UPDATE

菲尼克斯电气

工业安全专刊

网络卫士

工业网络的信息安全“防疫战”

IRMA在放哨

数据安全

MNR 110462 6/2020-01-31/00

SECURITY

phoenixcontact.com.cn

与安全相关的数字

270万
瑞典医疗咨询电
话信息泄露

14,000
新加坡卫生部艾滋病
登记处泄露的数据

Functional safety

1250万
一家印度政府医疗机构服
务器泄露孕妇有关的数据

100
Facebook约100名开发者被允许
访问不该访问的个人数据资料

Cybercrime

2900万美元
Nikkei黑客欺骗将2900万美元
转移到一个银行账户

175天数
平均来说，一次袭击保
持不被发现的时间

40,000
汉堡王近40000份
客户记录被公开

2016年以十亿欧元计的亏损

德国 **55**

世界范围 **432**

500万
近500万DoorDash
用户在数据泄露
中受到影响

1 网络攻击每隔
一段时间发生
3分钟
在德国 (2018年)

数据盗窃
指德国公司注册的
网络钓鱼攻击 (2018年)

48%
电子邮件客户数据

21%
客户数据

20%
财务数据

赵春风先生
经理_IMA Marketing

工业控制系统的功能安全

长久以来，工业生产，不论是离散的还是连续的，工业控制系统一直都关注功能安全（Safety）。为了保护生产设备和操作人员的安全、降低安全风险、提高安全意识、减少财产和生命的损失，安全标准、技术、产品和系统不断地更新和完善，因为这些损失是有形且易见的，所以被给予了更多的关注。

随着工业实时以太网技术的日趋成熟和大量应用，工业控制系统也越来也网络化。工业4.0、工业物联网、人工智能、大数据、云、5G等新技术、新概念的诞生和应用，推动了工业控制系统的互联互通性进一步加强和升级。数以亿计的设备和人连接起来，形成了一个网络化的世界，大量的数据在其间穿梭，网络和信息的安全风险也随之增加。

工业控制系统的网络和信息威胁来自各个层面和各个方面，例如：办公网络、移动设备、外部远程接入、病毒、恶意软件以及黑客攻击等等。这些风险造成的破坏有时候是很巨大的，影响是深远的，例如：知识产权、生产信息等数据丢失或泄露、生产设备的停机从而导致客户订单的交付延期、公司形象受损、甚至人身伤害等等。

网络和信息安全的威胁无时无刻，无处不存在，遭受到攻击不代表工作没有做好，没有做好防御工作那才是真正的威胁。应对网络和信息安全，最重要和最根本的是加强、提高人的意识，包括管理者和操作人员，其次才是系统规划、风险评估、实施等各个环节的细致工作和闭环递进。

总部位于德国柏林的菲尼克斯信息安全公司，前身为成立于2001年的Innominate公司，一直专注于工业控制系统的网络和信息安全，旗下的mGuard系列产品，在为工业网络提供了坚固的防火墙同时，也可为信息的安全传输搭建私密的VPN通道。

菲尼克斯电气是为数不多首批获得TUV颁发IEC62443认证的企业，在安全软件，安全系统和服务、安全产品研发和生产等多层面获得认证。mGuard和PLCnext控制器的总体设计及开发过程严格遵循此标准。

从网络和信息安全培训，到安全系统的规划、风险评估和实施多个角度，菲尼克斯电气为客户提供完整且完善的产品、系统和服务。网络基础设施的防浪涌保护，网络防火墙mGuard，内置信息安全防护的PLCnext控制器，为保障用户的网络和信息安全，菲尼克斯电气给出了系统化的解决方案，做到软硬兼施，防治并举。

一旦创建了安全防御，
就能永保安全了吗？

8

工业安全

我们监视的不是
通讯的内容，
而是数据流量

14

与疫魔竞速，菲尼
克斯电气鼎力驰
援“雷神山”！

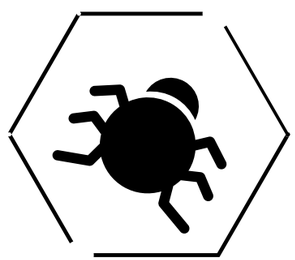
37

工业网络的信息
安全“防疫战”

34

网络卫士

9



最著名的网络攻击

21

20亿台设备受
到漏洞威胁

32

各行各业的视频盒

28

锂离子电池的艰难之旅

22

SEC
URI
TY

网络卫士

Lutz Jänicke博士在菲尼克斯电气负责安全产品和解决方案。我们就网络安全相关问题对他进行了专访。

Lutz Jänicke博士实际是一名电气工程师。但在攻读博士学位以及毕业后从事研究工作时，他偶然关注了这个话题并产生了兴趣。他是菲尼克斯电气接触系统性网络安全保护的第一人，目前已经成为国际知名的数据安全专家。此次采访在巴德皮尔蒙特的一个古堡中进行。

➔ 您好，Lutz博士，我们今天在这里安全吗？

现在应该是安全的。但在过去古堡是如何被攻破的呢？ 攻城者往往在放火后发起猛攻，甚至会挖掘地道推倒城墙。换句话说，人们通过寻找古堡的弱点来攻城掠地。在这一点上，今天和一千年前并没有什么不同。

安全从来都不是简单的技术问题，而是一个持续的过程。在这一点上自古到今都是如此。

➔ 一旦创建了安全防御，就能确保永远安全了吗？

不，这是一个持续的过程。

您必须事先考虑如何组织防御，以便为多种可能性做好准备。然后，防御措施要走在攻城措施的前面。在中世纪，我们可以花很多年来做这件事，但现在我们必须快速行动。

错误通常发生在传统的分工合作中。在项目协同时，您同样依赖于同事的出色表现。一个同事的错误可能会引起一系列的连锁反应。“四眼原则”则可以帮助我们有效规避这方面的问题。与传统的城堡建筑一样，防御概念从一开始就需要到位。这就是所谓的设计安全性。

这是项劳动密集型的工作，让有创造力的人恼火不已，而且价格昂贵。最后，您得到的产品看上去与不安全的产品也没有什么不同，但价格却更高。从这一点出发去说服不重视设计安全的人，真是不太容易。庆幸的是，立法机关正在进行相关立法，这有助于实现关键基础设施的网络安全性。另外一旦生产停机，很快就会导致几百万欧元的损失，甚至可能由于无法正常交付导致大量客户流失而造成公司倒闭。如果不在设计安全性上投资，实际上就是把钱省在了不该节省的地方。

➔ 整体威胁是否在增加?

