安全变电站网络架构的设计与调试

Andreas Klien[1], Yann Gosteli[2], Stefan Mattmann[3]

[1]OMICRON electronics GmbH, Klaus, Austria (andreas.klien@omicronenergy.com)
[2]Centralschweizer Kraftwerke (CKW) AG, Luzern, Switzerland (yann.gosteli@ckw.ch)
[3]Centralschweizer Kraftwerke (CKW) AG, Luzern, Switzerland (stefan.mattmann@ckw.ch)

关键词：网络安全, IEC 61850, 入侵检测, 变电站自动化

摘要

电力设施网络安全审核员越来越多地将控制中心视为高危攻击途径，同时将变电站视为网络攻击的潜在切入点。这些重大风险因素存在于日常工作流程中，包括如何实现保护和控制系统的调试，以及如何实施远程维护访问等方面。因此，必须对保护和控制系统的网络架构进行安全性审查。为此，瑞士发电和配电设施公司 Centralschweizer Kraftwerke AG (CKW) 于 2016/2017 年启动了为其二次系统开发新网络安全参考架构的项目。他们的设计采取应对措施处理不同的攻击途径，同时在可维护性和安全性之间提供合理的平衡。设计纳入多个安全级别，涵盖多个防火墙层。此外还应用了入侵检测系统 (IDS)。事实证明，为变电站选择适合的 IDS 并非易事，因为许多 IDS 并不支持变电站网络的要求。本文首先列举了几种最重要的变电站攻击途径，随后描述了由 CKW 在 110kV 新建变电站项目中首次实施的安全架构。最后总结了为变电站选择适合的 IDS 时可以借鉴的经验，以及在该项目的工厂验收测试中获得的启示。

1. 引言

1.1. 变电站攻击途径

在本文中，我们将对变电站的网络攻击定义为攻击者修改、降级或禁用变电站的保护、自动化或控制设备当中至少一种服务的事件。为此，攻击者可能会利用 Figure 1 中描述的攻击路径之一 [1]。

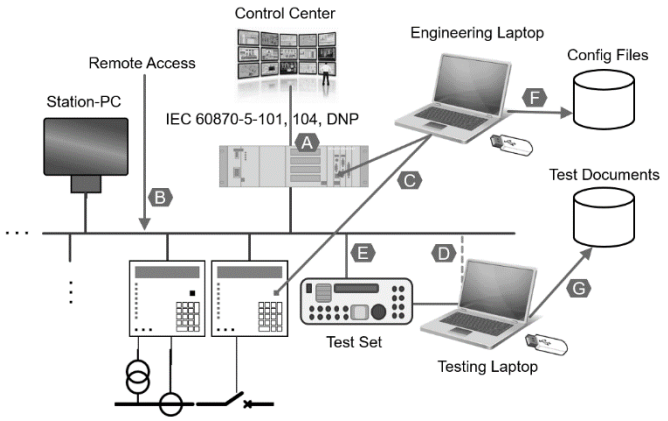

图 1 变电站的攻击途径 [1]

攻击者可能通过控制中心连接 (**A**) 进入，与乌克兰电网遭受首次网络攻击时发生的情况类似，网关设备固件被修改（导致设备毁坏）[2]，或者通过远程访问连接 (**B**) 进入，类似于 2016 年乌克兰第二次网络攻击 [3] 以及针对关键设备 PLC 的“TRITON”网络攻击 [4]。

另一个进入点是通过直连变电站设备或变电站网络的工程师 PC (**C**)。当保护工程师将其 PC 连接到继电器以修改（保护）整定值时，PC 可能会在继电器上安装恶意软件，与 2010 年著名的“Stuxnet”网络攻击中 PLC 的遭遇类似 [5]。

