国 际 电 信 联 盟

ITU-T X.1333

(01/2022)

国际电信联盟
电信标准化部门

X系列：数据网、开放系统通信和安全性

安全应用和服务(2)– 智能电网安全

在联网控制系统中使用远程访问工具的安全导则

ITU-T X.1333建议书

ITU-T X系列建议书

数据网、开放系统通信和安全性

公用数据网	X.1 – X.199
开放系统互连	X.200 – X.299
网间互通	X.300 – X.399
消息处理系统	X.400 – X.499
号码簿	X.500 – X.599
OSI组网和系统概貌	X.600 – X.699
OSI管理	X.700 – X.799
安全	X.800 – X.849
OSI应用	X.850 – X.899
开放分布式处理	X.900 – X.999
信息和网络安全	
一般安全问题	X.1000 – X.1029
网络安全	X.1030 – X.1049
安全管理	X.1050 – X.1069
生物测定	X.1080 – X.1099
安全应用和服务（1）	
组播安全	X.1100 – X.1109
家庭网络安全	X.1110 – X.1119
移动安全	X.1120 – X.1139
网页安全（1）	X.1140 – X.1149
应用安全（1）	X.1150 – X.1159
对等网络安全	X.1160 – X.1169
网络身份安全	X.1170 – X.1179
IPTV安全	X.1180 – X.1199
网络空间安全	
网络安全	X.1200 – X.1229
反垃圾信息	X.1230 – X.1249
身份管理	X.1250 – X.1279
安全应用和服务（2）	
应急通信	X.1300 – X.1309
泛在传感器网络安全	X.1310 – X.1319
智能电网安全	**X.1330 – X.1339**
验证邮件	X.1340 – X.1349
物联网（IoT）安全	X.1350 – X.1369
智能交通系统（ITS）安全	X.1370 – X.1399
分布式账簿技术（DLT）安全	X.1400 – X.1429
应用安全（2）	X.1450–X.1459
万维网安全（2）	X.1470–X.1489
网络安全信息交换	
网络安全概述	X.1500 – X.1519
漏洞/状态信息交换	X.1520 – X.1539
事件/事故/启发式信息交换	X.1540 – X.1549
政策的交换	X.1550 – X.1559
启发式和信息请求	X.1560 – X.1569
标识和发现	X.1570 – X.1579
确保交换	X.1580 – X.1589
网络防御	X.1590–X.1599
云计算安全	
云计算安全概述	X.1600 – X.1601
云计算安全设计	X.1602 – X.1639
云计算安全最佳做法和指导原则	X.1640 – X.1659
云计算安全实施方案	X.1660 – X.1679
其他云计算安全	X.1680 – X.1699
量子通信	
术语	X.1700 – X.1701
量子随机数发生器	X.1702 – X.1709
QKDN安全框架	X.1710 – X.1711
QKDN安全设计	X.1712 – X.1719
QKDN安全技术	X.1720 – X.1729
数据安全	
大数据安全	X.1750 – X.1759
数据保护	X.1770–X.1789
IMT-2020安全	X.1800–X.1819

欲了解更详细信息，请查阅ITU-T建议书目录。

ITU-T X.1333建议书

在联网控制系统中使用远程访问工具的安全导则

摘要

远程访问工具（RAT）广泛用在控制系统上，用于监测、控制和维护，以降低维护成本并最大限度地缩短发生故障时的响应时间。RAT提供远程操纵控制系统的能力，但与此同时，RAT的不安全配置和RAT中的漏洞可能会显著增加控制系统的攻击面。最严重的问题是从外部网络访问控制系统的接口，这可能允许攻击者从互联网访问控制系统。

ITU-T X.1333建议书描述安全使用RAT进行监测、控制和维护的总体情况。在本建议书中，确定了因使用RAT而使网络配置面临的威胁，并提供了安全导则，以适应在联网控制系统中使用RAT的安全配置和安全措施。

对RAT的使用提供组织良好的安全控制将有助于数字服务提供商操作控制系统，以减少攻击面和来自外部网络的威胁。此外，使发达国家与发展中国家之间的安全水平保持一致将是有益的，因为这不是一个局部问题，而是一个全球性问题。

历史沿革

版本	建议书	批准日期	研究组	唯一识别码*
1.0	ITU-T X.1333	2022-01-07	17	11.1002/1000/14798

关键词

控制系统；导则；远程访问工具；安全

* 获取建议书，请在您的Web浏览器地址栏中输入网址http://handle.itu.int/，其次建议书的识别码，例如http://handle.itu.int/11.1002/1000/11830-en。

前言

国际电信联盟（ITU）是从事电信领域工作的联合国专门机构。ITU-T（国际电信联盟电信标准化部门）在电信，信息和通讯技术领域是国际电信联盟的常设机构。国际电信联盟电信标准化部门负责研究技术，操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

世界电信标准化大会（WTSA），每四年举行一次，确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第一号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性和适应性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提醒注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其它机构提出的有关已申报的知识产权的证据、有效性或适应性不表示意见。

至本建议书截止之日起，国际电联尚未收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新消息，因此特大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：http://www.itu.int/ITU-T/ipr/。

目录

ITU-T X1333建议书

在联网控制系统中使用远程访问工具的安全导则

1 范围

本建议书为在电信网络上联网控制系统中使用远程访问工具（RAT）提供了安全导则。它涵盖以下内容：

- 确定针对RAT不安全配置的威胁及其对联网控制系统的影响；
- 安全控制及其对RAT安全配置的基本理由；
- 每个安全控制的实施导则；以及
- 附录一中RAT安全配置的示例。

2 参考文献

下列ITU-T建议书和其他参考文献的条款，通过在本建议书中的引用而构成本建议书的条款。在出版时，所指出的版本是有效的。所有的建议书和其他参考文献均会得到修订；因此本建议书的使用者应查证是否有可能使用下列建议书和其他参考文献的最新版本。当前有效的ITU-T建议书清单定期出版。本建议书引用某个文件，并非意味着该文件作为单独文件出现时具备建议书的地位。

