IEC 62443工业安全标准

框架介绍

创享价值
激发信任

白皮书

摘要

互联技术的广泛部署已经改变了世界上许多行业的工业格局。今天所谓的智能工厂正在积极利用互联系统的潜力来简化生产、提高产量并减少浪费，同时也提高了生产的灵活性。

同时，工业环境中对互联技术的日益依赖使我们更容易受到网络安全的威胁。从窃取专有技术知识到工厂停工的威胁，甚至是关键工业资产的损害和破坏。工业运营中的网络攻击风险非常令人担忧，它可以造成巨大的经济损失，甚至危及生命。因此，采取行动加强工业网络安全比以往更加重要。

在本白皮书中，我们将讨论工业4.0所体现的创新工业技术，以及这些进步如何使它们反而更容易受到网络威胁。我们然后将介绍IEC 62443系列标准概况，并讨论这些标准中提出的工业网络安全框架的整体方法的优势。本文最后将介绍TÜV南德意志集团的工业网络安全方法以及TÜV南德意志集团IEC 62443认证的优点。

TÜV南德意志集团

TÜV®

目录

21世纪的工业革命 3

工业4.0和网络安全的挑战 3

IEC 62443系列标准概述 5

IEC 62443系列的主要文件 7

TÜV 南德意志集团对IEC 62443框架的处理方法 9

与TÜV 南德意志集团合作的优势 10

TÜV 南德意志集团专家介绍

Markus Müller （马库斯•穆勒）
工业安全团队负责人
TÜV 南德意志集团产品服务部（德国）

Markus Müller是德国慕尼黑TÜV南德意志集团工业安全服务的团队负责人，负责根据IEC 62443标准进行安全测试和认证。在2019年加入TÜV南德意志集团之前，Markus在西门子公司作为内部审核部门安全团队的一员，从事体系评估和审核，并进行黑客和渗透测试。Markus拥有慕尼黑大学（路德维希-马克西米利安-慕尼黑大学，LMU）的信息学学士学位，以及慕尼黑工业大学和俄罗斯托木斯克理工大学的信息学硕士学位。可与Markus取得联系：m.mueller@tuvsud.com。

21世纪的工业革命

在过去的300年里，不断采用新兴技术和其他创新是几乎所有行业的生产式系统和流程的一个决定性方面。从18世纪初最早使用蒸汽和水为机械设备提供动力，到19世纪末引入工业装配线，最后到20世纪60年代末开发基于可编程逻辑控制器（PLC）的“智能”设备，各行业一直在寻求新的方法，以利用先进技术来简化生产及流程，并更好地满足不断增长的全球市场的各种要求。

工业创新工作在过去十年主要集中在如何扩展先前的自动化成功经验。利用数字技术和新开发的信息通信技术（ICT）解决方案，21世纪上半叶的先进工业活动正在充分利用工业物联网（IIoT）的力量。在此大环境下，生产或流程链的各个环节相互无缝连接，网络物理系统（CPS）实时监测工业环境中的活动，并不断与其他CPS以及操作员进行交流。

因此，工业4.0技术和体系的采用使高需求产品的制造商能够迅速扩大生产能力，同时使其他生产商能够更广泛地提供定制产品。它还有助于改善基于流程的行业，如食品生产以及化工或药品制造，从而对资产和供应链活动进行更有效的管理和监督。最后，工业4.0模式的优点有助于支持和维护关键工业部门的基本运作，如医疗保健和能源。

工业4.0和网络安全的挑战

工业4.0技术的应用增加了对网络威胁的潜在风险。最广为人知的网络威胁是那些来自外部的威胁，它们试图以勒索赎金或其他财务支付作为消除或消灭威胁的代价。但是，网络威胁也可以来自内部，比如说来自一个疏忽大意或心怀不满的员工。还有一些意外的网络风险，如没有正确地保护系统登录和密码，或打开来自看似可信来源的电子邮件。

以下只是过去十年间发生的针对工业运营网络攻击的一些事例：

- **伊朗核电站（2010年）——**一个含有Stuxnet病毒的较早版本的USB闪存盘被引入伊朗纳坦兹核电站的计算机网络。该恶意软件随后攻击了用于控制该厂铀离心机运行的软件，影响了该国大约20%的铀浓缩能力。[1]
- **德国钢铁厂（2014年）——**据报道，黑客利用鱼叉式钓鱼邮件进入德国一家钢铁厂的网络，然后便进入该厂的生产网络并获得对工厂基本设备的控制。工厂操作人员无法关闭工厂的一座高炉，该钢厂遭受了重大损失。[2]

