文档级别：内部　　行文编码：975-4-08-2304-01-6

工业信息安全的未来

——工业网络生态系统与工业防火墙

董鉴源

山河实验室

工业信息安全发展研究小组

摘　要：工作报告通过回顾工业信息化的历史，对其发展过程中遇到的一些问题与现象进行分析，总结了由于时代局限导致的部分现状，以及新一波工业浪潮之下，工业信息安全未来发展的方向和趋势，最后提出了工业信息安全领域策应市场的些许建议，包括产品规划路线、安全技术积累、人才建设储备以及发展迭代策略等。

关键词：工业网络生态系统；工业信息安全；工业防火墙。

引言

工业是国民经济的主体之一，是立国之本。根据世界银行提供的数据，国际的工业化迄今已经有三百多年的历史，全球范围的工业先后经历了蒸汽机时代、电气化时代和信息化时代。随着德国在 2013 年的汉诺威工业博览会上正式推出“工业 4.0”的概念，美国也提出了“工业互联网”的概念，与之对应的则是国内提出的《中国制造 2025》战略计划，至此，工业正式步入了智能化时代。

工作报告将对智能化时代背景之下工业网络生态系统面临的各种安全威胁进行分析研究，总结现有针对工业信息安全问题的关键防护技术，阐述工业信息安全产品部署的意义与面临的挑战，并深入讨论未来工业防火墙的发展趋势和市场价值。

工业的信息化进程

到了上个世纪五十年代，发达国家陆续进入后工业化社会，信息技术的创新逐步应用到了工业领域，工业的信息化取得了巨大成就。在这一时期，美国、德国和日本先后成功研制出了第一代数控机床。

之后随着信息技术的不断进步，工业的信息化进程也在同步发展，后工业化社会对信息的依赖充分得到了证明。

与信息技术一致的是，工业的信息化进程同样经历了电子管时代、晶体管时代、集成电路时代等，这种一致性几乎是全盘接受了信息技术的优缺点。

进入二十一世纪以来，互联网技术异军突起，信息技术以惊人的速度迅猛发展，其中无论是硬件技术还是软件技术的更新换代都过于短暂，工业的信息化进程囿于成本奇高和人才稀缺等等各种因素，逐渐跟不上信息技术的前进步伐而产生了一定的滞后性。

新型工业化

新型工业化是发展经济学中的一个重要概念，特指知识经济形态下的工业化进程。

知识经济是以知识为基础，以脑力劳动为主体的经济模式，与过往的农业经济和工业经济相比，高素质的人力资源逐渐成为知识经济的关键要素，它促使现代化社会的发展方式从过去那种资源大量消耗、环境严重污染的旧式工业化向科技高、效率高、能耗低、污染低的新型工业化进行升级。

旧式工业化所带来的种种弊端，在随后的改善和治理过程中，迫使先行完成工业化的发达国家转变了思路，提出可持续发展的新概念，而信息化发挥出来的至关重要作用，让发达国家渐渐地意识到了知识产业的重要性，工业化、信息化与知识化得以有效融合。

知识经济时代，没有经过传统工业化的发展中国家可以直接通过新型工业化缩小与发达国家的工业差距，实现赶超战略，借助知识产业直接达到工业文明的繁荣。但是，由于计算机科学与技术的历史相比其它学科而言非常短暂，同时人才培养严重落后于技术迭代以及市场需求，高素质的人力资源缺口在各个行业的信息化中被极限放大，新型工业化对严重失衡的高科技人才的竞争始终处于绝对劣势。

新型工业化未来不会消失，而且会占据越来越多的工业比重。与此同时，信息技术的进步也将持续，绝不可能停下脚步等待工业化的追赶。

新型工业化向工业智能化转变带来的机遇和挑战

工业 4.0 在 2013 年被德国正式推出之后，又入选了《思想·创新·增长——德国 2020 高技术战略》的十大未来项目，它将加速实现工业信息化走向工业智能化，而新型工业化完美地起到了承上启下的作用。