无。

3 定义

3.1 他处定义的术语

本建议书使用了他处定义的以下术语：

3.1.1 人机接口human machine interface（HMI）[b-IEC 61924-2]：操作员与之交互的系统部分。接口是用户与机器、设备和系统进行交互之手段的集总。接口提供输入手段，允许用户控制系统和输出，允许系统通知用户。

3.2 本建议书定义的术语

无。

4 缩写词和首字母缩略语

本建议书使用了以下缩写词和首字母缩略语：

DDoS 分布式拒绝服务

DMZ 非军事区

DNS 域名服务

DoS 拒绝服务

EWS 工程工作站

HMI 人机接口

ICMP 互联网控制消息协议

IDS 入侵检测系统

IPsec 网际协议安全

LAN 局域网

MAC 媒体接入控制

MDM 移动设备管理

MDMS 电表数据管理系统

NAC 网络访问控制

NFC 近场通信

PIN 个人识别号码

PLC 可编程逻辑控制器

RAT 远程访问工具

RFID 射频识别

SIEM 安全信息和事件管理

SSH 安全外壳

SSL 安全套接层

TLS 传输层安全

URL 统一资源定位符

VM 虚拟机

VPN 虚拟专用网络

5 惯例

本建议书使用下列惯例：

关键词“**应该**”（**should**）指的是一项建议性的、并非绝对要求的要求。

关键词“**可以**”（**may**）表示允许作为选项但并非建议遵守的要求。

在本建议书的正文中，有时会出现“能”（can）或“能够”（could）一词，在这种情况下，它们将被解释为“能/能够”（is able to或was able to）。

附录一中出现的“必须”“应”“将”应解释为没有规范性意图。

6 概述 – 在联网控制系统中的RAT

控制系统用于实现工业目标，例如，物质或能量的制造和运输。控制系统负责保证达成工业目标的预期结果或性能。为确保控制系统的性能，操作员监测来自现场网络中传感器的信息和数据（见图1）。根据数据和信息，操作员可以在需要时控制系统。为维护控制系统或解决技术问题，控制系统供货商的维护工程师可能会访问控制系统。

远程访问工具（RAT）广泛用于工业网络，用于控制系统监测、控制和维护，以降低维护成本并最大限度地缩短发生故障时的响应时间。根据一份报告[b-Kruglov等]，2018年上半年，31.6%的控制系统计算机上使用了RAT，这个数字不包括远程台式电脑连接的数量。

在大多数控制系统情况下，RAT通常用于：

- 从操作员工作站监测/控制人机接口（HMI）；
- 从工程工作站监测/控制HMI；
- 将多个操作员连接到一个操作员工作站；
- 通过外部网络将远程操作员连接到操作员工作站；以及
- 通过外部网络从控制系统供货商维护工程师的计算机上提供对联网控制系统的维护。

这些用例展示了使用RAT进行控制系统监测、控制和维护可以是操作控制系统必不可少的要求。此外，使用RAT将降低维护成本。例如，在上述用例中的前3个项目符号中，可以减少HMI软件的许可证数量。此外，最近的智能设备也可以用作RAT客户端。例如，最终客户可以通过在其智能手机中使用RAT来监测和控制其光伏电池（PV）。

图1显示了基于用例在联网控制系统中使用RAT的一般配置。

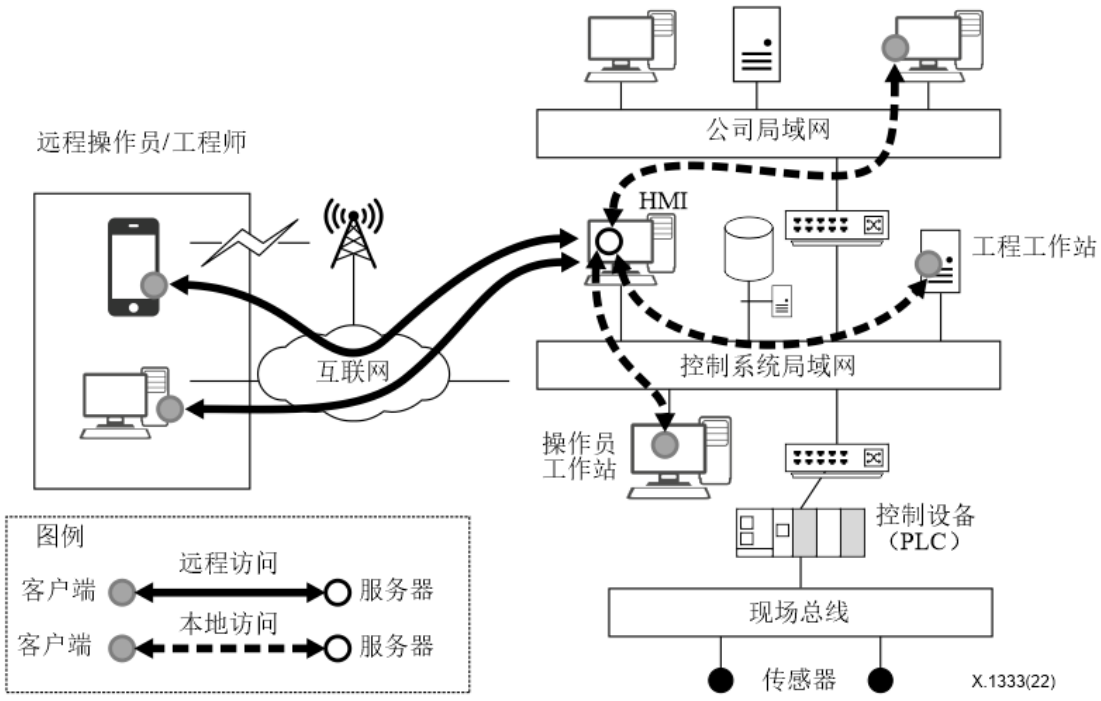


图1 – 在联网控制系统中使用RAT的网络配置

在其他情况下，操作控制系统的组织可以将小型控制系统附加到传统的控制系统上。例如，运行大型发电机的站点可以采用新的燃料电池系统来增加其清洁能源的容量。燃料电池系统包括HMI计算机、控制设备、传感器、电池及其他系统。因此，在本例中，HMI和控制设备可以连接到位于燃料电池系统现场侧的同一子网络上。图2显示了现场使用RAT访问HMI的配置。