这是肯定的。我们这个行业的统计数据很难获得，但向FBI报告的美国网络安全事件造成的损失在过去十年中增长了十倍。从2008年到2018年，损失从2亿美元增长到20亿美元。 这些都是绝对真实的数据。

➔ 谁是背后的坏人？他们的动机是什么?

往往存在着各种各样不同的攻击者。如果是个人发动的攻击，那么造成的损害通常不太大。个人黑客可能是出于无政府的动机，也可能是出于非常现实的经济原因。他们会使用可以购买到的恶意软件，这些恶意软件对各种App的攻击司空见怪。

其次是由商业机构组织的付费购买的高级黑客攻击，在俄罗斯就存在专门组织这类犯罪的机构。

还有国家行为体参与的此类行为。您可以通过读取服务器活动的时间戳来了解被指控的人员。令人震惊的是，你经常会在一个非常特定的时区找到匹配的时间。即使是网络黑客也有固定的办公时间。

➔ 当你自己是一个“好人”时，你如何训练你的网络防御能力？如果您自己不是攻击者，如何获得所需的黑客工具?

建议不要登录一些非常小众的网站。可以下载国安局不定期发布的黑客工具，也可花少量的费用去购买。这些工具可用于实验室环境，但请不要用于恶意攻击。

但您也需要真实的环境来测试您的工具，并对可能出现的攻击采取防御措施。如果让这样的工具出没在我们的网络系统种，我们的网络会发生我们无法控制的事情。所以我们必须很小心。我们实验的网络必须能够承受得住实验所造成的各种后果。

➔ 我们生活在一个日益网络化的世界。但我们只有在经历了惨痛教训后才会考虑安全问题。这是事实吗?

很多规模较小的公司确实是这样的。规模较大的公司通常要谨慎得多。例如，菲尼克斯电气的IT部门对可能发生的网络袭击总是保持警觉。我们的办公网络一直处于安全监督下。

➔ 是什么让菲尼克斯电气开始考虑此类安全问题?

2002年，我们在柏林创办了一家名为Innominate的公司。这家公司创立伊始是从事移动防火墙业务，但很快就进入了工业自动化领域。菲尼克斯电气于2008年接管了In-nominate公司。

然而，菲尼克斯电气不能仅仅依靠防火墙；我们还需要在考虑如何确保所有过程数据的安全性。我的工作职责是在一定程度上实现安全问题的大众化。我们制定培训计划指导人们操作并开发相关工具。 每个软件开发人员都必须面对安全问题，并遵循一定的指导原则。

➔ 网络安全如何实现与传统产业和传统信息技术的协调统一?

它们实际上协调的很好。我们都是某些专业领域的专家。IT领域需要我们这样的人。

但在生产领域往往大相径庭。通常没有人负责安全。设备启用后，没有人考虑如何将其安全集成到网络中。生产人员往往在意的是设备有没有连接到控制器。因此，要实现生产网络的安全，还有很多额外的“幕后操作”要做。

但在财务控制中，我们通常仅将网络安全问题视为成本因素。这样考虑也不无道理。我们偶尔会因安全问题遭受非常大的损失。因此，每个人都认为网络安全问题不会影响他们公司的运营。

➔ 在网络安全方面，菲尼克斯电气在哪些领域积极活跃?

我们积极改善自己公司和客户公司的网络安全性。这对我们业务的发展很有帮助，因为这也增加了我们对生产领域问题的理解。而且我们新通过的TÜV

认证表明，我们可以胜任规划和提供包括盘点、安装、调试和培训在内的所有流程的工作。

我们刚刚完成并成功通过了TÜV Süd的一个非常复杂的多阶段认证流程。由此可见，我们是多么认真地对待这件事。

➔ 在你看来，当涉及到安全问题时，公司的未来会是怎样的?

原则上，可以认为大规模增长的威胁会使管理承受压力。在供应链中，由于安全性日益成为供应商评估中的一个方面，客户给供应链带来了更大的压力。在立法上，制定新的规则也是不可避免的。

➔ 现在我们来谈论下开放与隐私的问题。当涉及到网络攻击时，网络保护行业本身是不是在夸大隐私权?

这是一个文化问题。诚然，就已经发生的威胁和攻击进行信息分享对每个人都很重要。尚未在证交所上市的公司也已经就这些进行了相当公开的交流。隐瞒绝对是有害的。

但是，如果德国一家上市公司坦言他们遭受了一次严重的网络安全攻击，其股票价值会下跌。但即使这样，人们思考的方式也在慢慢改变。每个人都有可能受到攻击。这不是软弱的表现。只有那些不作为的人，才真的有过失。而那些声称自己没有受到攻击的人可能只是没有注意到被攻击而已。

➔ 这也适用于菲尼克斯电气吗?

当然了。如果我们在市场上占有重要地位，如果没有为此作出充分的准备，那便是我们的错误。我们不断地在日常的防御战斗中进行自我教育，所以我们是在为自己和我们的客户进行训练。 ■

phoenixcontact.de/services

“被攻击并不意味着你做得不好。但是不把它们阻挡在外则意味着你的工作做得不够。”

Lutz Jänicke博士

“菲”凡云时代
护驾有我在！

2020年伊始，一场新冠肺炎疫情打破了工作的常规，全民复工掀起在线办公热潮。

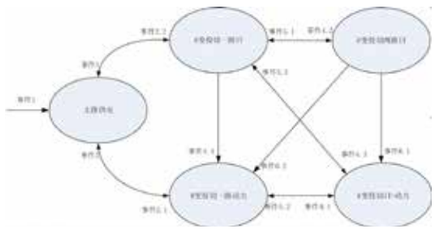
不能面对面的交流，可以开个云会议、做个云存储、来个云协作，云供应商为各行各业的用户，提供了云主机、云托管、云存储等基础云服务，以及超算、内容分发与加速、企业IT、云会议等方面的服务和解决方案。

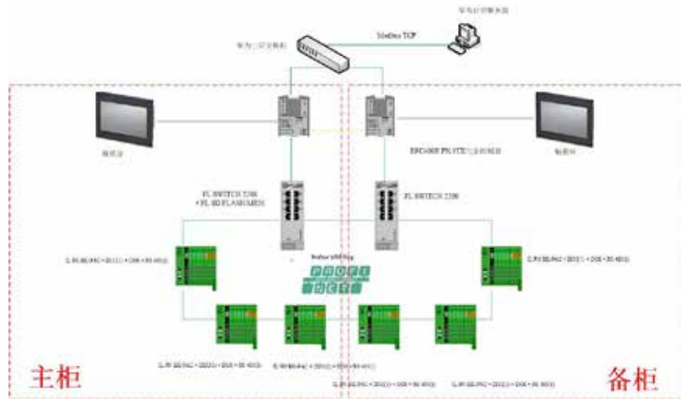
每天华为云上都有亿万条数据信息不停地被传递，保障这么庞大的用户群体的使用，必须要求华为云数据中心的硬件设备稳定运行。

