消除，就会通过操作员确认请求（OperatorAckRequested）输出指示来等待操作员确认。操作员确认OperatorAckConsumer的上升沿随后恢复正常操作，即输出过程值而非安全替代值。在最简单的情况下，OperatorAckConsumer连接到安全数据接收端的安全应用程序中，例如，连接到一个按钮或人机界面中的某个元素。不过，这并不排除更复杂的场景。例如，图 9 展示了一个双向 OPC UA 安全连接，在两个方向上各有一个安全数据源和一个安全数据接收端。在这个示例中，两边都可以进行操作员确认（OA）。为此，信号一方面连接到相应OperatorAckConsumer输入端，另一方面连接到OperatorAckProvider输入端。后者的结果设置相关安全数据接收端的操作员来确认Operator - AckProvider。将此输出连接到OperatorAckConsumer可对连接另一端的安全数据接收端进行确认。

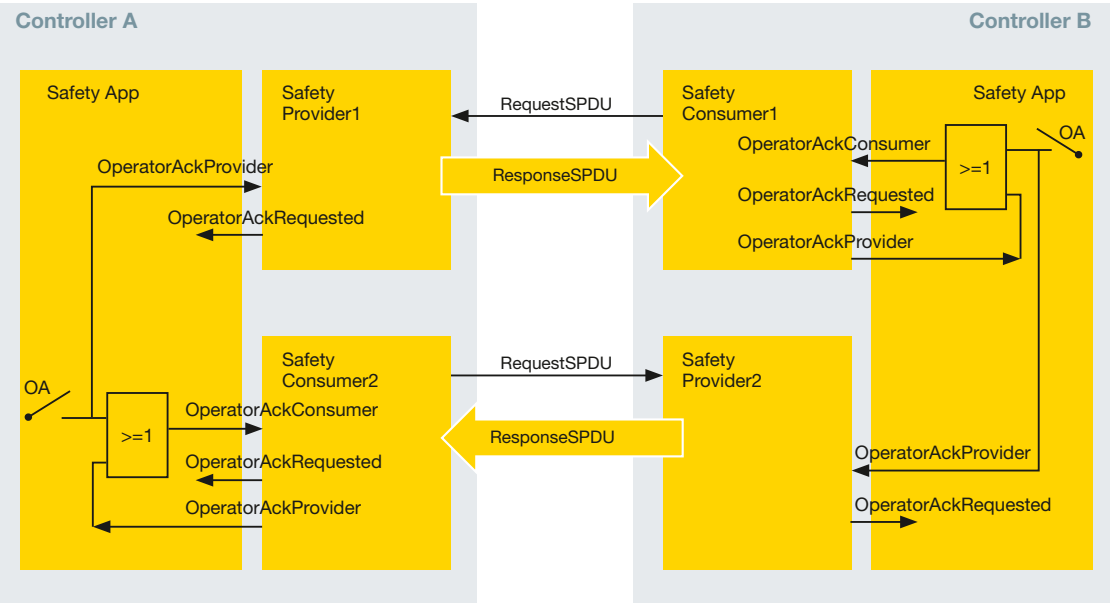


图9：双向通信，双方都可以进行操作员确认。

2.4 用于现场级通信的 OPC UA 安全协议

OPC基金会正在开发现场交换（OPC UA FX，简称 UAFX）规范，旨在扩展和增强 OPC UA 的功能，以满足现场级应用的需求。目前，这些规范已用于控制器-控制器通信，不久后也将适用于控制器-设备通信。 OPC UA安全协议通过标准UAFX连接进行传输，采用 IEC 61784-3 中所述的通道间原则，除了进行标准数据有效负载交换之外，还能在自动化组件之间传输安全数据有效负载。这一原则减少了对安全传输功能的评估，使得底层 UAFX 连接无需进行额外的功能安全评估。安全功能实体包含非安全和安全的输入输出变量。功能实体（FE）内的安全应用也必须按照安全工作流程进行开发。安全应用直接与安全提供者/安全消费者相连，它们通过安全协议交换数据（见图10）。OPC UA 映射器用于连接安全层和底层通信，支持安全提供者和安全消费者之间的通道。

