CLAROTY

Cyberworld

白皮书

# 网络化物理系统 (CPS) 网络风险管理

## 网络安全从业者入门指南

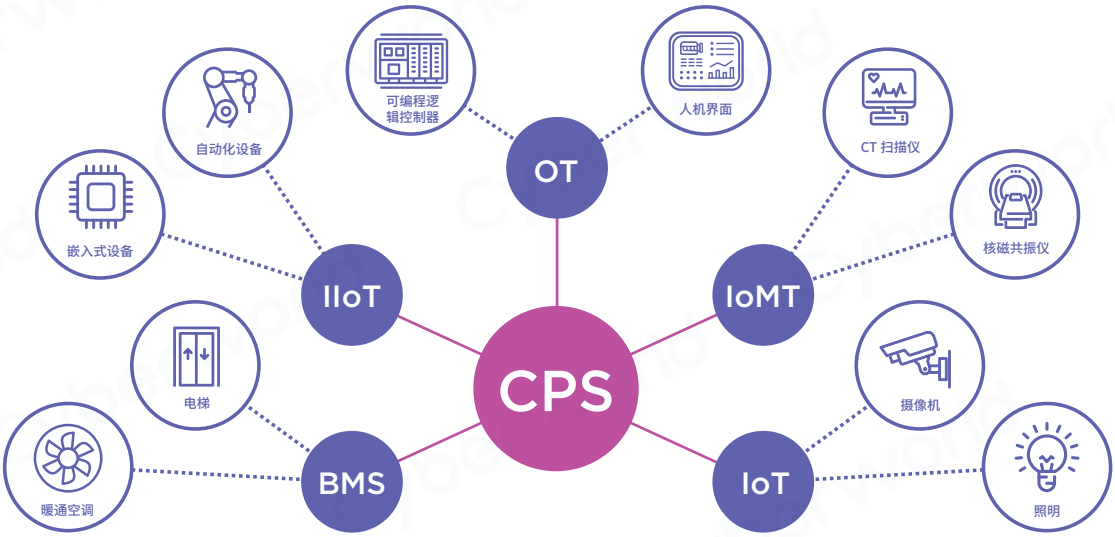
# 目 录

## 概述

所有网络安全专业和各部门人员都有一个共同的总体目标，就是要降低网络风险。但是，对于工业、医疗保健、其他以网络化物理系统 (CPS) 为运营基础的关键基础设施领域的企业来说，这一目标正在逐步消失。

原因之一是：简单地评估网络风险和确定其优先级，是首席信息安全官（CISO）及其团队长期以来管理 IT 环境中网络风险的方法。如果要进一步降低CPS环境的网络风险，就要抛弃许多传统的方法和解决方案。根据预估，关键基础设施领域 95% 的 CISO 不仅要负责 IT 安全，还要负责 CPS 安全。越来越多的人开始面对这一严重后果的严酷现实。

本指南的其余部分是借鉴 Claroty 与 CISO 、其他网络安全从业人员合作支持其 CPS 安全之旅的第一手经验。重点放在该旅程核心目标的基础上：CPS 网络风险管理。




## 网络化物理系统（CPS）的定义

那么，CPS 到底是什么？

根据 Gartner® 的说法，CPS 是协调传感、计算、控制、联网和分析的工程系统，以便与物理世界（包括人类）进行交互。当安全时，它们可以实现安全、实时、可靠、有弹性和适应性强的性能。

CPS 的主要类型包括：

- **运营技术 (OT)** 资产，例如制造、发电、运输和其他关键物理过程中不可或缺的可编程逻辑控制器 (PLC)、执行器和远程终端单元 (RTU)。
- **物联网 (IoT)** 设备，例如各种设施和环境中的安全摄像机、运动传感器，甚至是自动售货机。
- **医疗物联网 (IoMT)** 和其他互联临床设备，例如支持医疗服务的生命体征监测系统、核磁共振仪和输液泵。
- **楼宇管理系统 (BMS)**，例如支持智能楼宇安全、效率和适宜性的联网电梯、火灾报警器和暖通空调系统。

## 快速回顾风险

在深入研究 CPS 网络风险管理影响之前，需要快速了解风险本身的基本含义、变量和其他重要因素。

从本质上讲，风险是对不良事件的可能性和潜在影响的衡量。这个简单的定义不是特定于CPS、网络安全或其他事物。无论情况如何，它都保持不变，并且可以通过以下等式轻松证明：

$$\text{风险} = \underbrace{\text{可能性}}_{(\text{威胁} \times \text{漏洞})} \times \text{影响}$$