作为自动化系统整体解决方案提供商，菲尼克斯电气为华为数据中心低压配电系统的可靠监控提供全新的基于工业以太网PROFINET冗余系统解决方案，确保整个供电系统可靠稳定运行！

数据中心用电设备种类多，且大部分为一级负荷中的特别重要负荷。为了保证供电的连续性，在华为云数据中心项目中设置一台动力变压器、多台IT变压器和一台R变压器（即：N+R架构），而供电回路采用“两路市电 + 柴油发电机”的方式。整个监控系统要求采用可靠稳定的冗余控制器对各个

安全系统





线路上的变压器、设备和负载进行实时监控，遇到供电异常的情况，根据预设的设备优选权和实际各个回路的用电负载进行自动投切，以确保主设备供电安全。同时，均衡其他用电设备负载，以减少业务影响范围。

分布式冗余控制器解决方案

针对华为的具体技术要求，菲尼克斯电气分别从简洁、高效、可靠三个维度考虑，突破了传统总线式控制方案，制定基于工业实时以太网PROFINET的分布式冗余控制器解决方案。

整个解决方案贯穿了华为云数据中心，设计标准严格遵循高可靠性、模块化、高品质、绿色环保的建设理念，采用菲尼克斯电气高可靠性冗余控制器RFC460R PN 3TX和IL系列Profinet远程IO。两个控制器为了确保其独立稳定运行，分别安装在不同的独立控制柜内，任意一个CPU或者控制柜故障，另一个控制柜能够无缝接管整个监控系统，以确保系统安全可靠。两个主控制柜通过交换机连接不同楼层的远程控制柜，通过MRP环网方式确保控制器和IO站点之间的通讯冗余。

远程控制柜一共有6个，分布在各个楼层的现场控制柜内。这些远程站都采用菲尼克斯电气经典Inline系列产品，本体自带2个网口，支持工业实时以太网PROFINET协议。模块化的设计能够更加灵活的配置接入的信号数量和类型，同时也不受到底板槽位的限制。单个耦合器能够携带多达63个扩展模块，满足各种现场设备接入的需求。超强的电磁抗干扰能和-20~60℃的宽温设计，以及弹簧式信号连接方式，能够更稳定可靠的运行在现场环境中。

全系列的可视化解决方案

菲尼克斯电气提供全系列的可视化解决方案：全身IP67防护等级的面板式工控机到多点触控、超高精细度的触摸屏，从入门级可视化软件到SCADA系统软件Visu+，菲尼克斯都能够为客户提供高性价比的方案和专业的服务支持。该项目中采用了菲尼克斯BTP系列的触摸屏和Visu+ express软件，连接到冗余控制器RFC460R上，实时显示用电回路状态和现场各个设备状态，并记录和备份各种异常突发情况。

IT行业的控制思维一般都基于高级语言模式，菲尼克斯电气核心控制软件PCWorX符合标准的IEC61131-3的5种编程语言，能够满足各种行业和用户的应用需求。此次项目中，整体软件架构采用ST编写控制策略，FB进行封装，对象实例化调用的模块化架构方式，能够快速的完成控制部署，并有利于后期的扩展和维护。PCWorX的运行仿真功能，结合实际应用中的仿真程序，能够快速有效的模拟现场各种突发情况，在软件层面上就能实现控制逻辑模拟，提高现场调试的效率。

监控系统的主要特点：

1、采用高性能的冗余控制器，系统无缝切换，保证控制系统的高可靠性；

2、MRP环网架构保证通信网络的高可靠性；

3、基于PROFINET实时以太网保证系统实时性；

4、模块化设计、分布式安装，工厂预安装预调试，节省时间20%以上；

5、硬件自诊断功能，连续记录系统中存在的故障；

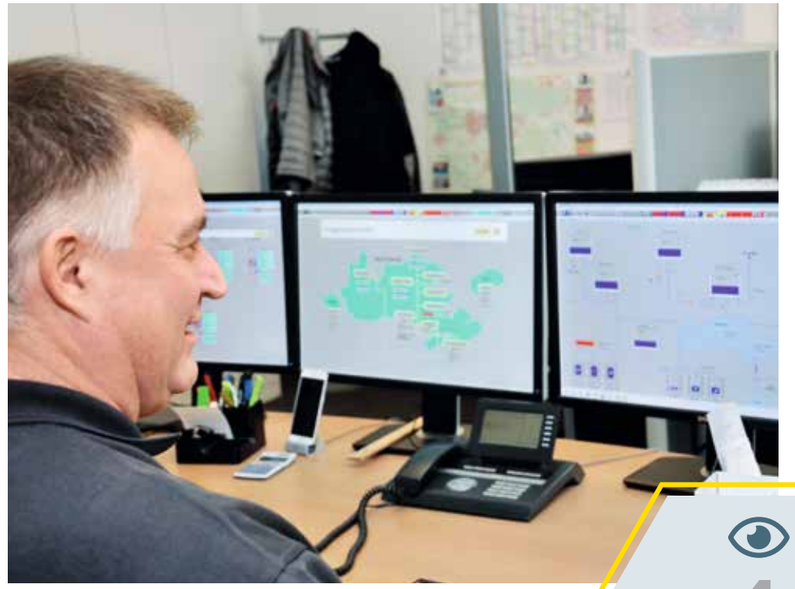
6、工业级产品，较强的抗干扰能力，具有很好的工业环境适应性；

7、基于数学建模的智能算法，面向对象的编程思路。

IRMA在放哨

系统发生异常时，IRMA会发出警报提醒我们。但是它始终在后台运行，对我们的系统活动不会产生任何影响。

两台水泵为水箱供水



在控制室中，Thorsten Hamann始终可以实时了解巴德皮尔蒙特的供能情况

4

控制室监控：
供气、供水、供电和
集中供暖情况

18,000

皮尔蒙特公共事业
公司供能地区服务
的居民数量

只有在征得同意的情况下，才可以走进Frank Jakob和Thorsten Hamann的工作区域：他们的帝国与巴特皮尔蒙特公共事业公司其他部门的办公区域之间隔着一道防盗门。这两人供职于公用事业公司的控制工程部门，负责检查供电、供水、废水处理和供气管网的信息，并在必要时启动修理或服务工作。这不是一个可以随心所欲进行参观的地方。“这正是我们安全概念第一阶段的内容。”