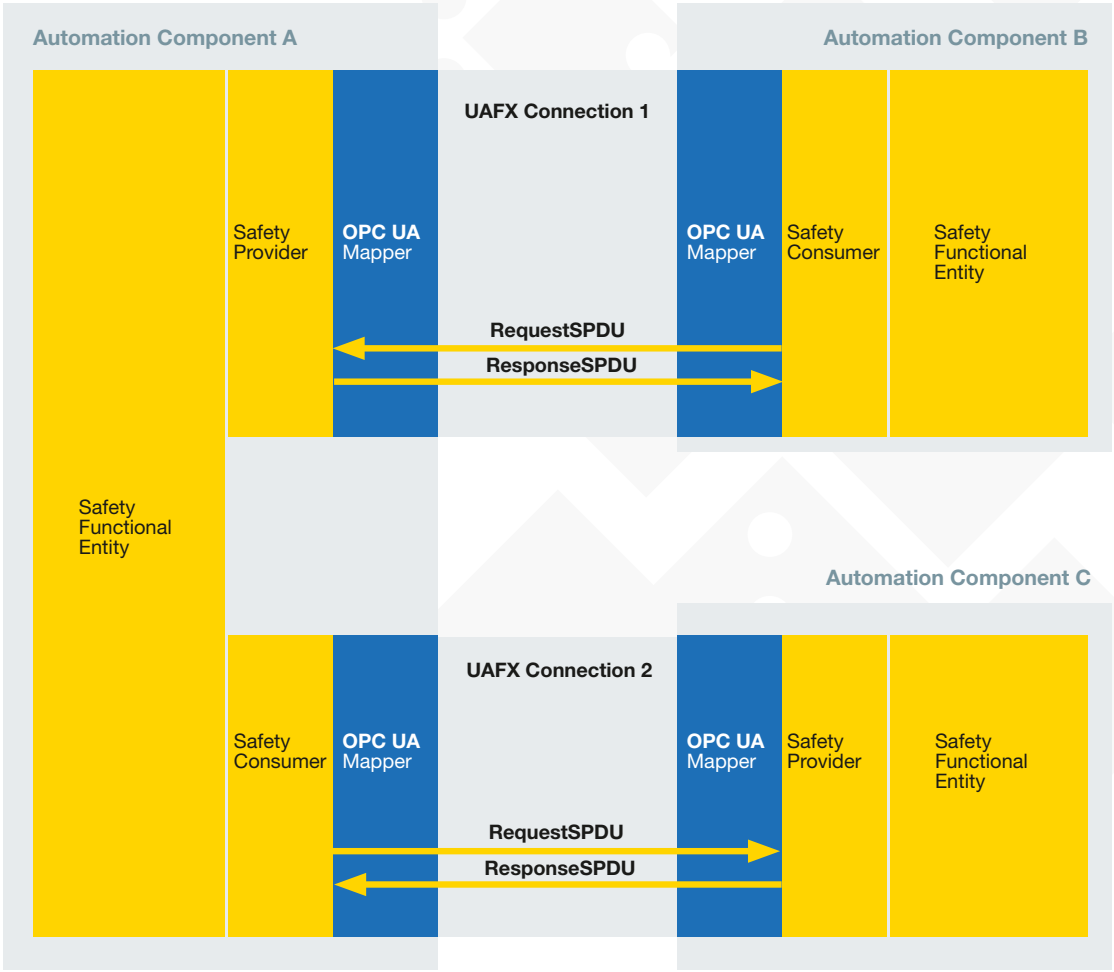


图10: 自动化组件之间的安全连接

最基本的安全通信类型是双向通信，即一个自动化组件（AC A）上的安全应用向另一个自动化组件（AC B）上的安全应用发送数据。安全数据接收端通过Request SPDU发起通信。安全数据源会复制接收到的标识符和计数器，添加所请求的安全数据，并通过校验和对所有数据进行加密，然后以Response SPDU进行回复（见图 11）
一个自动化组件AC可以同时充当安全数据接收端和发布端。安全数据源和接收端之间的连接可以在运行时建立和终止，这样不同的接收端可以在不同时间连接到同一个安全数据源。