用来测试 IEC 61850 系统 (**D**) 的笔记本电脑通常直接连接到变电站总线，这也是感染智能电子设备 (IED) 的潜在方式。因此，可采用新的 IEC 61850 测试工具，在测试 PC 和变电站网络之间进行网络安全隔离。然而测试设备本身 (**E**) 也是潜在的攻击进入路径。正因为如此，测试仪供应商必须投资加强其设备，以确保攻击者对于该进入路径失去兴趣，这一点很重要。

整定值 (**F**) 和测试文档 (**G**) 的存储文件也可能是感染源。其服务器或存储位置因而也属于关键外围，不应位于普通的办公室 IT 区域。因此，有必要针对此类数据引入单独的、隔离的和受保护的数据管理解决方案。

2. 新的变电站网络安全架构

2.1. OT 网络安全领域的前沿进展

瑞士电力行业协会 VSE 成立了运行技术 (OT) 安全工作组，随后发布了行业推荐文件：《电力系统运行技术基本保护手册》。手册参考了国家标准技术研究所 (NIST) 的“关键基础设施的网络安全框架”[7]，该框架持续修改完善，最新版本于 2018 年更新。NIST 框架基于以下假设：针对网络攻击防护无法做到 100% 万无一失。只要足够了解并经过充分准备，所有安全措施都可能被攻破。基于这一点，NIST 框架建议采用包含以下五个步骤的流程：“识别”、“保护”、“检测”、“响应”，“恢复”。因此，第一步就是明确攻击途径（识别），如本文上一节所述。之后，即可在后续步骤中实施应对措施（保护）。如果攻击者仍然能够突破这些障碍，则必须检测该攻击（检测），并最好立即采取行动（响应），以尽快恢复正常状态（恢复）。借助在“检测和响应”中获得的信息和经验，可以识别新攻击途径，采取新应对措施，使流程得以重复进行。

瑞士的行业建议非常重视组织内部人员、技术和流程的互动。例如，连续监视或入侵检测（检测）仅在报警消息得到适当响应时才有意义。因而报警消息需要让参与响应过程的每位人员理解，包括 OT 工程师和 IT 安全专家，否则响应过程将变得效率低下。此外如果 IDS 传递的误报过多，最终会导致所有报警遭到忽略。

2.2. CKW 的 OT 网络安全计划 [6]

近年来，OT 安全（特别是控制和保护系统的安全）这一主题在 CKW 日益受到重视。原因固然在于瑞士推行的行业建议，但也要归结于 CKW 近年来进行的 OT 安全评估。这些评估显示了变电站所用网络和站内控制技术的薄弱环节。例如，在站内控制计算机上发现了不安全的区域过渡和一些存在危害性的远程访问方法。此外，无法评估变电站网络中当前是否正在发生攻击，或者网络上是否存在可能预示即将发生攻击的可疑活动。

基于这些评估结果，CKW 内部设定了消除主要缺陷并加强其未来变电站网络安全架构要求的目标，这些结果也由此整合到 CKW 新变电站设计标准当中。

除了制定自己的设计标准，CKW 还得以参与瑞士工作组编制上述 OT 安全手册的工作。以这种信息交流为基础，CKW 能够始终将工作组的研究结果纳入其自己的设计标准。

CKW 项目团队于 2016/2017 年开始筹划新建变电站“US Rothenburg”，该变电站拟于 2020 年投入运营。他们在该项目中应用了 CKW 的新安全架构标准，并遵循了瑞士 OT 安全手册的最新建议。为了能够实施这些复杂的安全措施，CKW 决定自行实施网络架构和交换机配置。

