民用飞机生产线自动控制系统的信息安全问题探析

Information Security Issue of Civil Aircraft Production Line Automation Control System

上海飞机制造有限公司　王丰超　陈　磊　韩建宾　孙中刚　李汝鹏
国家国防科技工业局信息中心　赵　越

[摘要] 随着信息化技术越来越多地应用到工业控制系统，不可避免地也带来了各类风险和威胁，系统的信息安全问题也就越发需要引起重视。对民用飞机生产线自动化控制系统存在的安全隐患进行了探究和分析，结合其他领域的工控系统安全措施，针对本系统的一些威胁和漏洞提出了安全风险防范方案。

关键词：民用飞机　工业控制系统　信息安全

[ABSTRACT] As the growing number of information technology applied on the industrial control systems (ICS), which inevitably also brings a variety of risks and threats, information security of system should increasingly attract great attention. Civil aircraft manufacturing system is a large-scale industrial automation systems integrating a variety of information technology. Firstly the system with global perspective is introducd, and the potential security risks are superficially analyzed; Combined with security measures of industrial control systems of other areas, aiming at vulnerabilities of the system, finally, security strategies are recommended.

Keywords: Civil aircraft　Industrial control systems　Information security

近年来，随着数字化技术的迅速发展和广泛应用，以及民用飞机制造具有的高度复杂性和协同性，使得数字化、柔性化自动装配技术成为了现代飞机制造业的必然趋势。通过将网络数字技术应用到飞机生产线上，把企业资金信息、物流信息、生产设备状态信息、市场信息、生产能力信息等实时全面地提供给管理层，能够实现管控一体化，提高生产效率，从而满足快速需求和客户化定制。同时，数字化制造技术对于提高我国自行研制民用飞机的市场竞争力、推动民机产业的发展也具有重要意义。

数字化生产线控制技术从整体上改善了生产管理，提高了数字化设备的效率，从而提高了制造系统对产品品种和批量变化的适应能力，提高了产品质量和服务水平[1]。大型飞机装配是一个复杂而庞大的系统工程，围绕数字化生产线设备信息、质量控制信息和生产管理信息的及时采集与集成管理，开展数字化装配车间环境搭建，开发面向生产线的多源异构数据集成控制系统是飞机制造业发展的必然方向。然而，随着系统的复杂度提升以及信息化技术的运用，IT 技术的负面困扰也被引入了生产控制系统。与传统的 IT 信息安全不同，工业控制系统的安全事件轻则会导致系统性能下降、关键数据丧失，重则导致系统失控、环境灾难、人员伤亡、严重经济损失，甚至危害公众生活和国家安全。而民机生产作为大型工业系统，其信息安全更是关乎国家技术的安全，因此，本文将针对民机生产控制系统进行安全分析，并提出相应的安全建议，切实提高该系统的信息安全等级。

1　民用飞机生产线自动化控制系统

相比于传统工业，数字化车间通过结合柔性化装配和信息化管理技术，缩短了飞机制造周期，提高了装配质量。而早在 2000 年左右，美国洛克希德 · 马丁公司就已经使用数字化车间技术研制 F35，从而缩短了 2/3 的研制周期，而波音 787 飞机在研制过程中采用了基于 DELMIA 的数字化车间技术，这许多产品的成功案例都说明了数字化生产必将成为飞机制造的未来趋势。

大型客机是民用飞机的一种，其自动化生产线为民用飞机自动化生产线的典型代表。大型客机生产线自动化控制系统由智能装配子系统与智能工艺设计与生产管理子系统所组成。

（1）智能装配子系统是大客机体部件组装系统模块，分为平尾翼装配、中央翼装配、中机身装配、全机对接装配 4 大部分。其中平尾装配与中央翼装配工作内容相对独立，中央翼装配完成后送入中机身装配区域，中机身装配和平尾装配完成后送入全机对接区域。数字化车间通过集成自动导引车、虚拟五轴自动钻铆设备、MPAC 自动钻铆设备、自动制孔单元、激光跟踪仪、柔性工装、自动定位器等设备的装配线来完成以上装配工作。