- **乌克兰电网（2015年）——**由于一次协同网络攻击，乌克兰的三个地区的电力公司基本上被切断了电源，导致数十万人无电可用。据报道，这次攻击涉及使用BlackEnergy（BE）恶意软件，黑客用它来控制发电厂的断路器系统。[3]

- **沙特阿拉伯石油化工厂（2017年）——**沙特阿拉伯一家石油化工厂的计算机系统被黑客入侵，导致被植入了Triton恶意软件。黑客然后操纵了工厂紧急关闭系统的可编程储存器。据报道，这次黑客攻击的目的是为了引发爆炸，但由于攻击者的计算机代码中有一个错误而失败。[4]

- **台湾半导体工厂（2018年）——**WannaCry勒索软件的一个变种被第三方供应商意外引入台湾一家半导体制造商的计算机系统中。据报道，该勒索软件扩散到该公司几个最先进的生产设施中的10,000多台不同的机器上，导致这些设施关闭，估计损失超过2.5亿美元。[5]

展望未来，许多专家预测工业网络安全工作的环境将更具挑战性。诸如5G无线通信的部署以及对人工智能和机器学习使用的更多依赖将推动工业4.0技术部署的增长。但这些进步也使保持领先于威胁曲线的努力变得更加复杂。

此外，虽然许多组织为解决针对信息通信技术（ICT）系统的网络威胁做了很充分的工作，但针对运营技术（OT）的威胁管理问题最近才得到重视。因此，处理工业运营中使用的技术和系统安全的内部政策和程序的实施往往落后于组织的其他网络安全工作。一些专家称工厂和工业设施的领导人存在“网络安全意识差距”是造成这种鸿沟的原因，在此背景下，有关网络威胁潜力的相关信息仍然被忽视或被误解。[6]

最后，针对具有开发和实施有效网络安全防御措施所需经验的专业人员，是供不应求的。根据网络安全专业人员组织（ISC）[2]在2019年的一项研究，填补目前全球网络安全技能的差距将需要超过400万人接受当前网络安全实践和程序的培训，比目前的人员配备水平增加145%。[7]这意味着许多组织可能会很难寻求到能解决未来未知的工业网络安全威胁所需的技能和经验。

IEC 62443系列标准概述

上一节中提到的挑战表明，需要采取不同的方法来解决工业自动化和控制系统（IACS）特定的网络安全要求。然而，目前用于评估网络安全的许多标准和方法针对IACS应用时都存在局限性。

例如，ISO 27000系列为信息安全管理系统（ISMS）的发展提供了一个稳健的结构。因此，该标准主要侧重于IT运营。另一个标准，ISO/IEC 15408-1（也通常被称为“通用标准”），主要应用于政府的采购工作中。该标准也几乎仅关注产品本身，不能用于复杂的系统评估。

IEC 62443《工业通信网络-网络和系统安全》，是一系列国际公认的标准、技术报告和技术规范，为评估和减轻工业控制系统各方面的当前和未来的网络安全风险提供了一个系统的方法。部分基于一些不同国家网络安全标准中的原则，IEC 62443系列提供了一个清晰而灵活的框架，同样适用于不同行业的离散型和流程型制造的环境。

IEC 62443系列由14个独立的部分组成（截至2020年9月），详细说明了整个供应链中涉及开发、部署、使用或维护工业控制系统和组件的各个参与者（“角色”）的特定网络安全责任。这些角色包括：

- **资产所有者 ——**负责一个或多个IACS的个人或组织；
- **产品供应商——**集成到IACS的硬件或软件组件的制造商或开发商；
- **服务提供商——**为工业控制系统或组件向资产所有者提供支持服务或供应的个人或组织。服务提供商包括：
  - **集成服务提供商——为工业控制系统或组件提供集成服务的服务提供商；**
  - **维护服务提提供商——工业控制系统或组件安装后，为其提供支持活动的服务提供商**