**可能性**

该变量是指发生不良事件的概率。它是威胁和漏洞子变量的产物。

**威胁**

该子变量是不良事件的根源或触发因素。

**漏洞**

该子变量包含威胁可能利用的缺陷或情况，而导致不良事件发生。

**影响**

该变量反映了不良事件的后果。

## 风险控制和风险因素的作用

上述等式并非用数学上的字面意义来解释，但它突出了一个数学上准确的事实：如果仅消除该等式的其中一个变量，即分配一个零值，那么，所讨论的风险也将被消除。

尽管许多不同类型的风险不可能真正地被消除，但风险管理的基本原则揭示了如何减少风险：应用风险控制。

**风险控制**是旨在通过降低至少一个风险变量的程度来降低风险的措施。它们目的在于抵消**风险因素**，但这会产生相反的效果，就是增加了至少一个风险变量的程度。

让我们通过将这些概念应用于一种非常熟悉的风险类型来进行压力测试——网络暴露风险，就好比皮肤被阳光晒伤。

| “晒伤”的风险 = | 可能性 | | 影响 |
|---|---|---|---|
| | 威胁 | 漏洞 | |
| | “阳光” | “由阳光导致的晒伤情况” | “晒伤的后果” |
| **风险因素示例：** | • “存在太阳” | • “暴露在阳光下”<br>• “拥有白皙的皮肤” | • “疼痛耐受力低”<br>• “容易出现某些皮肤状况” |
| **风险控制示例：** | • “以某种方式摧毁太阳” | • “白天紫外线强的时段留在室内”<br>• “穿防晒衣并涂抹防晒霜” | • “使用冰敷、芦荟或其他有助于缓解晒伤的局部治疗”<br>• “看皮肤科医生” |

## 权衡成本和收益

“晒伤”的例子说明了为什么**成本效益分析（CBA）**对于风险管理至关重要。通常，将每种可能的风险控制应用于每种可能的风险因素既不可行也不可取，因为这样做的成本可能超过了收益。的确，摧毁太阳会消除晒伤的风险，但也会消除地球上的生命。因此，效果稍差和低成本的替代控制措施，例如涂抹防晒霜，是理想的选择。

“晒伤”的例子也突显出一些风险因素实际上无法被合理地消除或改变，因此必须被接受。这种决策一般被称为**风险接受**，在影响风险等式的威胁子变量的因素中，这种决策尤其常见。就像太阳一样，除了最极端情况外，许多威胁都会继续存在。这就是为什么从 CBA 的角度来看，优先考虑旨在减少漏洞或风险影响变量的控制措施是最有效和推荐的方法。

## 关于网络风险的说明

正如本指南的标题所暗示的那样，从现在开始，重点不再是一般风险、物理风险或其他类型的风险，而是网络风险。这种区别微妙而简单，网络风险反映了不良网络事件（例如，网络攻击或其他网络安全事件）的可能性和潜在影响。接下来研究这对 CPS 意味着什么。

## CPS 网络风险形势

了解 CPS 网络风险形势对于管理 CPS 网络风险至关重要。这就是本指南这一部分要介绍的内容。

### 如何发展至今

当前 CPS 网络风险形势的根源在于：从历史上看，工业环境的网络安全优先事项仅限于物理隔离 OT 资产。虽然医疗行业长期以来优先考虑保护数据，但传统的医疗设备并非如此，它们不支持网络。没有连网就意味着不需要网络风险控制。如今，工业和医疗行业 CPS 环境、IT 环境和互联网交织在一起，已是司空见惯。这一规范是数字化转型的产物，尤其是 IoT、IoMT、BMS 和其他 CPS 的爆炸式增长，各企业越来越多地与传统 OT 资产、传统医疗设备一起实施并取代它们。这种转变的好处是不可否认的，但它也使 CPS 环境面临网络威胁。不幸的是，此类威胁利用的连接性增长速度快于保护其安全的付出，这表明从业者必须应对的 CPS 网络风险正在恶化。仔细看看这些状况背后的数字。