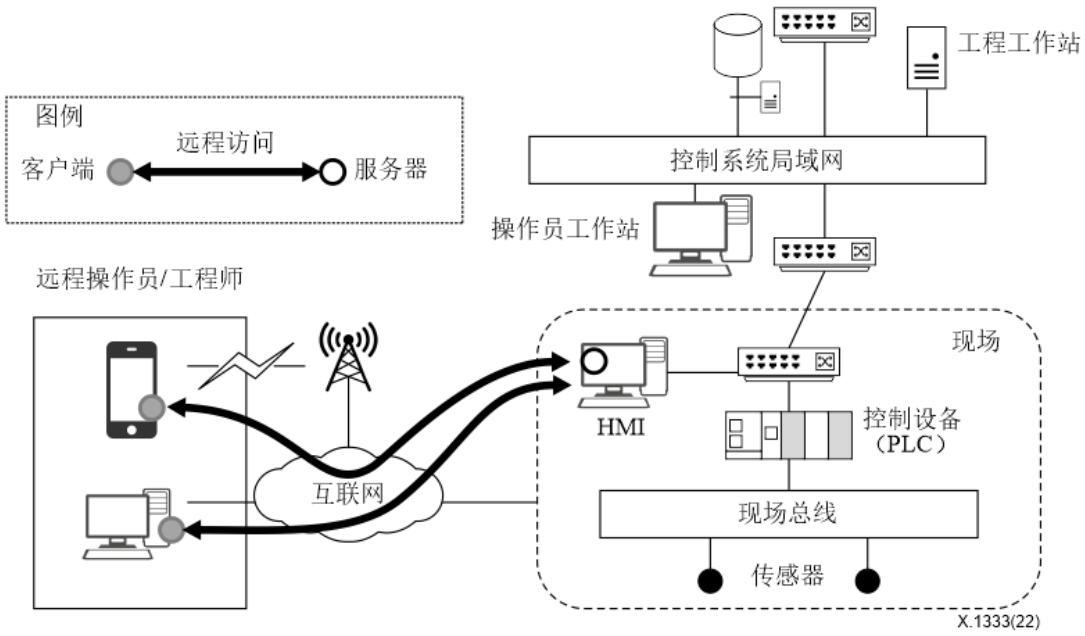


图2 – 在联网控制系统的现场网络中使用RAT的网络配置

RAT提供远程操纵控制系统的能力，它有助于降低维护成本。但与此同时，RAT的不安全配置和RAT中的漏洞可能会显著增加控制系统的攻击面。最严重的问题是，RAT可以作为一个接口，用于从外部网络访问联网控制系统，这通常可以从互联网来访问。因此，一旦攻击者可能危及联网控制系统的RAT客户端，则其就有可能造成系统故障。此外，很难检测到其活动。因此，本建议书侧重于来自联网控制系统外部的RAT连接。

7 在联网控制系统中使用RAT面临的威胁

7.1 RAT客户端面临的威胁

RAT客户端可以安装在远程位置的客户端计算机或者远程操作员或远程维护工程师拥有的移动设备上。远程位置可能在组织的物理保护和组织防火墙的逻辑保护之外。此外，当组织的计算机受到严密管理和严密锁定时，无法很好地管理客户端计算机。因此，使用RAT面临的一系列威胁可能来自安装了RAT客户端的计算机。

应考虑以下客户端计算机和RAT客户端面临的威胁：

- （T1）攻击者可利用客户端计算机或RAT客户端中的漏洞来危害客户端计算机或RAT客户端。一旦攻击者完全控制客户端计算机或RAT客户端，他们就可通过RAT连接到控制系统。
- （T2）攻击者可利用客户端计算机中的拆分隧道。客户端计算机通常不仅连接到RAT服务器，而且连接到任何其他联网系统。因此，完全控制客户端计算机的攻击者可通过未受保护的互联网连接传输从控制系统中获得的关键信息。
- （T3）攻击者可在客户端计算机上安装有针对性的恶意软件，确定敏感信息（例如，登录ID和密码）并窃取信息。一旦攻击者获得信息，他们就可以使用安装在任何其他机器上的RAT客户端而不是客户端计算机来访问RAT服务器。

- （T4）攻击者可通过开源工具支持的蛮力攻击、字典攻击或密码破解来实现对RAT服务器的访问。
- （T5）攻击者可通过删除日志数据来隐藏其在客户端计算机上的活动。由于此威胁，当组织调查事件时，操作控制系统的组织可能无法跟踪攻击者的活动。
- （T6）攻击者可利用对客户端计算机的物理访问。

7.2 RAT服务器面临的威胁

RAT服务器可以安装在联网控制系统中的HMI机器上。由于服务器应打开连接到互联网的服务，因此攻击者可利用该服务的端口。如果该服务未安全地受到保护，那么攻击者可通过该服务访问控制系统。

应考虑以下对客户端计算机和RAT客户端的威胁：

- （T7）攻击者可利用RAT服务器或安装了RAT服务器的机器中的漏洞来破坏机器或RAT服务器。这种攻击可能导致攻击者获得对控制系统的完全控制。例如，一旦攻击者访问机器或RAT服务器，他们就可提升其在设备中的权利或者获得对RAT服务器的完全控制。
- （T8）攻击者可对RAT服务器进行分布式拒绝服务（DDoS）和拒绝服务（DoS）攻击。

7.3 对客户端与服务器之间的通信信道面临的威胁

由于RAT服务器和客户端在联网控制系统中通过互联网连接，因此其他人都可以访问通信信道。如果通信未加密或使用包含已知漏洞的弱方法加密，那么攻击者可利用它们并访问所传输的信息和信道。