传统水疗度假村

控制工程部主管Frank Jakob说：“在这个控制室里，我们监控着这个都市大约18,000名居民的能源供应。”他说：“除了供电、供水和供气管网外，我们还监控着重要用户的集中供暖情况。 巴德皮尔蒙特是一个有着丰富传统的水疗小镇，拥有众多的公共设施和悠久的历史，如包括Steigenberger酒店、音乐厅和泵房的州立水疗中心。“

“用于监控供给的传感器几乎完全通过铜缆连接。”Thorsten Hamann解释说。“当然，我们也越来越依赖我们系统的数字化，以便更快、更可靠地采取行动。我们不仅安装了传感器，还组装了自己的控制柜，并对自己的控制系统进行编程，从而可在现场进行远程维护。” Hamann不仅需要熟悉供气、供水和供电领域的各种特殊问题，还负责IRMA监视。“作为能源供应商，我们必须满足对关键基础设施的要求。立法者要求我们采取特别严格的措施来保护和确保供能系统安全。”

这些措施由专家持续监控，他们会定期访问巴德皮尔蒙特公共设施并详细分析这些设施及其结构。我们将这些访问称为审核。如果供应商通过了该审核，则可将获得DIN 27001规定的继续运营所需的证书。“在上次审核期间，专家裁定我们的中央防火墙无法满足网络安全要求。” Frank Jakob告诉我们。

→

这个古老的基础设施极具迷惑性：这里面采用的是先进的控制技术

下图：
Frank Jakob
控制工程主管，
此处展示
IRMA的“家”

“你唯一一次注意到我们，就是发生了什么事但是我们却毫无办法。”

Thorsten Hamann,
Stadtwerke Bad Pyrmont

后台监控

“因此，现在迫切需要深入探讨这个问题。 这样，我们将来就可以在这里开展自己的管理工作。就在那时，我们想到了IRMA。”这个缩写是什么意思呢？菲尼克斯电气的安全专家HaukeKästing解释说：“IRMA代表工业风险管理自动化，它基于在菲尼克斯电气工控机上安装的经过案例检验的Linux应用程序。该系统在后台运行，并独立监视所有设施和通讯连接。”

我们监视的不是通信内容，而是数据流量。数据在巴德皮尔蒙特的公共事业网络中不断来回传输。控制系统发送测量值，智能电表报告功耗，传感器发送水位。这些数据通信首先由IRMA记录和“学习”。“这对我们来说是真正的工作。”Thorsten Hamann说。“我们必须‘教导’IRMA的各个通信合作伙伴，并对其进行注册。一旦IRMA足够智能，系统就会知道哪些活动是正常的。而且最重要的是，她会知道是否存在任何异常情况。比如：当控制器开始不仅与控制室进行通信，还与网络中的其他控制器进行通信。或网络实施不再试图与互联网建立连接。“异常时IRMA会发出警报提醒我们。但是IRMA始终在后台运行，这纯粹是一个监视系统，对我们的活动系统没有任何影响。”

便于了解我们的网络

对于Frank Jakob和他的同事来说，这是该系统的主要优势之一。而且，该系统还有一个非常令人愉快的附加作用，正如Thorsten Hamann所描述的那样：“有了IRMA，我们能以全新的方式了解自己的网络。IRMA向我们展示了实际上哪些设备之间在进行通信。有了这些知识，IRMA就会为我们构建一个不断更新的网络计划，这对于即将到来的新一轮认证很重要。而我们只需按一下按钮就可操作它。”

(lo) ■

网络攻击

公用设施大事记

十月
2019年
Langenfeld公共事业公司的网络遭受安全攻击

多于
150
2018年报告的针对关键基础设施的网络攻击

九月
2019年
斯图加特公用事业公司的网络收到安全攻击

2032年
德国将安装4000多万个智能电表网关

中心照片：
对一切了如指掌
的Thorsten
Hamann and Frank Jakob

这个水泵正在运行
而且可以对他进
行远程控制！

Martin Dickopp
和 Kilian Golm
当谈到数据安全时，
他们都神色严肃

数据安全

在数据安全方面，是时候采取行动了。位于柏林的菲尼克斯电气网络安全公司与每位黑客展开了“肉搏战”。今天，我们参观了这家公司。

菲尼克斯电气网络安全公司是一家初创公司。公司管理者年轻、大胆并渴望成功。尽管这家公司隶属于菲尼克斯电气集团，但却独立运营。当你敲开他们位于柏林-阿德勒肖夫的办公室的大门时，你马上就会意识到这一点。当然，你也可以按门铃。然后，你可以看见办公场所现代的外观，受到酷酷的接待。如果气场不合，一切就永远结束了。如果你想对他们进行深入了解，他们也会款待。

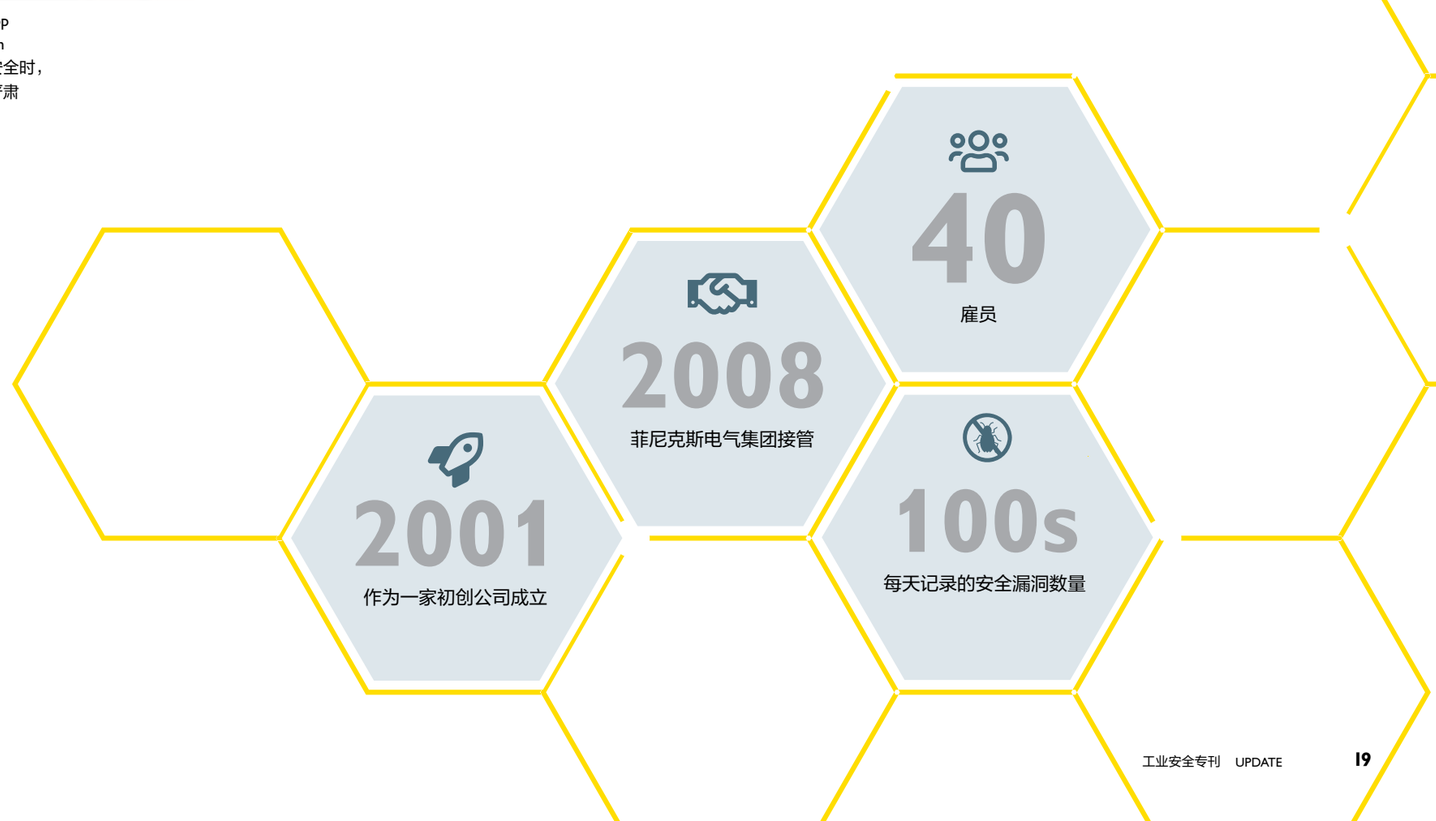
在Richard-Willstätter-Straße，事情不是那么简单随意。在数据安全和网络犯罪方面也不可以随意。“我们会密切关注最新发生的网络攻击事件。” Kilian Golm在谈话中告诉我们。最近遭受攻击的是一家数据安全领域的公司。这家总部位于柏林的菲尼克电气集团子公司的总经理强调：“这件事清楚地告诉我们网络犯罪现在有多么普遍和严重。”