### 主要事实和数据

**1. 关键基础设施领域的数字化转型正在加速**，创造了比以往更多的网络化物理连接。

**830亿**

到**2024**年，**物联网连接数**将达 **830 亿个**，其中 70% 将位于关键基础设施领域 [1]。

**70%**

到**2026**年，购买的新工业CPS中 **70%** 将包含智能设计功能 [2]。

**40%**

到 **2028** 年，**40%** 的医疗保健机构将制定正式的数字孪生计划 [3]。

**2. 这种连通性放大了 CPS 固有的易受攻击性质**，并强调了传统 CPS 漏洞管理方法的不足之处。

**80%**

**近 80%** 的医疗保健机构将医疗设备漏洞视为其网络安全防御中最重大的漏洞 [4]。

**70%**

去年，**70%** 的新 CPS 常见漏洞和披露 (CVE) 获得了“高”或“严重” CVSS 评分，但只有不到 8% 被利用 [5]。

**4%**

**平均而言**，以CVSS为主导的传统漏洞优先级排序方法的“效率”低于**4%**，这意味着 96% 的修复资源被浪费 [6]。

注 1：Junifer Research 于 2020 年 3 月 31 日发布的《2020-2024 年物联网：消费者、工业和公共服务》

注 2：Gartner 分析师 Rich McAvey 和 Lloyd Jones 于 2023 年 5 月 24 日发布的《赋能工业资产智能化，加强数字化能力》

注 3：Gartner 分析师 Gregg Pessin 于 2023 年 1 月 13 日发布的《创新洞察：医疗保健提供商数字孪生改变决策制定》

注 4：Claroty 于 2023 年 8 月 29 日发布的《2023 年全球医疗保健网络安全研究》

注 5：Claroty Team82 研究团队于 2023 年 2 月 14 日发布的《2022 下半年 XIoT 安全状况》

注 6：Jay Jacobs 等五人于 2023 年 6 月 15 日发布的《增强漏洞优先级：通过社区驱动的见解进行数据驱动的漏洞利用预测》

**3. 网络威胁行为者日益利用这些条件，**影响 CPS 的勒索软件和其他类型的网络攻击持续增加。

**80%**

2021 年，关键基础设施领域 **80% 以上**的企业遭受了勒索软件攻击 [7]。

**50%**

自 2022 年 2 月以来，**将近 50%** 的医疗保健机构经历过 CPS 网络安全事件 [8]。

## 对比 IT 与 CPS 的网络风险

正如上述数据所表明的那样，近年来，CPS 网络风险管理的主要责任转移到以 IT 为中心的网络安全从业者身上，其中一个关键因素就是采用数字化转型举措来创建或扩展 IT 和 CPS 环境之间的连接。这些条件会让 CPS 与 IT 的许多不同之处经常被忽视，还使保护 CPS 的工作进一步复杂化。

下表详细介绍了其中一些主要差异及其对网络风险的影响：

| 差异 | IT 环境 | CPS 环境 | 网络风险影响 |
|---|---|---|---|
| **主要功能** | 启用、控制数据和信息的流动。 | 启用、控制关键物理过程。 | 网络风险管理会对CPS、其所支持的关键流程或操作人员的安全产生实质影响。 |
| **典型构成** | 使用标准系统和协议的标准计算机、服务器和其他IT资产。 | 使用老旧系统和专有协议的非标准、复杂、本质上脆弱的资产。 | 大多数CPS与标准网络安全工具不兼容，这使得它们极难被发现，那更不用说保护了。 |
| **网络安全优先事项** | 数据和信息的机密性、完整性和可用性。 | 关键物理过程的可用性、完整性和安全性。 | CPS优先事项经常与标准网络安全优先事项发生冲突，从而使保护它们的工作进一步复杂化。 |
| **停机容忍度** | 普遍较高。 | 非常低或不存在。 | 需要停机（例如打补丁）的网络风险控制通常无法在 CPS 环境中实施。 |

注 7：Claroty 于 2022 年 2 月 19 日发布的《2021 年全球工业网络安全状况》

注 8：Claroty 于 2023 年 8 月 29 日发布的《2023 年全球医疗保健网络安全研究》

## CPS 网络风险管理的入门技巧

理想的 CPS 网络风险管理计划是能够有效且高效地评估、确定优先级并减少 CPS 面临的网络风险。这样的计划并不是一朝一夕能完成的，而是漫长的旅程。本指南这一部分会介绍首要建议、需避免的陷阱以及优化此过程的战略考虑因素。

### 1. 从资产发现开始

如果不了解构成 CPS 环境的所有资产，则几乎不可能管理 CPS 网络风险。发现这些资产应该是 CPS 网络风险管理过程中的第 0 阶段，因为它是所有后续 CPS 网络风险控制的基础。