2.3. 网络设计

在 US Rothenburg 的网络设计中，每个区域都设有防护墙，旨在尽可能阻止攻击。Figure 2 所示为 US Rothenburg 变电站网络。

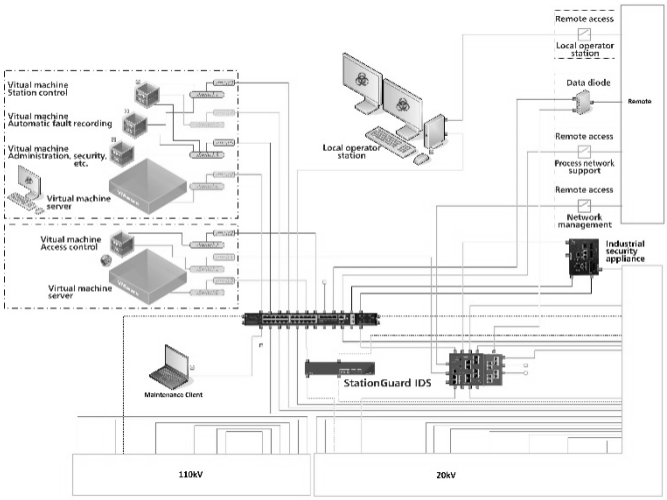

图 2 US Rothenburg 网络架构 [6]

该架构采取一系列安全措施应对本文 1.1 节中描述的所有攻击途径。远程连接得到最优先处理。这些远程连接不仅采用防火墙和隧道解决方案来保护，而且默认为禁用状态，仅在需要时才会启用远程访问连接。这意味着多名人员参与启用远程访问，类似于双重身份验证过程。

与控制中心进行监视控制和数据采集 (SCADA) 通信时使用 IEC 60870-5-101 串行协议。出于维护目的访问所有变电站设备都只能通过得到适当保护的特殊工作站进行，这些工作站已虚拟化并位于中央位置，此类维护远程访问还必须远程启用。

SCADA 系统、故障录波系统和安全系统服务器已虚拟化，并在变电站本地的主机上运行。甚至本地 HMI 工作站也只能通过附加的本地防火墙借助远程桌面来访问这些系统。采用基于角

色的访问控制 (RBAC)，也即并非每台设备对应一个密码，而是每位用户一个密码。其优点是工程师可在所有变电站使用自己的密码。如果员工离开公司，轻松删除其用户即可，无需更改密码。这种用户管理使用中央 Active Directory (AD) 服务器和变电站本地的 RADIUS 服务器实现。用户必须使用 AD 登录，AD 会为他们分配必要的权限。如果需要，可以从中心位置启用对中央 AD 的访问。此外，用户必须使用单独的用户名和密码登录每台 IED。因此，IED 将使用本地 RADIUS 服务器来检查用户和密码的身份验证，并检索为此用户分配的权限。这既适用于借助工程配置软件工具访问 IED，也适用于在 IED 显示屏上进行相关操作。不需要使用标准密码。

连接到变电站网络的所有 PC 均经过网络安全加强。主要方法包括根据变电站的通信矩阵配置 Windows 防火墙，以及根据该客户端的角色禁用不需要的操作系统功能。

作为附加安全措施的网络访问控制通过 MAC 身份验证旁路实现，也即只有注册设备才能连接到网络交换机。

如发生故障，交换机还必须识别并接受备用设备。在变电站网络交换机和防火墙中，访问控制列表配置为强制允许哪台设备与哪个其他网络设备通信，包括使用的协议和交换机端口。

站内总线网络与用于配置和维护的网络在逻辑上 (VLAN) 及物理上均保持隔离。这意味着对于每台 IED，IEC 61850 通信 MMS 和 GOOSE 所运行的网络在与维护工作所使用的网络是不同的。。此外，整个站内总线网络采用分段结构，比如，以下区段通过防火墙分隔：

- 110kV（GOOSE 和 MMS）
- 20kV（GOOSE 和 MMS）
- 本地 HMI
- 协议网关
- 辅助系统
- IED 和客户端的维护网络
- 管理网络、VM、RADIUS

从变电站到更高级别网络区域的通信还另外由数据“二极管”来保护。该数据“二极管”确保只能进行上传的单向通信，由此又增加一重安全性。

入侵检测系统 (IDS) 采用白名单方法监视系统中的整个网络流量，即默认情况下所有不在白名单中的未知流量都会产生报警。IDS 通过 RTU 向控制中心报警，并通过专门的报警记录协议向安全操作中心报警。

