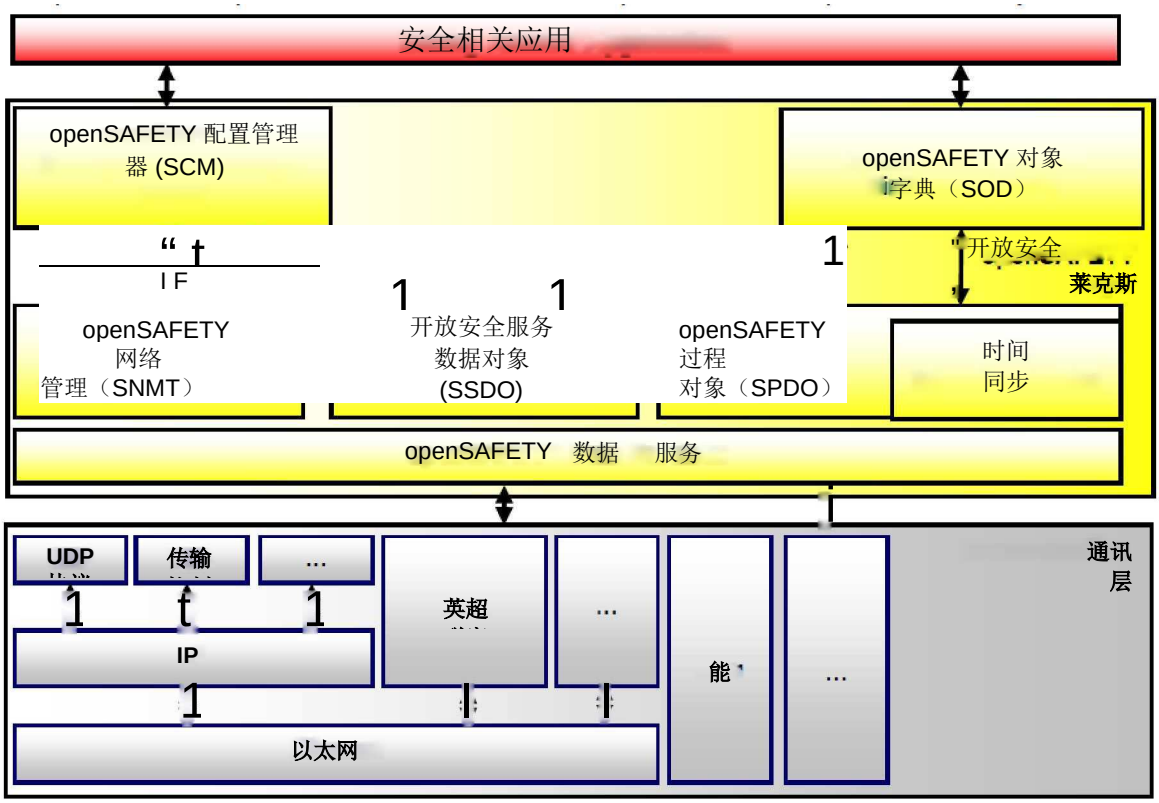
基于 UDP 的 openSAFETY

于 2024 年 1 月 24 日从 Confluence 导出

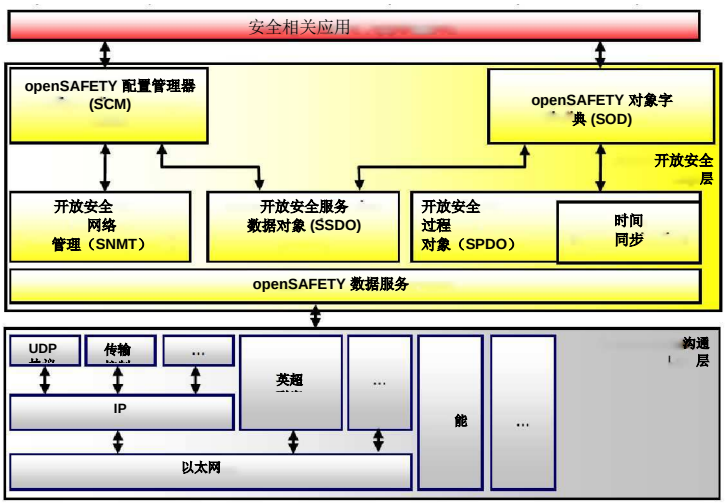
BnR 通用 pdf 模板版本 2

目录

openSAFETY over UDP 参考模型

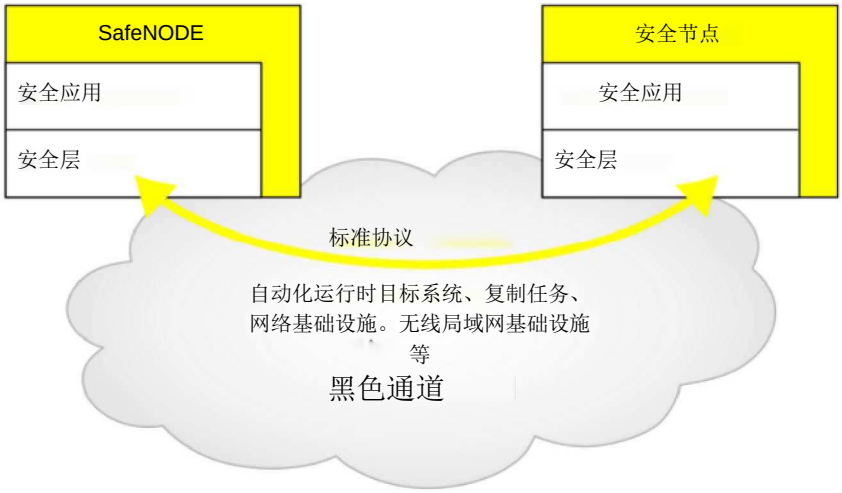


沟通模式



黑色通道原理 - 安全层

出于安全目的而不能使用的通道。

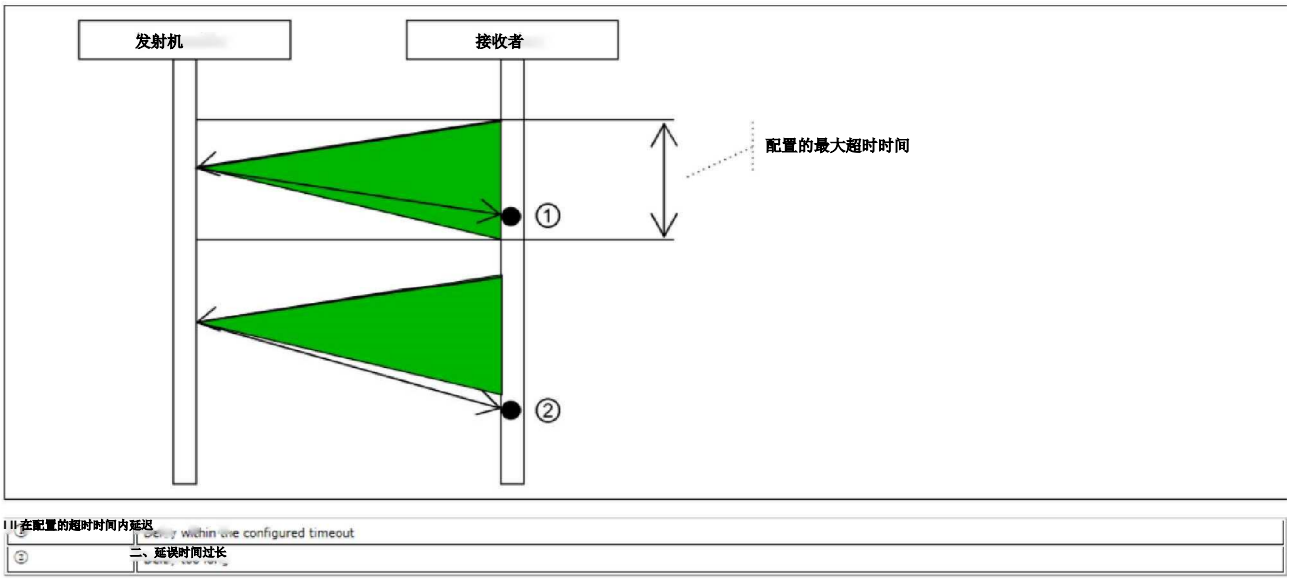


黑色通道原理使得通过通信传输安全相关数据成为可能

- 数据在独立的安全相关协议或“安全层”中受到保护，与传输无关。
- 安全层通信关系通常是点对点连接，其中连接的端点必须始终在可用于安全目的的节点（SafeNODE）中实现。
- 其间的所有组件都是黑色通道的一部分。因此，这些组件不具有安全相关特性。

监控 openSAFETY 中的安全响应时间

该图显示了监控响应时间的机制。



openSAFETY 使用时间戳独立监控接收到的数据包的寿命，并根据配置的期望对其进行检查。为此，接收器测量从发送请求帧到接收相关响应帧的时间。根据配置的超时限制检查测量的时间。

接收响应帧的最大允许时间是 openSAFETY 中时间 监控的决定性参数。如果在最大允许时间过去之前响应帧未到达接收器，则 openSAFETY 连接将更改为状态 FAILSAFE。因此，最大允许时间随后被称为超时。