应考虑以下对客户端计算机和RAT客户端的威胁：

- （T9）攻击者可利用未受保护的通信，获取敏感信息（例如，登录ID和密码），并使用该信息来访问RAT服务器。当通信信道受到弱密码保护时，攻击者可能会得到相同的结果。一旦攻击者成功访问RAT服务器，他们就可以完全控制控制系统。
- （T10）攻击者可利用包含公开漏洞的弱协议来访问RAT服务器或者造成RAT服务器的用户服务被拒绝。

8 在联网控制系统中使用RAT的安全导则

8.1 RAT客户端的安全导则

8.1.1 软件更新

安全控制

客户端侧RAT软件、操作系统和任何其他软件都应保持在最新状态。

目的

随着攻击技术的进步，该软件可能存在未知的漏洞。当宣布一个新的漏洞时，它是一个0日（0-day）漏洞。攻击者可利用0日漏洞来破坏RAT客户端设备。最近与RAT软件相关的漏洞数量有所增加。2019年，已发现31个虚拟网络计算或类似VNC的软件漏洞。RAT软件供货商会在发布新漏洞时提供安全补丁，用户能够通过采用安全补丁来缓解漏洞。使软件保持最新状态是保持客户端设备安全的最简单方法之一。

实施导则

为使软件保持最新状态，最重要的行动是定期检查是否有新的更新。不幸的是，用户进行这种定期检查并不容易，因此应考虑采用以下自动方法来使软件保持最新状态。

a) 每当执行RAT客户端软件时，应触发安全更新检查方法。

b) 如果有新版本的软件或新的安全更新，应在执行之前应用到客户端软件。

c) RAT客户端运行时也可能定期触发安全更新检查方法。

d) 如果有新版本的软件或新的安全更新，应在终止时应用于客户端软件。

在某些情况下，需要在安装安全补丁后重启RAT客户端设备。与典型的客户端计算机不同，控制系统的RAT客户端目前无法重新启动，因为远程操作员/工程师应持续监测控制系统。在这种环境下，安全更新检查方法在获得用户确认后安装更新软件。

此外，还应更新运行RAT客户端软件的设备中的操作系统和任何其他软件。应启用操作系统的自动更新能力。应定期检查每个应用程序的安全更新，并在补丁可用时立即应用安全补丁。

8.1.2 软件完整性

安全控制

应保护客户端侧RAT软件的完整性。

目的

可在客户端侧安装RAT软件的修改版本。攻击者可能会破坏更新服务器，或者攻击者可能会通过网络钓鱼电子邮件来分发异常更新。感染恶意代码的RAT软件运行正常，但恶意代码会在必要时泄漏信息或与攻击者建立连接。因此，为防止恶意RAT软件的不当行为，应保护RAT软件的完整性。

实施导则

如上所述，由于攻击者能够通过官方供应链分发恶意RAT软件，因此用户必须确定软件是否被修改存在问题。因此，应采用自动完整性检查程序来保护RAT软件的完整性。

对于自动完整性检查程序，应考虑采用以下方法。

a) 当执行软件或启动更新程序时，应启动完整性检查程序。

b) 如果没有任何迹象表明软件已被更改，则应启动软件或更新程序。

c) 完整性检查程序的状态应显示在屏幕上，以便用户知晓该软件是正常的。

d) 软件的完整性值应通过加密方法来生成，以确保软件不会被任何其他人修改。对这种方法，应使用安全的加密算法。

8.1.3 RAT客户端的安全配置

安全控制

RAT客户端侧的配置应符合拥有联网控制系统的组织的安全策略。

目的

尽管RAT软件为安全通信提供了安全能力，但只有在正确配置后才能安全地使用RAT。一般来说，用户希望避免不便，因此他们不想启用安全功能和使用强密码。此外，关于互联网协议安全性（IPsec），用户并不正确了解配置细节。这些错误配置将增加滥用RAT客户端软件的可能性。

实施导则

为了减少RAT客户端错误配置的可能性，最好由操作控制系统的组织来配置客户端。为管理组织对RAT客户端的配置，应考虑采用以下方法。

a) 对RAT服务器使用静态互联网协议（IP）：如果使用一个统一资源定位符（URL）访问虚拟专用网（VPN）网关或RAT服务器，那么远程操作员/工程师可能会遭受网络钓鱼、域名服务器（DNS）欺骗和DNS缓存中毒等多种攻击。对服务器侧使用静态IP地址或硬编码IP地址可缓解这些威胁，并在安全通信信道期间为远程操作员/工程师提供服务器认证。

b) 网络访问控制（NAC）解决方案或移动设备管理（MDM）：NAC提供验证计算机或笔记本电脑状态的能力，而MDM支持检查和控制移动设备的能力。NAC有助于组织在建立连接之前通过验证设备的配置来引导远程操作员/工程师对运行RAT客户端的计算机进行配置。如果设备配置错误，那么NAC将禁止来自设备的网络流量，直至远程操作员/工程师修复错误配置。如果远程操作员使用移动设备来访问RAT服务器，那么MDM是NAC的替代品。

c) 虚拟机（VM）映像：拥有控制系统的组织可将VM映像分发给远程操作员/工程师。在组织创建映像时，应基于组织的安全策略来配置与客户端设备、VPN客户端和RAT客户端有关的所有配置。此外，为保护VM映像本身，应对之进行加密，并在不使用它时，应将之存储于远程操作员/工程师的设备上。

8.1.4 控制用户对客户端设备的访问

安全控制

应仅允许经授权的用户访问RAT客户端软件。

目的

如果对RAT客户端软件的访问仅限于经授权的远程操作员/工程师，则可减少滥用RAT客户端的可能性。

然而，合法的远程操作员/工程师在使用RAT软件时可能暂时离开工作场所，这可能导致滥用所连接的会话。因此，当远程操作员/工程师停止或暂停工作时，应锁定设备。当远程操作员/工程师返回到RAT客户端设备前时，操作员/工程师能够通过使用已建立的识别和认证程序来恢复其工作。