数据发布端状态流程图
安全数据源需要实现的是一个非常简单的状态机。它只是等待请求到来，若接收到请求，就会发出安全消息。所有的安全检查都在安全接收端一侧进行。

数据接收端状态流程图
安全接收端发起安全的数据交换，然后等待响应，并检查是否存在潜在的通信错误（如完整性、及时性、真实性，需符合 IEC61784 - 3 标准）。一旦检查完成，就会将安全数据提供给自动化组件（AC）内的安全应用。如果发生通信错误，就会将故障安全替代值传递给安全应用，从而给出错误指示。

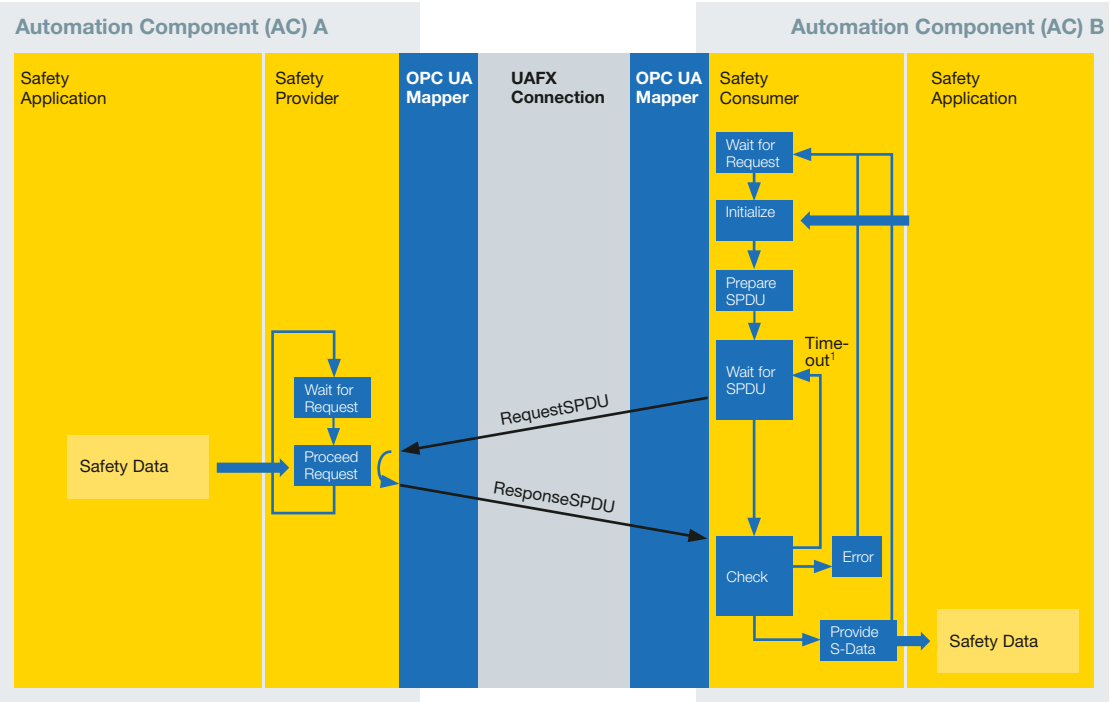


图11: 安全数据发布端与接收端状态机

[1] 为避免出现安全超时情况，SPDUs也可通过端到端延迟保证机制来加以保护。

3. 安全论证

3.1 定性推理

遵循国际标准 IEC 61784 - 3 [2]，OPC UA 安全协议必须能够处理在低网络层可能出现的所有通信错误。表 1 中列出了每种错误发生的情况下， OPC UA 安全协议规定的处理机制。尽管安全数据接收端仅对响应 ResponseSPDU 进行错误检查，但这些机制涵盖了包括请求（RequestSPDU）和响应中的错误。因为安全数据源会将RequestSPDU中包含的所有数据复制到ResponseSPDU，从而使接收端能够在后续检测到这些错误。