顾名思义，工业 4.0 的定位是驱动人类第四次工业革命的战略项目，涉及的具体内容有**工业互联网、工业云计算、工业大数据、人工智能、工业网络安全、虚拟现实、工业机器**

人以及**知识工作自动化**等方向。

通过纵观人类历史前三次工业革命的发展周期，以及当前工业信息化落后二十年的发展状况，可以确定未来至少还有五十年的发展空间，这也预示着工业智能化的市场充满了各种各样的机遇和挑战。

工业信息安全市场与投资策略

安全的概念很广泛，其本质是一个值得深思的问题，它在不同的行业有着近乎完全不同的定义。比如，食品安全、消防安全等与信息安全的差异就十分明显。

国家标准《GB/T 13745-2009 学科分类与代码》中，安全科学技术的代码为 620，是一级学科，计算机科学技术的代码为 520，同样是一级学科，但是信息安全技术的代码为 41320，是一级学科信息与系统科学相关工程与技术下的二级学科。密码学、安全协议、系统安全、软件安全、网络安全、信息隐藏、安全评测等则是信息安全技术下的三级学科。

国家标准定义了三级学科，其中 62 个一级学科或学科群，676 个二级学科或学科群，2382 个三级学科。2022 年的普通高等学校本科专业目录含特设专业与国家控制布点专业共计 771 个专业。网络空间安全专业作为工学计算机类特设专业与国家控制布点专业在 2015 年才被增设成本科专业。

信息安全行业是一个常青藤行业，未来长时间内不存在衰退期，它将随着新技术的不断出现持续发展。相对传统信息安全行业而言，工业信息安全市场仍然是一片巨大的蓝海，所以，工业信息安全行业将会成为信息安全行业的下一个增长点。

通过每年的投资数据分析，信息安全市场的规模接近六千亿人民币，工业信息安全市场的规模约一千三百亿人民币，工业网络安全市场的规模约五百亿人民币，其中防火墙产品占了一百多亿人民币。

工业信息安全行业的大多数市场份额集中在高端或者大型商业客户，而网络安全相比产品研发水平，更为注重的是网络攻防的服务水平。因此，无论是技术团队还是市场团队，低层次人员很难提供这种大型服务能力。

所以，想要投资工业信息安全市场，必须建设完善的安全团队，提前做足技术储备，才能在风口到来的时候享受到足够多的市场红利。

工业系统的历史遗留问题

工业 4.0 的工业网络安全，一方面是指，保护工业网络生态系统中的工业设备不被入侵和破坏，另一方面是指，保证工业网络生态系统中的工业数据以及信息是可信的。

但是，工业系统本身有很多历史遗留问题，包括但不限于工业信息设备的系统陈旧落后、工业通信协议在设计之初就缺乏安全性考虑、工业软件应用在开发时未考虑被黑客攻击的情况、工业软件系统研发人员缺乏必要的信息安全意识等。

另外，微软公司为了布局工业，对工业系统的早期发展进行了大量扶持和投入，这也导致了现在工业系统的主流操作系统仍然以 Windows 操作系统为主。不过 Windows 操作系统的安全性向来为业界所诟病，臭名昭著的震网病毒和勒索病毒都是 Windows 操作系统下的。当然，除了大量病毒木马之外，还有数不尽的各种系统安全漏洞。

至于工业系统开源技术解决方案，以数控机床来看，在上个世纪七十年代数控系统发展到第五代的时候，仍然早了 Linux 发布 0.01 内核版本二十年左右。虽然最近几年得到了不少改观，但是在可以预见的很长一段时间之内，开源技术解决方案仍然无法成为工业系统的主流技术解决方案。

由上观之，工业现场的工业网络生态系统中存在着大量以信息安全视角来看并不安全的工业设备，但是这些不安全的工业设备对于现场的使用人员来说却是可信的，姑且称其为“可信非安全设备”。