实施导则

可通过让远程操作员/工程师在执行RAT客户端软件时使用有别于执行常规任务所用帐户的帐户来实现此控制。换句话说，远程操作员/工程师应有另一个帐户来使用RAT客户端。此外，帐户的密码应是强密码。

会话锁定是解决后一个问题的有效方法。有两种类型的会话锁定；1) 操作系统级的会话锁定以及2) 应用程序级的会话锁定。大多数操作系统都有会话锁定能力，因此应该在一段时间不活动后启用它。取决于RAT软件，是否提供应用级的会话锁定能力会因软件而异。因此，当操作控制系统的组织选择RAT软件时，会话锁定能力的存在应是一个重要准则。

8.1.5 物理安全

安全要求

应仅允许经授权的远程操作员/工程师物理访问运行RAT客户端软件的设备，并应保护操作员/工程师使用设备的地方免受未经授权的访问。

目的

即使设备和RAT客户端软件被安全地配置为正确使用其安全功能，设备和设备所在的地方也应受到保护，使之免受任何攻击者未经授权的访问。

实施导则

为确保使用它们的设备、软件和环境的物理安全，应考虑采用以下方法：

a) 应通过使用近场通信（NFC）或射频识别（RFID）技术的适当门禁控制系统来保护远程操作员/工程师工作的办公室。为了更强大的安全性，或许会考虑使用生物特征识别（例如，指纹、虹膜和人脸识别）访问控制系统。

b) 办公室门前应安装闭路电视摄像机。

c) 运行RAT客户端软件的设备应使用钢缆锁或其他威慑物来防止被盗。

8.2 RAT服务器的安全导则

8.2.1 用户认证

安全控制

RAT服务应仅在使用双因素认证时才允许用户远程访问资源。

目的

传统的ID和密码认证可能会被破坏，仅凭密码或个人识别号码（PIN）等知识因素将无法确保访问用户是具有适当权限的人。

对本地访问，物理访问控制方法确定并允许合法用户访问系统资源。因此，即使攻击者知道合法用户的ID和密码，也不容易直接访问系统资源。不过，对远程访问，应用物理安全方法和用户识别方法并不容易。因此，即使ID和密码被盗，双因素认证也可降低冒充的可能性，而不是物理安全方法。

实施导则

认证因素可包括“你知什么”（知识因素）、“你有什么”（占有因素）、“你是什么”（固有因素）和“你在哪里”（基于位置的因素）。双因素认证目前倾向于通过占有因素和知识因素或者固有因素和知识因素来实施。

最近，大多数移动设备（例如，笔记本电脑、平板电脑和智能手机）都具有生物特征识别方法，因此包括指纹、虹膜或人脸等在内的固有因素可能是双因素认证的最佳选择。

不过，在某些情形下，可能无法使用生物特征识别方法。例如，如果远程用户在其工作时间内必须戴手套，那么应避免使用涉及指纹的方法。在这些情况下，可采用诸如加密令牌之类的占有因素。

大多数RAT软件都提供限制认证等待时间的能力。在这种情况下，如果RAT服务器在一段时间内没有收到来自用户的响应，那么它将丢弃认证请求。因此，它将有助于减少拒绝服务攻击的可能性。

8.2.2 用户授权

安全控制

远程用户的帐户应仅具有执行其功能所需的最低限度权限。

目的

为限制攻击的影响，远程用户的权限应限制为执行其功能所需的最低权限。

实施导则

RAT软件通常不提供细粒度的授权方法。大多数RAT软件都只提供两种模式，例如，只读模式和全控模式。因此，如果攻击者可访问RAT服务器，那么他们就可完全破坏设备。为避免这种威胁，授予远程用户帐户的权限应限制为执行其功能所需的最低权限。

为此，首先，远程用户帐户不应是管理员帐户，并且不应授予远程用户帐户能够更改RAT服务器的权限。安装软件、配置操作系统、配置系统或许可作为有限权限之一。

其次，还应对应用程序进行访问控制。远程用户帐户不能运行除软件操作和监测系统之外的任何其他软件。如果远程用户可在RAT服务器的机器上打开终端程序，那么用户能通过RAT服务器访问另一个系统。这对攻击者而言将是一个极大的“利好”消息。

8.2.3 定期重新认证

安全控制

RAT服务器应在一段时间后对用户和客户端设备进行重新认证。

目的

为确保只有经授权的远程操作员/工程师才能使用远程访问，RAT服务器应要求他们在长时间的远程访问会话期间定期进行重新认证。这有助于确保在RAT服务器与客户端之间建立连接的情况下，即使设备被盗，未经授权的人也无法使用远程访问。

此外，网络级重新认证有助于降低遭受会话劫持攻击的可能性。

实施导则

RAT服务器软件本身不提供一段时间后重新认证的能力，而大多数VPN网关都提供安全功能。因此，为正确实施此控制，应在RAT客户端与服务器之间使用VPN。

此外，大多数VPN网关都提供有关客户端重新认证的能力。因此，组织应启用VPN网关能力，以便在一段时间后对用户或设备进行认证。例如，当通过传输层安全性（TLS）1.3版进行RAT通信时，应启用握手后客户端认证扩展。如果启用了扩展，那么TLS服务器将在建立TLS连接后请求客户端认证。

8.2.4 软件更新

安全控制

RAT服务器软件、操作系统和服务器设备中的任何其他软件都应保持在最新状态。

目的

第8.2.4节中控制对应的目的与第8.1.1节中规定的目的相同。

实施导则

第8.2.4节中控制对应的导则与第8.1.1节中规定的导则相同。

8.3 网络的安全导则

8.3.1 网络访问控制

安全控制

应仅允许合法用户访问RAT服务器与RAT客户端之间的网络通信。

目的

访问网络通信是破坏服务或系统的第一步。攻击者可在RAT服务器与客户端之间收集信息和数据，并将伪造的数据注入通信信道，这可导致中间人攻击、恶意软件分发和DoS攻击。为保护RAT服务和控制系统，应限制恶意用户访问RAT服务器与客户端之间的网络通信。