用m来突破

这家总部位于柏林的公司成立于2001年，是一家典型的初创公司，成立伊始只有4名员工，从一开始就位于阿德勒肖夫的创新基地。公司创立之初聚焦在如何实现商务旅行者的数据安全。但很快，这些创业人就找到了发展的方向，把注意力集中在了工业网络通信领域。总经理Kilian Golm说：“我们开发工业安全系统的时候，其他人都还没有注意到这个领域。这个业务为我们带来了很多客户，其中一些关系至今依然存在。信任是安全行业发展的一大因素。”

Martin Dickopp从公司创业伊始就在这里工作：“我们成功的基础之一是mGuard产品和解决方案的开发。”这位安全专家解释道，“这些软硬组件实际上就是一个移动防火墙。m就代表移动。但是，这些设备不会对系统进行干预，而是作为后台的隐形设备来监控系统安全。换句话说，我们总是在隐形模式下行动。”

这个想法取得了成功，这项技术被注册为专利，公司曾经



工作圈

每个软件都有安全漏洞。鉴于当今系统的复杂性，这已无法避免。一旦发现软件的漏洞，尽快采取弥补措施至关重要。我们自己的产品安全事件响应团队（简称PSIRT）就专门负责为mGuard系列软件弥补漏洞。这支响应快速的团队每天都在筛选并分析可能存在的安全漏洞。或许您认为这种工作十分无聊，但是如果您知道他们每天都会发现并记录成百上千个安全漏洞就不会这么认为了！

在过滤掉涉及自己产品的消息后，专家们会分析这种漏洞可能带来的影响，有时甚至分析到源代码级别。如果该消息被确定为严重威胁，则会给出最高优先级，并会尽一切努力立即纠正这种情况。

而如果威胁不是非常紧迫，比如说，如果众多安全墙中只有一个倒塌。那么将在下一次定期更新中打安全补丁。“在后台进行的这项工作可以确保我们安全管理工作的质量。”Martin Dickopp解释说，“我们一直在后台尽忠职守地工作，我们的客户网络绝对安全，对此无需担心。”网络战士们都在悄悄地保护设备...

军备竞赛

数据的保护也需要国际性合作。继海陆空甚至太空被开拓为战场外，网络空间正成为无声的战场。

“网络安全不应在开发周期的末尾出现，而应在开发伊始就进行布局。”

Kilian Golm

的客户菲尼克斯电气在2008年接管了这家初创公司。2016年，这家总部位于柏林的公司更名为菲尼克斯电气网络安全公司。现在，菲尼克斯电气的这家子公司拥有40名员工。柏林分公司负责开发和改进安全软件，客户支持人员则负责包括培训在内的综合解决方案，而mGuard硬件在巴德皮尔蒙特组装。

每个网络都会受到攻击

“mGuard”网络安全设备具有支持路由器、防火墙、VPN（虚拟专用网络）、QoS（服务质量）和入侵检测的功能。服务范围由可高度扩展的设备管理软件补充。“mGuard具有1000多种配置选项，因此是菲尼克斯产品系列中最为复杂的产品之一。”Martin Dickopp的解释充满自信。

Dickopp说：“绝对的安全根本不存在。每个网络都是十分脆弱的。但是我们的产品会使攻击者需要付出很大的努力才能实现网络攻击，这会迫使他们放弃。”

原则上，网络保镖可以区分两种类型的攻击。有些攻击是随机的，分布在各个方向并攻击它们遇到的任何网络。另一些则是针对性的网络攻击。这些活动可能是由私人黑客策划的，他们野心勃勃，不断袭击防火墙和安全概念以展示自己的技巧。或者是由犯罪团伙甚至国家策划的。 Kilian说：“在为客户准备的威胁分析中，我们着眼于区分具有不同资源的攻击者。”Kilian Golm向我们描述网络安全服务概念，该概念已集成到企业集团的安全服务产品中。

mGuard
在巴特皮尔蒙德现场组装硬件

初露曙光的研究

如果您想采取合适的措施，就必须知道您的对手是谁。Martin Dickopp笑了：“我们参加了黑客大会，对互联网上难以访问的部分进行了研究，并在论坛和社区中交换信息。”任何人也可以邀请柏林的专家对他们认为安全的公司网络进行模拟攻击。“找到漏铜”是我们工作的座右铭。