IEC 62443系列中提出的具体要求也同样重视人、流程和技术在确保工业环境中的网络安全方面的作用。

为此，该系列的各份文件均属于以下四个类别之一：

- **通用——**构成“通用”类别（IEC 62443-1-x）的部分包括四份单独的文件，提供了网络安全过程的一般概述，并介绍了关键的概念、模型和定义。
- **政策和程序——**“政策和程序”类别的五份文件（IEC 62443-2-x）详细规定了IACS安全管理系统的要求，以及对资产所有者和服务提供商（包括系统集成商和产品供应商）的安全程序（SP）要求。
- **系统——**该系列的“系统”类别（IEC 62443- 3-x）的三份文件提供了系统安全要求、安全等级和安全风险管理以及系统设计的基本指导。
- **组件——**最后一个类别“组件”（IEC 62443-4-x），包括两份文件，一个是详细规定系统组件的技术安全要求，另一个是规定安全产品开发生命周期要求。

IEC 62443定义了工业安全的整体方法

IEC 62443系列提出的整体方法为寻求充分利用工业4.0技术潜力的工业组织提供了一个强大而全面的网络安全解决方案，同时将其风险降至最低。

IEC 62443系列的主要文件

在IEC 62443系列的14份独立文件中，有6份的网络安全要求为寻求保护其自动化控制系统免受网络威胁的工业组织提供了一个很好的起点。以下是对这些文件的重点摘要。

01 IEC 62443-2-1 第二版, 建立工业自动化和控制系统安全程序

IEC 62443-2-1规定了对IACS资产所有者的要求。安全程序必须定义适用于IACS安全操作的安全功能。这些安全功能的实施通常需要服务和产品供应商的支持，然而，资产所有者仍然对安全负责。

02 IEC 62443-2-4，IACS服务提供商的安全程序要求

该IEC 62443标准为集成或维护IACS相关的所有类型的服务提供商详细规定了一套全面的安全能力要求。由于这些要求大多与领域相关，该标准提供了“配置文件”的开发，可用于解决特定环境的独特特征。

03 IEC 62443-3-2, 系统设计的安全风险评估

该标准规定了定义IACS系统的要求，将考虑中的系统（SUC）划分为区域和管道，评估每个区域和管道的风险，并建立其各自的目标安全等级。

04 IEC 62443-3-3, 系统安全要求和安全等级

IEC 62443-3-3定义了适用于自动化系统和网络的系统安全要求。安全要求是基于IEC 62443-1-1中定义的七个基本要求（FR 1-7），包括 1）标识和鉴别控制；2）使用控制；3）系统完整性；4）数据保密性；5）受限的数据流；6）对事件的及时响应；7）资源可用性。IEC 62443-3-3中提到的安全等级（SLs）是基于IEC 62443-3-2中提出的自动化系统和网络的风险分类。

05 IEC 62443-4-1，安全产品的开发生命周期要求

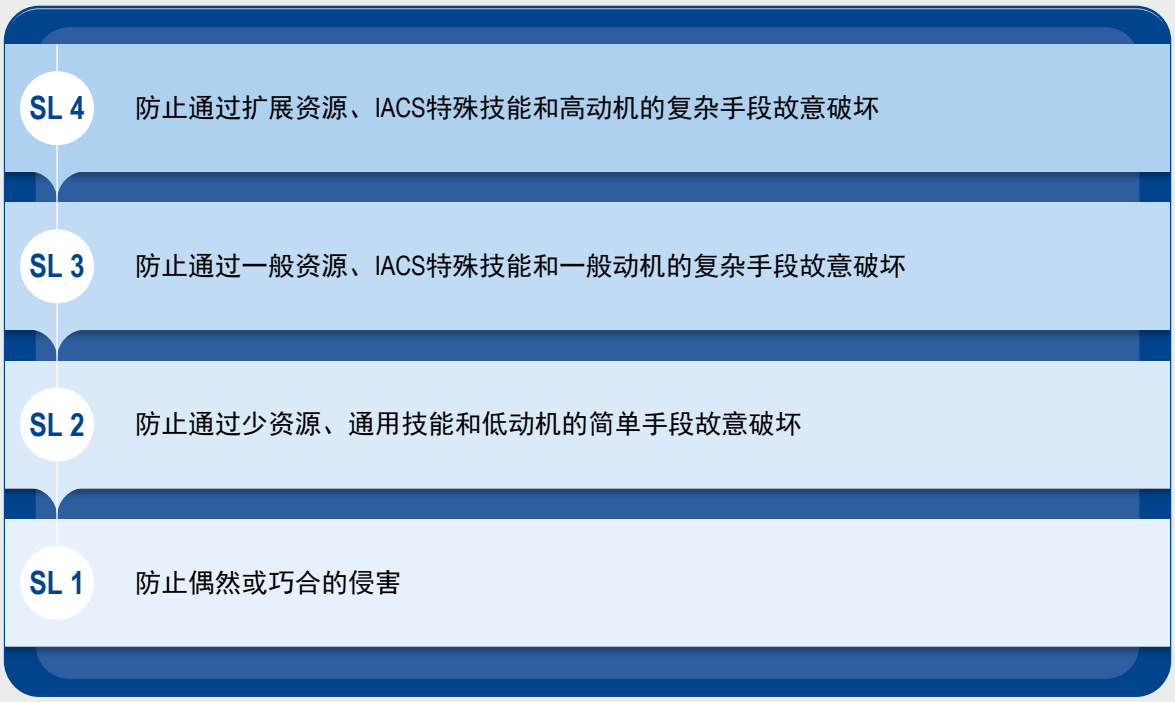
该IEC 62443标准描述了与工业自动化和控制系统环境中使用的产品的网络安全有关的产品开发生命周期要求。该标准中涉及的产品生命周期的具体方面包括安全要求定义、安全设计、安全实施、验证和确认、缺陷管理、补丁管理和产品报废的注意事项。