实施导则

有若干种方法可以控制对网络通信的访问并保护其内容。或可考虑选择以下方法：

- 可采用租用专线，以防止非授权用户访问电表数据管理系统（MDMS）与第三方服务提供商之间的连接。
- 应在RAT客户端与服务器之间采用诸如IPsec和安全套接层（SSL）VPN等安全通信措施。对RAT流量应在VPN内通过隧道传输。
- 如果VPN不可行，那么至少应通过TLS 1.3版来执行远程访问。

当采用安全通信方法（包括VPN和TLS）时，应考虑安全加密算法。[b-ITU-T X.1197]提供了一份有关安全算法和密钥长度示例的清单。在通信信道建立期间，如果客户端不使用安全算法和密钥长度，那么VPN网关或RAT服务器应拒绝连接请求。

8.3.2 网络级相互认证

安全控制

对RAT服务器与RAT客户端之间的通信信道应采用相互认证。

目的

对通信信道应实施相互认证方法，以便RAT客户端可在向RAT服务器提供认证证书之前验证其合法性。利用该功能，RAT服务可避免RAT客户端与服务器之间的中间人攻击。

实施导则

在RAT通信中使用IPsec、SSL VPN或经TLS的通信时，应使用服务器的证书和客户端的证书来做相互认证。客户端通过验证服务器的证书来对服务器进行认证，以确保服务器是合法的。

大多数VPN解决方案都提供服务器认证功能，但在许多情况下并未启用该功能。因此，当控制系统采用VPN来保护RAT服务时，应启用服务器认证选项。

此外，在TLS中，通常只有服务器通过验证客户端的凭证（如证书）来对客户端进行认证，因为服务器认证是一个选项。因此，如果服务器与客户端之间的通信受RAT服务的TLS保护，则应需要在服务器与客户端之间交换彼此的证书。

最后，应启用认证超时能力和限制并发会话能力。正确丢弃等待客户端认证响应的连接请求是缓解拒绝服务攻击的关键。

8.3.3 网络不当行为检测

安全控制

对RAT服务器所连接的网络应采用网络不当行为检测。

目的

即使RAT客户端采用了各种安全方法，运行RAT客户端的设备仍有可能遭受危害。例如，如果攻击者可通过受破坏的RAT客户端访问联网控制系统的网络，他们也可访问RAT服务器允许访问的任何资源。在这种情况下，远程操作员/工程师与攻击者之间的唯一区别仅是行为。远程操作员/工程师了解其所连接的网络和系统，而攻击者应需要进行侦察以找出目标在网络中的位置。因此，基于网络流量的网络不当行为检测系统可帮助检测网络攻击。

实施导则

网络不当行为检测系统应监测和检查RAT客户端与RAT服务器之间的所有消息。此外，检测系统还应监测和检查从运行RAT服务器的设备到联网控制系统中任何其他设备的所有消息。因此，应将检测系统置于RAT服务器所在的同一个子网中，并且它应从启用了端口镜像策略的网络设备处收集流量。例如，在如图2所示的网络中，启用了现场网络中网络交换机的端口镜像策略，检测系统从启用了端口镜像策略的接口处收集流量。

当应用安全通信方法（例如，IPsec、SSL VPN或基于TLS的通信）时，应将提供安全通信信道的安全设备置于RAT服务器所在的子网周边。例如，应将VPN设备置于网络设备之前，以便网络不当行为检测系统可对所有分组进行检查。

检测方法可分为静态检测、误用检测和异常检测等三种类型。对运行远程访问工具的环境，应采用误用检测和异常检测相结合的方式来检测已知的攻击和未知的攻击。

8.3.4 安全网络配置

安全控制

对安装RAT服务器的网络应正确分段和隔离。

目的

网络分段指的是将网络划分为若干较小的网络，而网络隔离指的是执行策略以控制主机之间的通信。通过将安装RAT服务器的网络与其他网络相隔离，即使RAT服务器被攻破，也可防止攻击者访问其他控制系统资源。

实施导则

安装RAT服务器的网络应与控制系统中的其他网络相隔离，并应根据白名单规则来控制与RAT服务器之间的往来通信。可以通过非军事区（DMZ）的概念来实施此类安全措施。防火墙对包含RAT服务器的子网进行划分，依据防火墙中的规则，仅允许经授权的通信，例如，1) RAT客户端与RAT服务器之间的通信；2) RAT服务器与控制系统中其他资源之间的通信。或可对防火墙规则采用服务级的访问控制清单。这意味着应将规则定义为IP地址和端口号的组合。

例如，现场网络中的HMI可以通过防火墙与现场网络中的其他资源相隔离，如图3所示。防火墙根据其规则来检查所有进出RAT服务器的分组，并定义规则以确定允许RAT服务器上的哪些服务与其他设备上的哪些服务进行通信。允许由HMI上的工程工作站（EWS）软件服务发起的通信到达控制设备（即图3中的可编程逻辑控制器（PLC））。与此相反，防火墙阻止由HMI上的安全外壳（SSH）发起的通信。