这些情况共同导致了传统防火墙以及传统的信息安全技术并不能很好的保护工业网络生态系统中的工业资产。

信息安全产品分类

信息安全产品的分类有不同的标准：

一、按照美国标准来讲，分为九类，包括鉴别、访问控制、入侵检测、防火墙、公钥基础设施、恶意程序代码防护、漏洞扫描、取证、介质清理与擦除；

二、按照中国标准来讲，分为七类，操作系统安全、数据库安全、网络安全、病毒防护、病毒控制、加密、鉴别；

三、按照中国军标来讲，分为六类，物理安全、平台安全、数据安全、网络安全、用户安全、管理安全；

四、按照市场标准来讲，分为五类，基础安全类、边界安全类、终端安全类、审计管理类、工具支撑类。

基于不同的分类，整个信息安全市场拥有一百多条信息安全产品线，并且随着新技术的出现在不断递增，例如信息安全领域目前最火的云安全产品线以及未来即将爆发的人工智能安全产品线等。

工业信息安全产品线

目前，公司的工业网络安全基础非常薄弱，技术储备与积累不足，人才管理和建设落后，想要进行产品设计与迭代面临着非常艰巨的挑战，因此，有必要调整产品的研发策略以及研发顺序，从而有效地稳步推进。

结合现状深入分析之后，建议未来根据实际情况可先后布局的工业信息安全产品线，大致如下：

1、**工业网络安全审计系统**；
2、**工业防火墙**；
3、**工业互联网安全网关**；
4、工业单双向网闸；
5、工业网络漏洞扫描系统；
6、工业网络入侵检测与防御系统；
7、工业网络流量分析系统；
8、**工业设备接入控制系统**；

9、工业网络风险评估系统；

10、工业网络安全平台工具集；

11、工业安全管家；

12、**工业网络零信任架构体系**；

13、**基于工业云计算和工业大数据的安全威胁态势感知**。

上述工业信息安全产品线布局成熟之后，则可以成功构建针对未来工业信息安全市场的综合性工业网络立体化安全解决方案的基础服务水平。

（具体的硬件指标参数与软件设计功能详见产品文档）

综合性工业网络立体化安全解决方案

工业信息安全尚未引起业界的普遍重视，大多数客户首当其冲是为了应付某些类似等级保护的合规需求，并不在意真正的网络攻防问题。一旦过了这个浮于表面的危险阶段，工业信息安全行业将会迎来很多重要的变化，整个工业信息安全市场也将随之打开。

工业网络生态系统随着工业 4.0 的推进一定会变得越来越复杂，单一的工业信息安全产品将不再满足工业信息安全市场的变化需求，因此，综合性工业网络立体化安全解决方案的大型服务能力会逐渐演变成工业信息安全市场的绝对刚需。

从传统防火墙的历史看工业防火墙

防火墙技术诞生于上个世纪八十年代，几乎与路由器同时出现。经过了接近四十年的快速发展之后，市场上形形色色的防火墙产品已经成为信息安全领域边界安全解决方案里无可争议的重要产品线。

防火墙产品的分类方法比较多，从不同角度来看有不同的分类。从逻辑上讲，防火墙产品可以简单分为主机防火墙和网络防火墙；从物理上讲，防火墙产品可以简单分为硬件防火墙和软件防火墙；从功能上讲，防火墙产品可以简单分为应用防火墙、系统防火墙等。另外，还可以基于技术选型、部署位置、性能结构等进行分类。

传统防火墙技术先后经历了五个发展阶段，基于包过滤技术的第一代防火墙产品、基于代理技术的第二代防火墙产品、基于状态监测技术的第三代防火墙产品、基于统一威胁管理的第四代防火墙产品以及基于下一代防火墙技术的第五代防火墙产品。

不过，第一代工业防火墙产品是以深度包检测技术为主进行研发的，它融合了前四代传统防火墙产品的一部分功能，由于国内各家公司的产品标准并不统一，进而导致了市场上第一代工业防火墙产品的质量严重参差不齐。