（2）智能工艺设计与生产管理子系统以产品数据管理系统（PDM）所形成的单一产品数据源为核心，驱动飞机产品的数字化协同设计、试验仿真、虚拟制造验

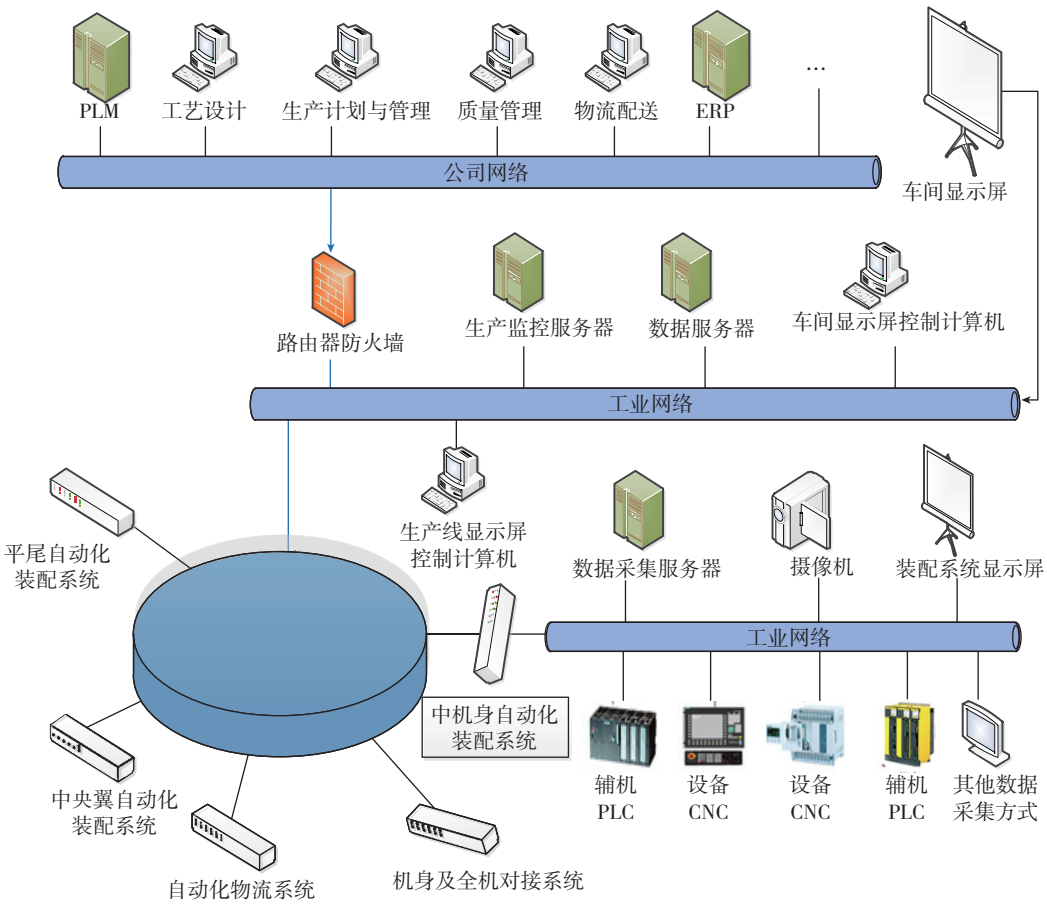

图1　智能工艺设计与生产管理子系统网络架构

Fig.1　Intelligent process design and network infrastructure of production control subsystem

证等工艺设计工作，并通过单一产品数据源的支撑，配合生产管理与物流配送系统以及经营计划系统，形成满足大客研制的低成本高效率的数字化生产线信息系统体系。子系统主要由精确化多源异构信息采集与处理、数字化装配工艺设计与仿真、准时化生产计划与管理、自动化物流配送、全程化产品质量检测与追溯管理、系统化设备管理与故障诊断等功能单元组成。