3. 入侵检测

CKW 的安全架构基于设立网络区段，彼此由防火墙分隔。防火墙配置会准确指定哪些协议可用于跨网段通信。但是，防火墙允许的协议（例如 IEC 61850 中使用的 MMS/GOOSE）和设备供应商工程配置软件的私有通信协议也可能遭到利用，造成设备受到攻击乃至发生感染。对于这类场景，CKW 希望能够在早期阶段检测到未经授权的活动。为此，CKW 决定在其参考架构中使用 IDS。

为了能够分析最关键的流量，即网关和 IED 之间的通信，至少应将网关的所有流量镜像到 IDS 中。通常情况下，不需要覆盖间隔层交换机，因为通常只有多播流量（如 GOOSE 或采样值）来自该交换机。为了确保同样能分析所有网络分支中的所有单播流量，建议将所有交换机镜像到 IDS 中。

在 CKW 架构中，IDS 连接到所有网络交换机上的镜像端口。这意味着 IDS 会分析站内总线上的流量以及从远程传入流经防火墙之前和之后的流量。

3.1. 变电站 IDS 的要求

事实证明，为变电站选择适合的 IDS 并非易事。一项重要的要求是负责所有 IED 和网络设备的保护、控制和网络工程师能够轻松操作 IDS。为了支持报警响应过程，IDS 报警应可轻松关联变电站中的事件和 HMI 中的事件日志。因此，IDS 应基于变电站运行的视角，而非仅限于 IT 专业安全术语。

直到最近，实现 IDS 仍然只有两种主要方法：基于签名和“基于学习”的方法。

基于签名的方法配合使用黑名单，类似于标准 PC 的病毒扫描程序。该方法扫描已知的病毒和恶意软件的特征模式。但问题是对变电站的网络攻击仅发生过少数几次，然而即便是从未发生过的新的攻击，也可能产生严重的后果。变电站 IDS 必须能在事先对攻击不了解的情况下检测攻击。

因此，更多 IDS 系统采用的是“基于学习”的方法。IDS 会查看不同协议的通用协议参数，以了解每个参数的平均值和频率。
之后，在正常运行期间，每当网络通信明显偏离所学平均值，即触发报警。而这样一来，对于在学习阶段未发生的所有事件都会触发误报，比如，其中就包括跳闸和开关操作或例行保护测试。由于系统不了解网络上报文的含义，因此报警消息参考的是通用协议参数，例如“MMS confirmed-write-response failed”。这会导致大量误报，每项报警都需要由 IT 专家和 IEC 61850 专家进行检查。响应过程中的这种资源占用对于 CKW 来说是不可接受的。

3.2. 使用的 IDS 方法

对于 IEC 61850 变电站，整个自动化系统（包括所有 IED、数据模型及其通信模式）以标准化格式 (SCL) 进行描述。该信息允许使用不同的方法来检测入侵：监控系统可以创建变电站自动化系统的系统模型，并可以将网络上的每个数据包与该模型进行比较。甚至包含在通信（GOOSE、MMS、SV）信息中的变量，也可以根据系统模型得出的期望值进行评估。因此，该系统模型包含一个白名单，与系统模型不匹配的所有数据包都会触发报警。CKW 选择了基于此方法的 IDS (OMICRON StationGuard)。
这种方法的优势在于，不仅可以检测到格式错误的数据包和禁止的 MMS 控制操作等网络安全威胁，还可以检测到通信故障、时间同步问题以及由此导致的某些设备故障，进而触发报警。
通过使用 SCL 文件中的变电站描述部分，可以自动创建变电站的概览图，并可在该图中显示报警。这类显示有助于识别触发报警的操作是否为有意之举：例如，该事件可能由工程师在测试情况下引起，或者可能确实是受感染测试笔记本电脑的恶意活动。