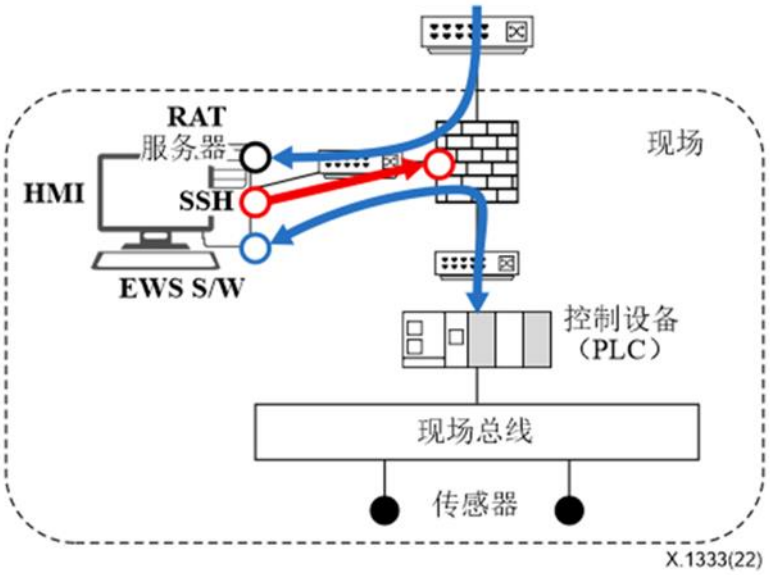


图3 – 在现场网络中使用RAT的网络分段和隔离

8.4 审计跟踪的安全导则

8.4.1 日志记录

安全控制

对系统和网络安全事件应做好日志记录并保护好日志。

目的

系统和网络安全事件日志是任何系统安全管理的核心。通过对安全相关事件的审查和分析，可以及时发现安全问题。因此，RAT服务器生成的事件日志粒度越细，组织就越容易检测到安全问题。

实施导则

一些RAT软件提供更细粒度的日志记录能力，例如，每个应用程序的使用情况和服务器设备中的数据操作情况，而其他软件提供简单的日志记录能力，例如，与RAT服务器的连接以及断开与之的连接。因此，组织在选择RAT软件时应考虑RAT软件生成的安全事件日志的粒度。

如果RAT软件提供简单的日志能力，那么组织还应考虑安装RAT服务器的操作系统的日志记录能力。为此，服务器设备中的远程用户帐户应与其他帐户相隔离。在这种情况下，安全管理员应对远程用户帐户记录的安全事件进行审查，以检测不当行为。

除了系统事件日志外，还应生成网络事件日志。应记录所有RAT连接请求及其结果（即成功或失败）。此外，还应记录与远程连接协议（例如，终端协议、工业控制协议和互联网控制消息协议（ICMP））有关的所有事件。如上所述，在攻击的第一阶段，攻击者通常会对系统进行侦察。可用各种远程连接协议来侦察。因此，网络事件日志将帮助安全管理员检测RAT服务器上出现的不当行为。

生成的日志应安全地存储在日志服务器中。如果日志存储在系统的本地存储器中，那么攻击者就有可能操纵或破坏日志。因此，事件日志应存储在单独的日志服务器中。

安全管理员应定期对日志进行审查和分析。

8.5 安全威胁与安全控制之间的关系

表1显示了安全威胁与安全控制之间的关系，当中小格中的空心圆表示为缓解具体威胁而应实施的特定安全控制。

表1 – 安全威胁与安全控制之间的关系

		7.1客户端						7.2服务器		7.3网络	
		T1	T2	T3	T4	T5	T6	T7	T8	T9	T10
客户端	8.1.1软件更新	O									
	8.1.2软件完整性	O	O								
	8.1.3安全配置	O	O	O							
	8.1.4用户访问控制				O		O				
	8.1.5物理安全						O				
服务器	8.2.1用户认证								O		
	8.2.2用户授权						O				
	8.2.3定期重新认证						O				
	8.2.4软件更新							O			
网络	8.3.1网络访问控制									O	
	8.3.2相互认证								O	O	
	8.3.3不当行为检测					O				O	O
	8.3.4安全网络配置										O
审计	8.4.1日志记录					O					

附录I

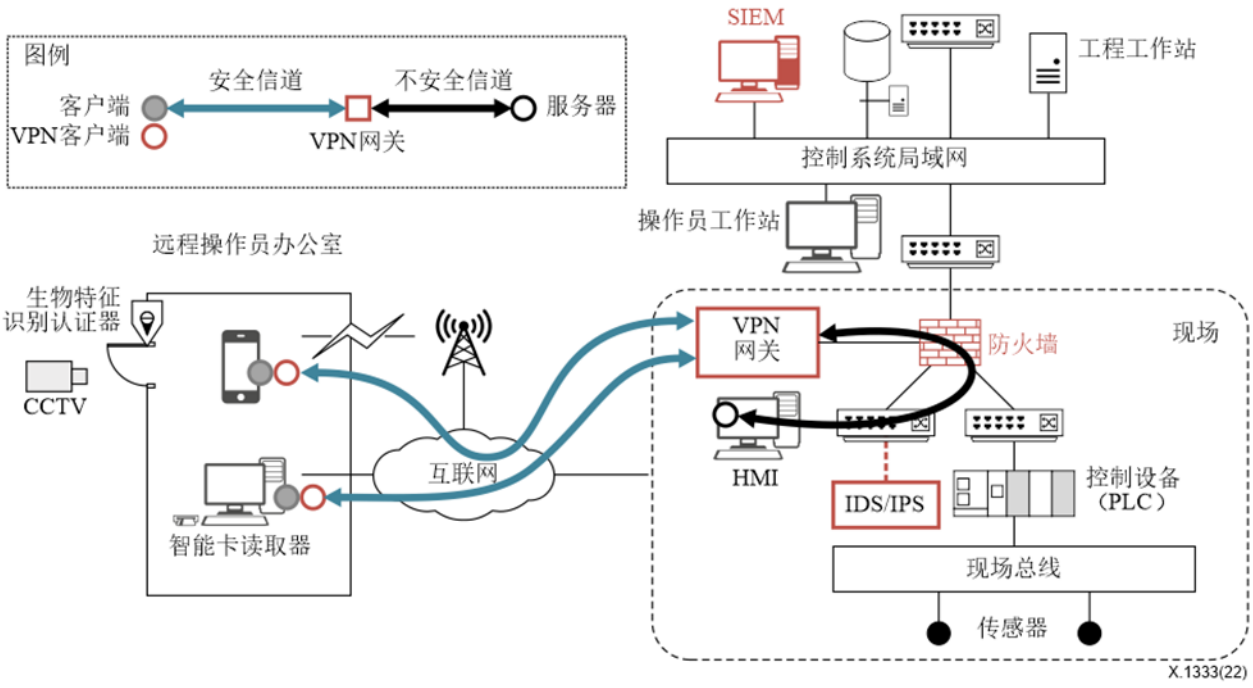
在可持续能源中的远程访问工具安全配置示例

（此附录非本建议书不可或缺的组成部分。）

I.1 系统概述

许多传感器和执行器安装在发电机上。传感器将测量数据提供给控制设备（例如，图I-1中的PLC），操作员根据数据，通过HMI或工程工作站来监测发电机的状态。操作员根据状态，通过HMI（或工程工作站）和PLC来控制执行器。例如，当台风来临时，操作员会停止风力涡轮机叶片的旋转。连接传感器、执行器和控制设备的网络称为现场网络。在现场网络中，通常安装用于监测和控制发电机的HMI。