总体来说，在时下的工业网络生态系统中部署陈旧的传统防火墙产品没有太大的实际意义，而第一代工业防火墙产品又存在着很多技术伪装的成分，甚至想要开发部署严格意义上基于下一代防火墙技术的第二代工业防火墙产品，也会因为受限于当前的工业环境无法提供足够的市场商业价值，间接导致业内的大部分公司不愿意进行太多投入，从而影响到现在整个工业防火墙市场的发展速度。

下一代工业网络防火墙

相较于第一代工业网络防火墙产品，第二代工业网络防火墙产品的起步很高，跨越了传统防火墙产品的多个发展阶段，是直接按照下一代防火墙技术的标准进行研发的。

遗憾的是，国内市场上现存的第二代工业网络防火墙产品都只实现了下一代防火墙技术的有限功能，并未出现真正意义上的基于下一代防火墙技术推向市场的第二代工业网络防火墙产品。

尽管如此，为了满足工业网络生态系统未来的信息安全变化需求，经过工作中长期的研究总结，山河实验室工业信息安全发展研究小组在第二代工业网络防火墙产品的基础上，提出了对下一代工业网络防火墙产品的定义以及要求：

(A)、满足高性能低延时的工业级硬件；

(B)、基于安全内核的定制操作系统；

(C)、利用前五代防火墙技术适配各种工业场景；

(D)、智能化的安全机制与策略；

(E)、可以对系统化层次化结构化的防火墙功能进行灵活配置和扩展；

(F)、提供与第三方安全厂商各类产品的交互性通信协议；

(G)、能与工业零信任架构体系或安全威胁态势感知等综合性工业网络立体化安全解决方案的其它系统进行完美融合来有效防护工业资产。

（下一代工业网络防火墙产品相关技术可参考《基于第六代防火墙技术的工业网络生态系统安全研究》学术论文）

工业防火墙开源技术解决方案

通过对搜索引擎得到的一百多个防火墙开源技术解决方案进行评估分析，基于下一代防火墙技术的开源技术解决方案屈指可数，而且距离商业化目标非常遥远。

因为下一代防火墙技术的开源技术解决方案的过度缺乏，加上下一代工业网络防火墙产品的研发周期特别长，难度非常大，这就意味着市场上的主流工业防火墙产品都有很大的进步空间，故此，一些技术创业型安全小公司则可以拥有很多机会进行弯道超车。

工业防火墙评价体系

工业防火墙可以从物理硬件安全、操作系统安全、防火墙产品功能、工业数据安全这四个纬度的安全指标进行全面评价。

《信息安全技术 第六代防火墙安全技术要求和测试评价方法》

（此处省略具体评测标准）

工业信息安全的未来

目前，工业信息安全的整体技术解决方案还是偏向于对早期工业设施的基础保护，而这种基础保护的效果其实非常有限。

尽管工业现场面临着工业设施更新换代困难的压力，以及工业系统充满了多种信息安全隐患的现状，但是随着工业的进一步发展，过往的困境将会不断地得到合理改善，从而走过艰难的过渡阶段。

如果成功借助工业 4.0 的工业网络安全大势，工业信息安全势必会迎来脱胎换骨。

未来预期的工业变化也会引入更多更高的工业信息安全需求，促使工业走向工业 4.0 引领的工业智能化时代，由此绽放出多姿多彩的新型工业文明。

结束语

工业信息安全作为信息安全领域的一个重要应用分支，相对于政府信息安全、军队信息安全和金融信息安全等领域，虽然起步很晚，也比较落后，但是必将迎难而上，大步追赶，最终肩负起来其应尽的责任，有效保障工业文明的繁荣发展。

参考文献

（此处省略全部参考资料）

二零二三年四月十三日 于 中国·济南

『初次修订』

注释：行业报告引用的详细数据全部来自风华资本的京正数据库。

编辑校对：李海龙 沈誉水

行业报告·工业信息安全·二零二三年