Communication Error	Safety Measures			
	MonitoringNumber	Timeout with receipt	Set of IDs for SafetyProvider	Data integrity check
Corruption	–	–	–	x
Unintended repetition	x	x	–	–
Incorrect sequence	x	–	–	–
Loss	x	x	–	–
Unacceptable delay	–	x	–	–
Insertion	x	–	–	–
Masquerade	x	–	x	x
Addressing	–	–	x	–

表1: 遵循IEC 61784-3标准的通信错误保护措施

3.2 定量评估

OPC UA中使用32 位循环冗余校验算法（CRC）具有4.0 x 10^{-10}的条件残差概率或更低。这意味着在 2.5 x 10^{9}个有故障的 RequestSPDUs 中，平均不到一个未被检测出故障。图 12 展示了从 1 到 1521 字节的所有 SPDU 长度以及所有相关比特误码率时的残余错误概率。每个值都是使用双码（例如Castagnoli方法 [6]）计算得出。

图 13 显示了需要对所有可能的用户数据长度进行迭代计算的必要性，该图展示了在较长时间段内针对选定用户数据计算出的条件残余错误概率。在这些情况下，残余错误概率比期望值（4 x 10^{-10} ）高出几个数量级。该图还表明，必须针对所有比特误码率计算残余错误概率。计算比特误码率的“最坏情况”（p=0.5）并不一定能得出最高的条件残余错误概率。