06 IEC 62443-4-2, IACS组件的技术安全要求

IEC 62443-4-2将IEC 62443-3-3中提出的安全要求和安全等级应用于构成IACS的组件，如嵌入式设备、网络组件、主机组件和软件应用程序。该标准的目的是规定组件的安全功能，以减轻特定安全级别的威胁，而不采取补偿性的对策。

对于IACS资产所有者来说，这六个标准涵盖了IACS实施和运行的全部范围，包括产品供应商、集成服务和维护服务提供商的活动。因此，它们为有效的IACS网络安全管理系统提供了基础，同时也为识别未来的漏洞和实施必要的安全改进提供了途径。

技术评估-安全等级



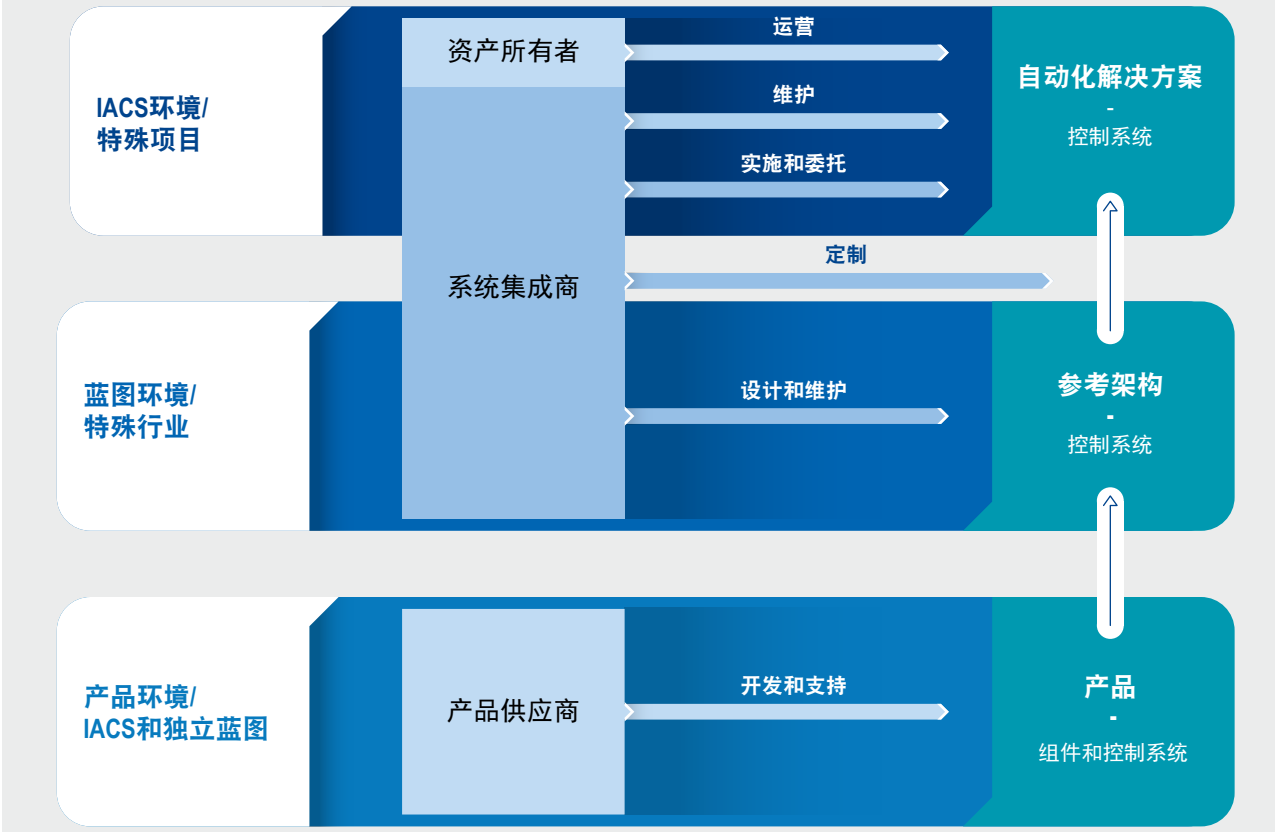
TÜV 南德意志集团对IEC 62443框架的处理方法

对于一个或多个IEC 62443标准的认证可以作为组织将网络威胁的潜在风险降到最低的整体战略中的重要一步。对于资产所有者和运营商来说，IEC 62443认证提供了符合工业网络安全要求的保证，并证明了组织对其产品的安全性和完整性的承诺。对于供应商和集成商来说，认证可以帮助满足运营商对IACS相关产品和服务的采购要求，同时也为其产品的安全性提供客观保证。

TÜV 南德意志集团采用了一种全面的认证方法，该方法反映了IEC 62443框架，并完全涵盖了适用于IACS供应链中每个参与者的独特安全要求，包括供应商、集成商和运营商。

IEC 62443认证提供了符合工业网络安全要求的保证，并证明了组织对其产品的安全性和完整性的承诺。

IEC 62443框架



对于供应商来说，TÜV 南德意志集团根据IEC 62443- 4-1的要求提供流程认证，该要求涉及产品开发生命周期的安全性，是IEC 62443系列中特殊产品标准认证的先决条件。以此为基础，供应商就可以寻求IEC 62443- 4-2的产品认证，该标准涵盖了IACS组件的技术安全要求，以及IEC 62443-3-3，其概述了自动化和控制系统的安全要求。