以下是 Claroty 建议的资产发现策略的高级概述：

#### i. 确定可视化目标

就您当前的 CPS 可视化、网络安全目标与利益相关者保持一致。利用这些见解，确定 CPS 可视化的目标。第一个目标应该是获得完整的 CPS 库存，作为 CPS 网络风险管理计划的基础。

#### ii. 选择发现方法

接下来，确定哪些资产发现方法可实现您的 CPS 可视化目标，然后选择支持这些方法的信誉良好的供应商。您可能需要混合使用以下几种方法来发现环境中的所有 CPS：

| 发现方法和说明 | 注意事项 |
|---|---|
| **被动监察**，利用环境中的交换机和端口在 CPS 之间复制流量。将副本发送到服务器进行分析，以识别 CPS 是否存在。 | **优点：**安全、稳健、持续<br>**缺点：**实施时间长，无法发现所有 CPS |
| **主动查询**，使用有针对性的查询来发现环境中的 CPS 。查询必须采用资产的本机协议，并模仿平常的流量，以确保其安全。 | **优点：**快速、简单、有效<br>**缺点：**仅提供时间点（非连续）可视化，其安全性需要在行的供应商 |
| **项目文件分析**，可解析 CPS 环境组件上的项目文件，以揭示项目的资产和周围的 CPS 。不需要直接连接，该方法适用于物理隔离环境。 | **优点：**快速、有效、安全、不需直接连接<br>**缺点：**仅提供时间点（非连续）可视化 |
| **基于主机的发现**，在 CPS 环境中的“主机”资产上安装一个文件。执行该文件，从主机和附近的 CPS 收集详细信息，然后解散该文件。 | **优点：**快速、安全、有效<br>**缺点：**仅提供时间点（非连续）可视化 |
| **基于集成的发现**，从环境的现有基础设施（例如交换机、防火墙、EDR 解决方案、CMDB 等）中提取重要的 CPS 详细信息。 | **优点：**快速、安全、非入侵性<br>**缺点：**成功取决于环境和供应商的技术 |

## 常见陷阱

**在评估供应商时，未考虑 CPS 协议覆盖范围。**

大多数 CPS 使用与标准工具不兼容的专有协议，但 CPS 安全供应商通常也不支持这些协议，并非所有此类供应商都支持所有 CPS 协议。因此，在评估 CPS 安全供应商时，验证协议覆盖范围和发现方法至关重要。

### iii. 实施发现方法

与选定的 CPS 安全供应商合作，执行您的发现方法，直到您可以验证所有 CPS 是否已填充到您的集中式 CPS 库存中。

### iv. 丰富 CPS 档案

验证您的CPS库存是否提供了全面且丰富的配置文件，其中包含环境中每项资产的详细信息的列表。如果缺少关键的资产级别详细信息，请覆盖其他发现方法来填补空白。下面是重要详细信息的列表。

## 常见陷阱

**忽视充分丰富资产状况的重要性。**

您的CPS库存不仅要包含环境中资产的基本标识符，还应该提供包含每项资产完整详细信息的配置文件。诸如此类的细节有几十个，它们是网络风险控制的前提。因此，可视化的深度非常重要。在CPS可视化目标中优先考虑的重要细节包括：

| | | | | | |
|---|---|---|---|---|---|
| 供应商 | 类型 | 类别 | IP 地址 | MAC | 型号 |
| 操作系统 | 操作系统版本 | 固件 | 序列号 | 协议 | 开放端口 |
| 关键性 | 修补程序级别 | 站点 | USB | APP | 软件 |
| 接口 | 机架槽 | 首次查看 | 上次查看 | 所有者 | 历史记录 |
| EOL | 创建设置 | 策略 | 安装日期 | 还有更多..... | |

### v. 利用 CPS 可视化

现在，您应该准备好利用新发现的 CPS 可视化，继续进行 CPS 网络风险管理的下一阶段。

## 2. 确保可以准确地对 CPS 网络风险态势进行评分

现在,几乎所有关键基础设施部门的CISO都要确保其企业的CPS网络风险态势能准确地反映在与执行领导层分享的更广泛的风险评分中。除了完整的 CPS 可视化外,这还需要一种**风险评分机制**:

- 反映 CPS 环境中一系列风险因素和控制

每个CPS环境都有各种因素和控制措施影响其网络风险态势。因此,您的CPS网络风险评分机制需要考虑和量化这些因素和控制措施,以确保其提供的评分准确。关键示例包括分段和端点保护等现有安全措施,以及CVE、不安全协议、老旧系统等风险因素。