谁需要专业数据卫士的保护呢？“事实上，每一家企业都需要。我们的客户涵盖小型的家族机械制造商到全球的大型工业公司。当然，还有我们自己的公司。网络犯罪无国界。”Golm强调，“网络安全是一个持续的过程，而不是一次性的。您必须在设计时就确保网络系统的安全。当今的公司和技术应从开发伊始就考虑产品及其生产设施的安全性，而不应将其视为开发结束时的最后一次安全检查，并将安全概念生硬地嫁接到系统中。”(lo) ■

phoenixcontact.com

最著名的

网络攻击

现在工业安全事故发生的次数越来越多。

其中最著名的是

超级工厂病毒

2010年的攻击，影响了SCADA系统。

病毒

Industroyer

在2016年引起了轰动，

Triton

专门攻击安全控制器。

WannaCry

是一个勒索软件，到2017年已经感染了23万多个系统。

URGENT/11

是一个安全漏洞，在2019年夏天被发现，影响全球超过20亿台工业设备。客户可以在mGuard产品系列的帮助下保护自己的网络安全。

锂离子电池的艰难之旅

电动汽车的浪潮正达到顶峰。这与各种新技术的开发和测试有关。在位于布隆伯格的菲尼克斯电气实验室，研究人员对重达800公斤的锂离子电池组进行了测试。让我们一起来看看这幕后的故事。

关于电动汽车自燃的报道已经屡见不鲜。由于人们需要较高能量密度的电池且电动汽车的行驶需要使用电池，这个话往往成为人们讨论的焦点。随之而来的还有电池的耐用性、恒定载荷和安全性的问题。这也从一个侧面解释了为什么布隆伯格的菲尼克斯电气测试实验室对汽车行业非常重要。

“我们正在努力提高蓄电池的耐用性。“说这话的人没有戴魔法帽，也没有时间机器。 Michael Jonca是菲尼克斯电气电池实验室的负责人。他给人的印象不仅非常讨喜，而且是非常可敬。因此，他们并没有在说花言巧语，而是在努力通过真正的技术实现突破，解决电动汽车的能源问题。

时空之王

“我们的工作是在生产阶段人工老化锂离子电池。 通过先进的测试方法，我们强调可以提高这种敏感能源的耐用性，甚至超过电动车辆的使用寿命。”这是一个有点魔力的时间机器！“我们严格遵循制造商的规范。”Jonca解释他的任务时说。

菲尼克斯电气测试实验室是由菲尼克斯电气公司于1994年成立的一家独立的测试机构，现以Phoenix EMV-Test GmbH的名义运营。 它成立的初衷是进行电磁兼容性测试（简称EMC），从那时起，这个测试一直是强制性的。尽管这个实验室与菲尼克斯电气关系密切，独立性一直是它的一个重要特征， 这种独立性是这家高科技公司迅速取得成功的一大基石。成功的另外一个重要原因就是其一直秉承客户为王的理念。

因此，在Königswinkel10的神圣大厅里，经常以严苛客户的要求为标准。“但十分抱歉，这些设备和测试对象都是禁止拍照的。”汽车工业需要十分严苛的高标准。 2011年起，菲尼克斯测试实验室一直是这些汽车公司及其800公斤重的能量存储系统不可或缺的合作伙伴。今年春天，一个占地约950平方米的现代化锂离子电池和模块测试实验室正式投入使用。

“这个测试中心的建设初衷就是为了测试电池。”我们和菲尼克斯测试实验室的市场营销专家Thomas Worsch一起，开始了对测试机构的参观。 Michael Jonca解释说：“电池是理想的测试对象，因为出于安全的考虑，我们可以单独处理用于测试的复合物和样本。”“虽然我们没有在这里测试任何破坏性场景，我们也没有故意将测试对象排除在破坏性力量之外。我们的耐用性和使用寿命测试也会使大型电池承受相当大的压力。“因此，我们与当地消防队进行了非常密切的合作，他们必须在不危及实验室其他设施、员工和周围居民的情况下迅速控制住可能发生的火灾。”

艰辛之旅

大型电池块的测试需要几个月的艰苦工作，第一步是电气测试设备。“我们在这里开足马力充电，一两个小时后就能充满电。然后将充放电过程重复上千次。因此，我们的实验

“我们正努力提高电动汽车电池的耐用性，甚至远远超过车辆的使用寿命。”

Michael Jonca,
电池技术测试实验室负责人

Michael Jonca in a part of the modular battery labs

T-shocker模拟
温度下降
常量变化范围自
–40°C至+75°C

电动汽车中的电池

室耗电量与菲尼克斯电气产品生产的实际耗电量相似。”

在测试结束后，测试对象会被放置一到两个星期再交给客户。“电池中的化学反应不会突然结束。”电池实验室的负责人解释说：“这种化学反应往往还会持续一段时间。运输途中可能会被引燃，所以不能立即交给客户。”

为航运业带来的震动

接下来的测试变得越来越机械了。我们走向下一个实验室。这听起来就像一个游乐场:“这是我们的振动器，换而言之这里是我们的振动室。在这里，我们在一个可以进行冷热模拟的环境下将电池组持续摇动两周左右。”试验台有房子那么高，尺寸非常大。“我们用一台5吨重的吊车将测试对象连同它的框架一起吊到合适的位置。”单是摇动钢板就有35吨重。它安装在地基上，否则它周围很大的范围内的地面都会颤抖。”Thomas Worsch解释说。Jonca补充说：“在这里，我们也测试航运业和工业用组件，不仅仅是电池，还有整个控制柜。试验台采用“单轴振动法”进行振动。为了在三种方向上摇动同一个测试对象，它在测试系统中的位置会改变。这个试验台还有一个作用:“我们还可以模拟机械冲击，比如开车越过路缘。这时测试对象的荷载高达50克。”

根据客户的要求，电池有时需要在菲尼克斯电气实验室中测试6个月，有时甚至需要将近一年半的时间。电池还必须经历下一个痛苦的考验：T-shocker。“在10到30天内，电池组必须能够承受-40° C到+75° C的温度下降。这些都是汽车工业非常典型的需求。“在这里，电池外壳需要承受非常大的强度。”

18

原型电池组的最长测试周期为18个月

2

电池实验结束两周后被送还

最后一道关卡：游泳池

如果测试对象到目前为止仍然一切良好，那么下一个即将到来的“折磨”就是将其放到游泳池中。“这个大泳池是全新的。”Jonca的声音在这个专门的游泳区回响。天花板上有一台大型吊车，它可以将电池放入冷水或温水中。“我们还可以把水加热。”

每个电池组都由工程师和相关员工组成的团队负责，各自的测试程序是完全不同的。“目前，我们正在测试十二种不同的对象，也测试了十二种不同的能源。”如果您和友善的Jonca先生一起通过了他的“刑讯室”，你可以确信，在这里安然无恙逃脱的测试对象几乎可以轻松地耐受任何“酷刑”。(lo) ■

phoenix-testlab.de/en/start

振动器能摇晃重达四吨的测试对象

这些模块易于从测试程序中分离出潜在故障

各行各业的视频盒

在体育和娱乐行业，一开始就确定的胜利是无聊的。但在工业安全应用方面，一个安全的产品会让人心跳加速。全新的Smart Camera Box是这样的赢家吗?