对于集成商，TÜV南德意志集团提供符合IEC 62443-2-4要求的流程认证，该要求涉及所有类型的IACS服务提供商的安全程序功能要求。与其他认证机构不同的是，TÜV南德意志集团还根据IEC 62443-2-4和IEC 62443-3-3的要求，为集成服务提供商提供蓝图（即提供商特殊的解决方案架构）认证。蓝图认证为系统集成商提供了一个经过验证的安全架构，可以为未来安全自动化解决方案的开发进行定制。

最后，对于资产所有者和运营商，TÜV南德意志集团提供IEC 62443-2-1第二版（CDV 2019）的最新要求的认证，该要求定义了IACS的网络安全管理系统要求。此外，TÜV 南德意志集团还可提供ISO 27001认证。

TÜV 南德意志集团的IEC 62443认证仅在产品或流程接受涵盖适用标准中所有详细要求的评估的情况下才能获得。我们的认证还包括对IEC 62443认证的流程和产品进行年度监测。我们的认证框架的这些额外方面旨在验证是否继续符合认证要求，以及认证的IACS产品和系统的不间断安全性。

与TÜV 南德意志集团合作的优势

TÜV 南德意志集团一直积极参与适用于部署和使用IACS的网络安全框架的开发。我们的工业网络安全专家参与了关键的标准制定活动，包括IEC 62443系列中的大部分单独标准，并继续从事于与工业网络安全相关的持续监管和标准制定活动。

除了IEC 62443认证之外，我们的服务还包括准备一份全面的差距分析，可以作为希望实施IEC 62443框架的公司的路线图。我们还提供工业网络安全研讨会，以提高对标准的理解，并提供定制化的培训，以进一步探讨特殊要求或情况。

因此，我们有独特优势，可以帮助组织全面了解IEC 62443的要求以及未来的监管制定。反过来说，我们的客户能够设计和实施高效的工业安全系统，以满足认证的要求，同时也肯定了组织对安全的坚定承诺。