一般来说，较大的超时会提高 openSAFETY 通信针对延迟和数据包丢失的稳定性，但会延长最大安全响应时间（有关其他信息，请参阅安全响应时间一章）。

通信路径的超时由以下 SafeDESIGNER 参数决定：（“额外容忍的数据包丢失”+ 1）*“安全数据持续时间”。

超时必须考虑数据包从发送器（例如 SafeIO 模块上的安全输入通道）到接收器（例如 SafeLOGIC 控制器）的所有传输时间。Automation Studio 功能“网络分析器”可用于为确定超时提供支持（有关“网络分析器”的其他信息，请参阅诊断和服务 → 诊断工具 → 网络分析器部分）。该工具可用于确定从接收器到发射器或从发射器到接收器的典型数据传输时间。

以下规则适用于建立 openSAFETY 通信：

“网络分析仪的价值”* 2 + SafeLOGIC 循环时间 * 2 ≤配置的超时 ≤通信的最大安全响应时间

最大允许安全响应时间取决于具体应用，并且必须根据相应的安全功能来确定。

从安全角度来看，超时有两个重要后果：

- 如果黑色通道出现延迟（例如丢包、无线通信），发射器的数据可能会出现明显的时间延迟而到达接收器。超时指定接受延迟的时间。因此，如上所述，超时是安全响应时间计算的直接部分。
- 黑色通道上的数据可能会丢失。超时指定可接受的数据丢失量。如果安全相关事件短于超时，则不再保证接收器上会检测到该事件（有关其他信息，请参阅最小信号长度一章）。