几个星期前，编辑部的电话突然响了起来。电话另一端，一位同事问道:“这期杂志的主题是关于安全的吧?我们有一些很棒的东西愿意跟大家分享。是一个用于基于图像的监视系统的视频盒。”“开玩笑吗？视频终端盒有什么新奇的?你可以在亚马逊上花50欧元买到监控野生动物的摄像头。它们甚至有WiFi功能。”“我说的这个完全不同。你为什么不与开发盒子的同事见面谈谈呢?”

上图的分线盒基于2018的一个新品开发的

这是一个装置，不是一个简单的盒子

Tommy Göring

这项研究很快就发现，视频摄像头技术发展十分迅速，不适合菲尼克斯电气涉足。“然而，通过我们的Smart Camera Box，我们在摄像头和视频中心之间建立了面向未来的连接。”这位工业通信接口部门的专家强调，通常必须在视频监视系统中为摄像头构建额外的控制柜，该控制柜配备有来自不同制造商的解决方案，然后由两名技术人员安装。

“我们一定可以做得更好。所以，大约一年半前，我们开始开发解决方案。”汤米·戈林（TommyGöring）打开盒子。“首先，它可实现IP65和IP67防护等级，使用数年后依然可以高度密封。而且其适用-40°C至+70°C的温度范围，几乎可以在任何地方使用。”该智能盒由230 V电源供电，然后通过以太网供电（一种组合的电源和数据电缆）转发给摄像头。

连接比比皆是

通过菲尼克斯电气TRABTECH电涌保护产品线可更换的插拔式防雷元件，可以保护电子模块内部和连接的摄像头免受电网自发性意外故障的损坏。“当雷电或过电压导致电涌保护装置脱扣时，它们还会向视频中心发送SNMP消息。” 如果有人恶意破坏外壳，则特殊的接近传感器将确保在控制中心触发另一个警报。因此智能盒可以通信。

数据通常通过光纤传输至到控制中心的接收设备，特别是在远距离传输时。“为此，盒子有自己的光纤分线盒。在这里，光纤可以用一个插头连接和固定，只需插入摄像头电缆即可。”

工业需要有形监控

几天后，我们见到了产品经理Tommy Göring，约定去参观视频盒。但在我们进行现场参观前，产品经历必须得先简要解释下菲尼克斯电气是如何发现视频监控这个开发方向的。“这一点也不难。很长时间以来，我们都在积极开发以太网络相关产品。我们不时会收到关于我们的光电转换器是否适合千兆数据传输的询问。但是自动化工程师并不需要这么高的传输速度。所以我们观察了到底是需要传输什么。并确定高质量的摄像头也配有标准以太网的RJ45接口。这就是为什么客户需要实现千兆数据传输。

另一方面，如果摄像头位于控制中心附近，则也可以连接标准以太网电缆。而且，如果要将Smart Camera Box集成到现有的早期网络中，也考虑使用两芯线（例如同轴电缆）将其连接到现代以太网。

在现代世界，“高端摄像头除了光模块，还有很多其他功能。它们已经成为自己的计算机，可以评估仍处于照相机时代的图像。换句话说，它们可以检测到人何时靠近栅栏。”

这是一个装置，不是个简单的盒子

“盒子最多可以连接四个摄像头。我们根据全新的以太网供电标准IEEE802.3BT来供电，可显著提高电流强度。 它也可以用来驱动电动摄像头。”视频盒可以帮助获取每一个角落的图像。如果需要，它甚至可以发光。“我们还放置了一个顶帽式轨道，用于接入Wi-Fi或安装蜂窝路由器。 24V的输出可提供所需的能量。”

然后，他们展示了视频盒在视频通信方面的最后一张决定性的王牌。TommyGöring抓住梯子，把他的视频盒牢牢地夹在胳膊下，飞奔上梯子。 在上面，他演示了如何轻松连接和安装盒子以及摄像头。“由于我们开发了一种特殊的桅杆适配器，一位安装人员就足够了。这通常是两个人的工作。”

这款Smart Camera Box，将在2020年汉诺威工业博览会上亮相。而那些需要进行视频监控的人员应该耐心等待这款出色产品的面世。

非常感谢这位同事以及她极富有说服力的展示。我的野生动物监控摄像头根本竞争不过它！ (lo) ■

update.phoenixcontact.com/en/

视频照明也可以用盒子来控制

卡萨布兰卡的问候

新销售部门服务于马格里布国家

菲尼克斯电气在这个摩洛哥西部的港口和地中海贸易城市建立了一家新的销售公司。在该公司工作了多年的Youssef Asmi负责这个城市相关工作的开展。他之前在加拿大工作了十二年。现在，他决定回到自己的祖国。因此，作为地区经理的Youssef Asmi和新的子公司将成为马格里布三个国家（摩洛哥、阿尔及利亚和突尼斯）客户的联系点。

像谷仓的门一样打开

20亿台设备受到漏洞威胁

2019年7月，宣布已发现11个零日漏洞，这些漏洞会影响实时操作系统Wind River VxWorks。VxWorks已在超过200万台重要的工业试验、医疗和公司设备中得到应用。

这11个安全漏洞被归类为URGENT / 11，远程攻击者无需任何用户交互即可获得对设备的控制，并可跳过防火墙等安全系统。

由于应用广泛，更新运行VxWorks的所有设备通常十分不容易，甚至是不可能。但是菲尼克斯电气可通过mGuard安全路由器提供一种简单且易于改装的解决方案：安全设备能够方便地集成到网络中，并完全保护VxWorks设备不受所有关键的URGENT / 11漏洞的攻击。

世界级科学家应邀访问巴德皮尔蒙特

麻省理工学院的Suzanne D. Berger教授在德国进行考察研究

来自麻省理工学院的四位科学家组成的代表团前往巴德皮尔蒙特参观了菲克斯电气，以及建在此处的数字化工厂。Suzanne D. Berger教授访问德国是为了新书的研究工作。2013年，她发表了《美国制造：从创新到市场》研究。Berger教授在书中探讨了为了通过创新创造价值，美国是否需要提高其生产部门的效率。

现在，她正在着手一个新项目：在“未来工作”工作组中，麻省理工学院各个学院的专家正在共同努力，以确定新技术对公司员工的影响。麻省理工学院的团队在寻找技术前沿公司时注意到了菲尼克斯电气。