脚注

[1] “Stuxnet worm hits Iran nuclear plant staff computers,” BBC新闻, 2010年9月26日. 可见 https://www.bbc.com/news/world-middle-east-11414483（截至2020年7月20日）。

[2] “A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever,” 《连线》杂志，2015年1月8日。可见https://www.wired.com/2015/01/german-steel-mill-hack-destruction/ （截至2020年7月20日）。

[3] “Alert (IR-ALERT-H-16-056-01): Cyber-Attack Against Ukrainian Critical Infrastructure,” 由美国国土安全部工业控制系统网络应急响应小组（ICS-CERT）发布，2016年2月25日。可见 https://ics- cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01 (截至2020年7月20日)。

[4] “A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try,” 《纽约时报》，2018年3月15日。可见https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html (截至2020年7月20日)。

[5] “TSMC Chip Maker Blames WannaCry Malware for Production Halt,” 发布在《黑客新闻》网站，2018年8月7日。可见https://thehackernews.com/2018/08/tsmc-wannacry-ransomware-attack.html(截至2020年7月20日)。

[6] “Overcoming Cyber-Apathy”，ARC咨询小组网站的博客文章，2020年2月28日。可见https://www.arcweb.com/blog/industrial- cybersecurity-imperative（截至2020年7月20日）。

[7] “(ISC)² Finds the Cybersecurity Workforce Needs to Grow 145% to Close Skills Gap and Better Defend Organizations Worldwide,” 发布在(ISC)2的网站，2019年11月6日。可见https://www.isc2.org/News-and-Events/Press-Room/Posts/2019/11/06/ISC2-Finds-the-Cybersecurity-Workforce-Needs-to-Grow--145 （截至2020年7月20日）。

Greater China

联系我们，了解更多信息

https://www.tuvsud.cn/zh-cn/industries/manufacturing/machinery-and-robotics/iec-62443-industrial-security

info.cn@tuvsud.com

创享价值，激发信任

作为一家安全、可靠和可持续发展解决方案等方面值得信赖的合作伙伴，TÜV南德意志集团提供测试、认证、审核及知识服务。自1866年以来，集团始终致力于通过保护人类、环境和资产免受相关技术风险的影响。公司在全球设立了1,000多个分支机构，并拥有超过25,000名员工，通过实现市场准入和控制风险，TÜV南德意志集团激发对现实和数字世界的信任，以创造更安全、更可持续发展的未来。

我们在大中华区的分支机构：

TÜV南德意志大中华集团
总部 上海
上海市恒通路151号3-13层 200070
电话：+86 021 6141 0123

上海测试中心
电话：+86 021 6037 6300
电话：+86 021 6037 9100

无锡
电话：+86 510 8820 3737

宁波
电话：+86 574 2786 6658

金华
电话：+86 579 8288 8708

南京
电话：+86 025 8779 0058

合肥
电话：+86 551 6537 8730

台州
电话：+86 576 8966 1886

苏州
电话：+86 512 6809 5318

成都
电话：+86 028 8592 0656

杭州
电话：+86 571 8111 0758

常州电池实验室
电话：+86 519 8109 8308

常州轨道实验室
电话：+86 519 8123 9872

武汉
电话：+86 027 8571 4927

郑州
电话：+86 371 5538 2208

重庆
电话：+86 023 8980 9513

北京
电话：+86 010 6590 6186

天津
电话：+86 022 8319 2258

青岛
电话：+86 532 8503 0106

青岛实验室
电话：+86 532 8513 1716

大连
电话：+86 411 8230 4203

沈阳
电话：+86 024 8668 5949

长春
电话：+86 431 8462 9833

香港
电话：+852 2776 1323

香港元朗实验室
电话：+852 2443 3774

深圳
电话：+86 755 8828 6998

深圳观澜实验室
电话：+86 755 3359 5385

广州
电话：+86 020 3832 0668

广州测试中心
电话：+86 020 3817 0580

厦门实验室
电话：+86 592 7706 188

厦门思明区办公室
电话：+86 592 7311 931

东莞
电话：+86 769 2168 7092

长沙
电话：+86 731 8458 5815

柳州
电话：+86 772 3858 696

台北
电话：+886 2 2898 6818

台中
电话：+886 4 2486 3966

*上述部分服务可能由于当地法规的原因而无法在您的地区提供。欢迎您与我们联系咨询。