在某些情形下，使用风力（风力涡轮机）、氢（燃料电池）和太阳能（光伏）等可持续能源的发电机由远程操作员来操作。远程操作员监测发电机的状态并对之实施控制，以实现高效发电。



图I-1 – 可持续能源控制系统的安全网络示例

I.2 安全配置

图I-1显示了可持续能源的安全网络配置示例。在本节的其余部分，将描述每个组件的安全措施，包括RAT客户端、RAT服务器、网络和安全事件日志。

I.2.1 RAT客户端

为RAT客户端创建一个单独的帐户，且客户端软件仅能由该帐户访问。

每当远程操作员打开RAT客户端软件时，都会启动更新检查和完整性检查过程，并将在启动RAT客户端软件之前进行更新。

NAC客户端检查设备的安全级别，如果丢失任何安全配置，那么它会阻止互联网连接。例如，若未开启杀毒软件和个人防火墙，则NAC不会允许任何通信连接。

所有运行RAT客户端的设备都在远程操作员的办公室进行操作。对办公室的访问控制通过安装在办公室门前的生物特征识别认证器（例如，指纹或面部识别）和闭路电视来实现。

I.2.2 RAT服务器

当远程操作员尝试通过RAT客户端建立一个RAT连接时，需要双因素认证（即密码和智能卡）。此外，还使用了VPN网关和RAT服务器的静态IP地址。

在相互认证之前，请求连接的主机在VPN网关被其IP地址和媒体接入控制（MAC）地址过滤掉。此外，VPN客户端与VPN网关之间的通信信道的生命周期为8小时。因此，远程操作员必须每8小时为VPN连接再提供一次其密码和智能卡。

HMI中远程操作员的账号与其他账号相分离，以限制远程操作员的权限，并为账号生成细粒度的日志。

I.2.3 网络

IPsec VPN保护RAT客户端与服务器之间的通信信道。在连接到RAT服务器之前，安装在远程操作员设备中的VPN客户端应与VPN网关建立一条安全信道。为提供128位的最低安全等级，如[b-IETF RFC 6379]中所述，对IPsec VPN，使用加密套件*Suite-B-GCM-256*。对IKEv2认证，如[b-IETF RFC 6380]中所述，对IPsec VPN，使用*ECDSA-256*。为了平衡安全性和开销，IKE SA的生命周期设置为24小时，IPsec SA的生命周期设置为8小时。

现场网络分为两个部分，例如，用于HMI的DMZ和用于PLC、传感器和执行器的现场网络。此外，防火墙位于控制系统局域网（LAN）、现场网络和用于网络隔离的DMZ之间。因此，允许来自HMI上的EWS的通信传输到现场网络，但防火墙会阻止从HMI到任何其他网络的任何其他流量。

入侵检测系统（IDS）或IPS安装在DMZ中，且它从配置为流量镜像的交换机端口接收传入和传出的网络流量。

I.2.4 安全事件日志

远程访问帐户生成的安全事件记录在HMI系统中，并将它们传输给安全信息和事件管理（SIEM）系统。运营可持续能源的组织的安全管理员将使用SIEM系统来定期查看日志。

参考文献

[b-ITU-T X.1197] Recommendation ITU-T X.1197 (2012), *Guidelines on criteria for selecting cryptographic algorithms for IPTV service and content protection*

[b-IEC 61924-2] IEC 61924-2:2012, *Maritime navigation and radiocommunication equipment and systems - Integrated navigation systems – Part 2: Modular structure for INS - Operational and performance requirements, methods of testing and required test results.*

[b-IETF RFC 6379] IETF RFC 6379 (2011), *Suite B Cryptographic Suites for IPsec.*

[b-IETF RFC 6380] IETF RFC 6380 (2011), *Suite B Profile for Internet Protocol Security (IPsec).*

[b-Kruglov et al.] Kirill Kruglov, Evgeny Goncharov (2018), *Threats posed by using RATs in ICS*, Technical Report, Kaspersky Lab ICS CERT.
https://ics-cert.kaspersky.com/reports/2018/09/20/threats-posed-by-using-rats-in-ics/

ITU-T系列建议书

A系列	ITU-T工作的组织
D系列	资费及结算原则和国际电信/ICT的经济和政策问题
E系列	综合网络运行、电话业务、业务运行和人为因素
F系列	非话电信业务
G系列	传输系统和媒介、数字系统和网络
H系列	视听及多媒体系统
I系列	综合业务数字网
J系列	有线网络和电视、声音节目及其它多媒体信号的传输
K系列	干扰的防护
L系列	环境与ICT、气候变化、电子废物、节能；线缆和外部设备其他组件的建设、安装和保护
M系列	电信管理，包括TMN和网络维护
N系列	维护：国际声音节目和电视传输电路
O系列	测量设备的技术规范
P系列	电话传输质量、电话设施及本地线路网络
Q系列	交换和信令，以及相关联的测量和测试
R系列	电报传输
S系列	电报业务终端设备
T系列	远程信息处理业务的终端设备
U系列	电报交换
V系列	电话网上的数据通信
X系列	**数据网、开放系统通信和安全性**
Y系列	全球信息基础设施、互联网协议问题、下一代网络、物联网和智慧城市
Z系列	用于电信系统的语言和一般软件问题

瑞士印刷
2022年，日内瓦