在2018年底于中国天津举行的世界经济论坛年会上，菲尼克斯电气被评为全球九家领先的智能工厂之一，这些工厂已经在实际生产中应用了IIoT技术。在生产区域的参观中，菲尼克斯电气展示了如何在短时间内改装设备和系统，能够实现新产品的生产。基于数字孪生技术，产品生产十分智能。这样，即使是小批量生产和特殊生产也可以实现，而这在纯批量生产中是十分不经济的。

D.Berger教授（中）及其团队和生产经理Tilman Potente博士（右）

打印机的创新

Protiq打印纯铜

通过纯铜的3D打印，Protiq在增材制造领域取得了重大突破。在2019年11月下旬在法兰克福举行的专业贸易展览会上，以总经理RalfGärtner博士为首的团队向大家介绍了全球独一无二的创新流程。

迄今为止，印刷纯铜被认为是不可能的，因为金属会反射熔融激光的射线，导致其被销毁。由于其优异的导电性，铜被用于制造用于部分硬化零件的电感器。但是生产过程复杂且耗时，通常需要数周的时间。

采用新工艺，可以将常规加工时间减少到几个小时。此外，可以直接在Protiq在线平台上传和配置组件的制造数据并直接订购。

protiq.com

“防疫战”

工业网络的信息安全

2020年，突如其来的疫情使大家对病毒的影响和安全防疫有了更深的认知，其实工控行业的信息安全也是不容忽视的。今天我们就一起聊聊工控行业的信息安全“防疫战”。

2010年Stuxnet震网病毒

Stuxnet震网病毒是世界首个大规模传播的专门针对工业控制系统编写的破坏性病毒，通过优盘和网络进行传播，该病毒近60%的感染发生在伊朗，其次为印尼（约20%）和印度（约10%）， 阿塞拜疆、美国与巴基斯坦等地亦有小量个案。这次事件使工业信息安全问题第一次大规模的暴露在人们面前。

2017年WannaCry（永恒之蓝勒索病毒）

2017年WannaCry（永恒之蓝勒索病毒）在全球大范围爆发，除了办公电脑和个人电脑之外，全球众多工厂的工控机出现了大规模感染，对生产线的正常运转造成了极大的负面影响。这次病毒的爆发，再次提醒工控行业要对信息安全加大重视力度。

对于各种计算机病毒，其传播途径主要是两个：一个传播途径是优盘传播，另一个传播途径则是网络传播。阻止病毒的优盘传播，可以通过锁定USB端口，禁止使用优盘的方式阻止其传播。

阻止病毒的网络传播却非常麻烦！原因：目前主流的生产线设备都是通过网络来进行数据交互，一旦设备离线就无法进行正常的生产运行，因此，通过将设备离线的方式来阻止病毒的传播也越发困难。

这就需要一种专业的工业网络安全设备——工业硬件防火墙。工业硬件防火墙类似于全国都在疯抢的口罩。口罩既能防止病毒进入人们的呼吸道，从而达到预防感染的目的，同时还能保证人们进行正常的呼吸。

工业硬件防火墙通过对所有数据进行比对处理，将每个数据包的特征信息与防火墙规则里的特征信息进行比对，符合放行规则的数据就放行处理，不符合放行规则的数据则丢弃处理，避免未经授权的数据通讯，从而阻止病毒的传播，并防止未经授权的访问。

其实在工控行业，除了面临病毒破坏的挑战，也面临信息泄露的挑战。

二、非对称加密：

采用两个密钥进行加密和解密，这两个密钥分别是公开密钥（简称公钥）和私有密钥（简称私钥）。公钥与私钥是一对，如果用公钥对数据进行加密，只有用对应的私钥才能解密；如果用私钥对数据进行加密，那么只有用对应的公钥才能解密。因为加密和解密使用的是两个不同的密钥，所以这种算法叫做非对称加密算法。

非对称加密的算法强度复杂，在安全性上面领先对称加密，但正是由于其算法复杂，运行速度慢，也就造成了加密和解密效率要远远落后于对称加密。

所以在既注重安全性又注重效率的通讯场合，一般混合采用非对称加密和对称加密两种方式来完成整个通讯过程。前期先采用非对称加密，后期再采用对称加密。前期的非对称加密主要用来传输密钥，这个密钥用来在后期通过对称加密进行数据的加密和解密。数据加密的密钥采用非对称加密方式来进行，所以保证了数据加密密钥的安全。数据加密和解密采用对称加密的方式进行，所以又具备了很高的效率。非对称加密和对称加密在这里实现了完美的融合。

至此，网络通讯过程中数据加密和解密的问题得到了很好的解决，看起来万无一失了，但是假如在通讯过程中，有恶意的第三方对正常的通讯进行拦截，然后伪造通讯进行冒充，就会造成所有的加密全部失效，这就需要使用签名来避免冒充和篡改。

发送方在发送加密数据的时候，使用自己的私钥进行签名，接收方接收到数据之后，使用加密方对应的公钥进行解密，如果解密成功且信息比对成功，就说明数据是发送方发来的，没有冒充，数据也没有出现篡改。而如果比对失败，就说明数据被篡改了。

mGuard系列解决方案

今天我们简单了解了工业网络中阻止病毒传播和防止信息泄露的主要技术，针对此类技术，菲尼克斯电气提供了mGuard系列解决方案，不仅内置工业防火墙，有效防止病毒在工业网络的传播，而且内置高强度加密和认证，有效保证远程通讯数据的安全。

与疫魔竞速

菲尼克斯电气鼎力驰援“雷神山”！

举国上下，众志成城，防疫防控。在加入这场没有硝烟的新冠战“疫”的同时，菲尼克斯电气在地方政府的支持下开始了井然有序的复工复产工作，并且有效实施了创新的防疫防控方案，受到相关政府领导的肯定和多家媒体的关注，登上了CCTV、JSTV、NJTV新闻。

菲尼克斯电气为武汉“雷神山”医院的建设免费提供产品和技术支持，克服重重困难，与合作伙伴一起于24小时之内完成产品的特殊调配和物流运输，紧急驰援一线赈灾防疫工作。

1月31日晚，菲尼克斯电气从合作伙伴处了解到，“雷神山”医院部分项目配电系统中，急缺电气产品。公司内部迅速响应，经过与合作伙伴众业达电气的通力合作和紧急协调，最终将所需的产品和设备及时发往项目工地。从沟通、选型、确认，到调货发货，24小时内完成所有工作。菲尼克斯电气的意选系列产品及时安装在“雷神山”医院ICU病房和办公室辅热与影像中心送排风部分的配电系统中，为一线医疗救助工作提供了强有力的电力保障！