- 灵活、可定制且透明

您的CPS环境是独一无二的。您的风险评分机制必须是能够自定义的,可根据您企业重要或无关的因素来自定义不同变量的加权方式。这些要素的透明度也是确保您能够理解、传达值得信赖且有用的风险评分的关键。

### 常见陷阱

**使用通用机制为 CPS 网络风险态势评分。**

虽然许多标准解决方案能够生成所谓的CPS网络风险评分,但它们通常缺乏生成准确且值得信赖的评分所需的范围、透明度和灵活性。

- 对网络风险进行多个级别的评分

不同级别的风险评分支持不同的用例。这些级别应包括:

| 资产风险评分 | 站点风险评分 | 环境风险评分 |
| --- | --- | --- |
| CPS环境中的每项资产都需要网络风险评分,能反映网络威胁损害该资产的可能性和潜在影响。 | CPS环境某个站点中所有资产的平均网络风险评分能反映该站点的CPS网络风险态势。 | 构成CPS环境所有站点中所有资产的平均网络风险评分能反映企业的CPS网络风险态势。 |

## 3. 使用风险评分来确定控制措施的优先级并评估其影响

CPS网络风险评分机制的准确性也很重要。它生成的评分是用作部署网络风险控制、确定优先级、评估对CPS环境影响的基础。

这些评分可帮助您回答以下问题：

> 我的 CPS 环境中的数十项资产受到相同的 CVE 影响。我应该先修复哪项?”

> “在包含CPS 环境的 50 个站点之间，我应该如何分配网络风险控制预算?”

> “我的网络分段计划在多大程度上影响了企业的 CPS 网络风险态势?

## 4. 考虑控制措施的操作限制

正如前面指出的，构成 CPS 环境的 OT、IoMT 和其他资产不仅支持从发电到医疗保健服务等关键物理过程，而且在很大程度上与标准网络安全方法不兼容。IT 环境中常用的许多控制措施并非在所有情况下都适用于所有 CPS 。这些限制在不同的资产和环境中都存在很大差异，常见的限制包括：

### 漏洞扫描

广泛用于扫描IT资产以查找CVE的解决方案会产生过多的流量，无法在CPS环境中安全使用。相反，使用特定于CPS的解决方案，被动地将资产详细信息与CVE数据库关联起来，以查明易受攻击的 CPS 。

### 补丁

通常修补任何漏洞都需要停机，而大多数CPS由于其所支持的流程而无法容忍停机。相反，请考虑替代网络风险控制，例如网络分段，以在不停机的情况下补偿当前的风险。

### 端点安全

防病毒、EDR和其他类型的标准端点安全解决方案使用代理，这些代理往往与许多不同类型的 CPS 不兼容。就像打补丁一样，应该考虑网络分段和其他替代控制。

## 5. 密切关注监管格局

所有CPS网络风险管理计划的另一个重要组成部分是网络安全监管格局。近年来，随着影响CPS环境的网络事件频繁发生，网络安全监管格局也发生了很大变化，现在针对CPS的法规越来越多。时刻关注与您的企业相关的法规、合规性要求以及审核的工作方式非常重要。以下法规、标准和框架对当今的关键基础设施企业作用最大：


IEC 62443　NERC-CIP　NIS2　NIST CSF　TSA 安全指令　OTCC:1-2022　SOCI 法案

## 总结

随着所有类型的CPS不断在关键基础设施领域激增，管理CPS网络风险对于网络安全从业者而言，会变得更加重要，而且更具有挑战性。本指南中分享的见解和技巧，旨在帮助您掌握这一责任的基础知识。但请记住，最重要的是，CPS网络风险管理是漫长的旅程。

Claroty在过去几年时间内帮助了数千名网络安全专业人员，让他们更有效、更高效地管理其 CPS 网络风险态势，并提供全面的 CPS 安全解决方案组合。

## 关于 Claroty

Claroty使工业、医疗保健、商业机构、大型企业和公建部门能够保护其环境中的所有网络化物理系统——扩展物联网(XIoT)。Claroty平台可以与客户现有的基础设施集成，提供可视化、漏洞和风险管理、威胁检测、安全远程访问的全方位控制。Claroty得到了全球领先的工业自动化供应商的支持和采用，拥有广泛的合作生态系统以及屡获殊荣的Team82研究团队。