撰写本文时，US Rothenburg 工厂验收测试 (FAT) 业已完成，调试工作尚在进行中。执行 FAT 时，必须完成几乎全部网络配置才能测试设计是否有效。我们还了解到，IDS 需要支持多级防火墙路由。防火墙前后的流量存在多次重复，可能会使一般的 IDS 显示混乱。不过，所选 IDS 完全可以满足该场景的要求。此外，针对防火墙配置创建通信矩阵需要花费大量精力，因为必须人工完成。由于 IDS 已从 SCL 中取得该白名单，因此将来也可自动执行此过程。

4. 结论与展望

如果攻击者能够影响一个或多个变电站，则可能对电网造成严重后果。变电站存在可能导致绕过防火墙的多种攻击途径。CKW 的安全变电站网络架构可为本文列出的攻击途径提供多项对策。这些安全措施提供高级别的安全性，同时还允许通过远程访问执行有效的维护和工程配置工作。该架构依赖网络核心中的入侵检测。对于 IEC 61850 变电站，可以采取 IDS 方法，使用 SCL 自动生成所有允许网络流量的白名单。这样还能以保护、自动化和控制工程师的语言显示检测到的事件，以便他们可与网络安全工程师协作，从而高效查明事件原因。

网络安全的本质是每项设计都有进一步完善的空间。例如，这些改进措施包括将当前使用的基于 MAC 的方法改为根据 802.1X 实行基于证书的网络访问控制 [8]。不过，为此需要有更多的 IED 支持 802.1X 标准，而目前情况并非如此。后续文章将对该项目调试中收集到的相应数据进行分析，并对该变电站未来进行的安全评估和渗透测试的结果予以记录。

5. 参考文献

[1] Klien, A.: ‘New approach for detecting cyber intrusions in IEC 61850 substations’, PAC World Conference Europe, Glasgow, 2019
[2] ‘Analysis of the Cyber Attack on the Ukrainian Power Grid’, SANS, E-ISAC, https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf, accessed November 2019
[3] ‘WIN32/INDUSTROYER - A new threat for industrial control systems’, https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf, accessed November 2019
[4] ‘Threat Research - Attackers Deploy New ICS Attack Framework “TRITON” and Cause Operational Disruption to Critical Infrastructure’, https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html, accessed November 2019
[5] D. Kushner: ‘The Real Story of Stuxnet

How Kaspersky Lab tracked down the malware that stymied Iran’s nuclear-fuel enrichment program’, IEEE Spectrum, February 2013
[6] Gosteli, Y., Klien A.: ‘Sichere Stationsleittechnik – Neue Cyber Security Architektur mit Intrusion Detection in der US Rothenburg’, bulletin.ch, 2019, 6, pp 50-52
[7] NIST: ‘Framework for improving critical infrastructure cybersecurity, version 1.1, National Institute of Standards and Technology, April 2018
[8] IEEE: ‘802.1X-2010 - IEEE Standard for Local and metropolitan area networks--Port-Based Network Access Control’, International Standard, February 2010

OMICRON 是一家以创新性的测试与诊断解决方案服务于电力行业的国际化公司。OMICRON 产品的应用可以让用户能够对其系统中的一次和二次设备的状态作出评估，并且完全可以信赖。 再加上在咨询、 调试、 测试、 诊断和培训方面提供的服务，形成了完整的产品范围。

全球超过 160 个国家的用户依赖于本公司的能力来提供质量优良的领先技术。 位于各大洲的服务中心提供广泛的知识及优质的客户服务。所有这一切，与我们强大的经销网络结合在一起， 使我们成为电力行业的市场领先者。

OMICRON 中国办事处

奥地电力技术咨询（上海）有限公司
中国上海市杨浦区杨树浦路 288 号建发国际大厦 303 室
(邮编： 200082)

电话： 021-53391010
邮箱： info.china@omicronenergy.com

更多信息、 其他资料以及我们全球各地办公室的联系信息，请访问我们的网站。
For more information, additional literature, and detailed contact information of our worldwide offices please visit our website.

www.omicronenergy.com