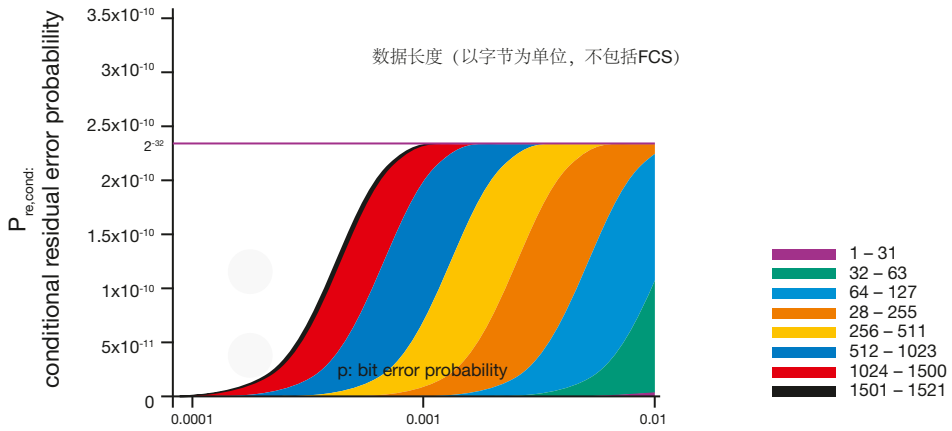


图12: OPC UA利用CRC算法，在 1–1,521 字节及各种比特误码率 p 条件下的残余错误概率

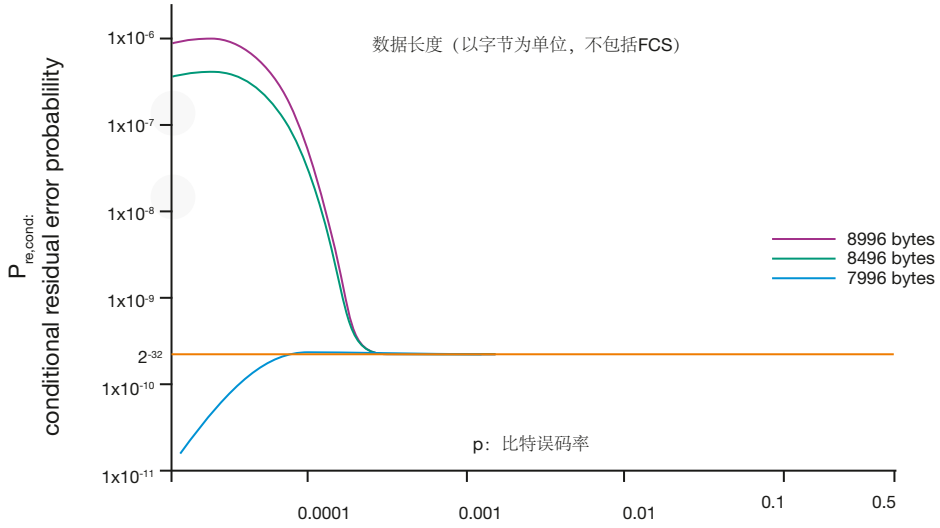


图13：反例：存在一些被选中消息长度的条件残余错误概率远高于 2^{-32}。

总结

OPC UA 安全协议首次规定了不同制造商的工业控制器和设备之间功能安全相关数据的标准化交换。基于非安全相关通信层的OPC UA 客户端/服务器和 OPC UA 发布/订阅模式的发展，我们定义了一个满足所有 IEC 61508 [1] 要求的安全通信协议。与安全现场总线协议不同，这里不存在“控制器”和“设备”的区别。所有通信用户拥有平等的权利，并且可以实现任意数量的安全数据发布端（安全数据源）和数据接收端（安全数据接收器）通信，这使得创建复杂的通信关系和网络拓扑结构成为可能。

OPC UA 安全协议具备根据应用需求来组织用户数据的能力，能够提供长度在 1 到 1500 字节的用户数据。依据 IEC 61784 - 3 标准，OPC UA 安全协议使用一组标识符（IDs）在运行时检查数据是否来自预期的数据源，或者是否由于寻址错误等原因从错误的数据源提供了数据。与已知的安全通信协议不同，OPC UA 安全协议允许安全应用在运行时选择这些标识符。从根本上说，这使得同一安全连接可被不同的通信用户使用。而反过来这又是模块化机器和自主移动机器人（AMRs）领域中复杂场景的先决条件，这些场景需要这种动态的连接设置。

参考文献

[1] IEC 61508. (2010).
电气/电子/可编程电子安全相关系统的功能安全.
国际电工委员会: www.iec.ch

[2] IEC 62280 (2014). 铁路应用—通信、信号和处理系统—传输系统中的安全通信.
国际电工委员会: www.iec.ch

[3] EC 61784-3. (2021). 工业通信网络—行规—第 3 部分：功能安全现场总线—基本规则和配置文件定义.
国际电工委员会: www.iec.ch

[4] IEC 61784-3-3. (2021). 工业通信网络—配置文件—第 3 部分：功能安全现场总线—CPF 3 的附加规范.
国际电工委员会: www.iec.ch

[5] IEC 62541. (2016). OPC 10000 统一架构.
国际电工委员会: www.iec.ch

[6] OPC 10000-15 OPC 统一架构(2021) —
Part 15: 安全性, www.opcfoundation.org

[7] Castagnoli, G., Brauer, S., & Herrmann, M. (1993).
24 位和 32 位奇偶校验位循环冗余校验码的优化.
《IEEE 通信汇刊》，41(6)，883 - 892

[8] Leach, P. (2005). 通用唯一标识符（UUID）统一资源名称（URN）命名空间，
征求意见文档: 4122,互联网协会，2005年.

[9] Walter M., Barthel H. (2020). OPC UA 第 15 部分实现功能安全通信：安全： atp!info,
Vulkan-Verlag GmbH, 2020. www.vulkan-shop.de

总部
OPC 基金会
美国亚利桑那州斯科茨代尔82街16101号
3B室，邮编 85260-1868 电话：480
483-6644 office@opcfoundation.org

OPC基金会 欧洲
opceurope@opcfoundation.org

OPC基金会 中国
opcchina@opcfoundation.org

OPC基金会 日本
opcjapan@opcfoundation.org

OPC基金会 韩国
opckorea@opcfoundation.org

OPC基金会 东盟
opcasean@opcfoundation.org

OPC基金会 印度
opcindia@opcfoundation.org