图 1 描述了数字化车间面向自动化装配硬件系统的软件系统组织与布局，数控设备、辅机等设备通过环形网络连接在一起，它们与上位数据采集软件的数据交换采用工业通用的数据接口及协议。中控室的服务器通过网络可以给上位管理信息系统提供生产信息数据。软、硬件采用分布式的体系结构，便于系统扩展。生产局域网通过硬件防火墙与外部局域网相连，这也是生产局域网与公司局域网的唯一通信接口，同时生产局域网还提供 ISDN/ADSL 连接服务。

2　控制系统的信息安全隐患分析

工控系统由于其特殊的应用场景，相较于普通的 IT 系统更注重系统的可用性、完整性和机密性，而由于系统存在着大量的重要信息，对其信息安全的保护同样不能忽视。2011 年工信部发布了《关于加强工业控制系统安全管理的通知》，明确了重点领域工业控制系统信息安全管理要求。民用飞机生产控制系统就是一个集成了众多 IT 技术的信息化系统，这样的 IT 系统应用到工业制造的模式中将面临来自信息系统以及工业系统的双重威胁，下面将就系统中的组成部分以及网络结构等进行分析。

2.1　人员安全素质

2010 年某烟厂制烟车间 WINCC 服务器感染病毒，导致各终端与 WINCC 服务器之间连接通信中断，整个车间生产受阻。事后查明却是由于工作人员将未查杀病毒的 U 盘插入机台终端的 USB 接口进行数据拷贝时，导致病毒进入工业网中所致[1]。很明显，此案例中的操作人员由于缺乏安全意识，而导致了一场灾难。这可能是因为该企业未制定相应的信息安全管理策略，也可能是由于对人员的培训与管理执行还不到位，但无论什么原因，可以看出人员素质对于系统安全可靠地运行

至关重要。

系统需要人员进行运维，正是由于人员对系统的可控地位，让其对系统拥有着很大的威胁。大型客机生产线建设采用了先进的数字化车间技术，在初次搭建自动化控制系统的过程中就应当重视人员的安全意识培训。在飞机生产车间这样的大型系统中，如果由于人员的安全素养不高而导致生产线事故，除了造成巨大的经济损失，还可能导致人员伤亡。另一方面，也不排除为了不正当目的而进行破坏或窃取机密的人员威胁。总之，人员作为系统的重要组成部分，对于生产制造的可靠运行至关重要，需要有充分的系统培训和管理约束。

2.2 系统与软件漏洞

工控系统所使用的操作系统是专用的，且通常没有内建安全防护，某些运行和管理终端也会使用 Windows 或 Linux 等通用操作系统。目前大型客机装配生产线中的自动化控制设备仍以 Windows 平台为主，为保证过程控制系统相对的独立性，工程师通常在系统投入运行后不会对 Windows 平台打任何补丁，更为重要的是打过补丁的操作系统没有经过制造商测试，存在安全运行风险。与之相矛盾的是，系统不打补丁就会存在被攻击的漏洞，即使是普通常见的病毒也会发生感染，可能造成 Windows 平台乃至控制网络的瘫痪。著名的“震网”病毒就是利用 Windows 系统和西门子 SIMATICWinCC 系统的多个漏洞感染了伊朗布什尔核电站，攻击了其中的铀浓缩设备。

飞机的生产管理系统是以产品数据管理系统（PDM）所形成的单一产品数据源为核心的数字化生产线信息系统，其中涉及的软件包括基于达索系统和 Windchill 系统的数字化装配工艺设计与仿真流程平台以及自行研发的计划管理信息系统等，而在 2009 年 PTC 发布了 Windchill 的一项安全漏洞，它可能会被具备 Windchill 使用凭证且心存恶意者使用。另外，当应用软件面向网络应用时，常需要开放其应用端口，常规的 IT 防火墙等安全设备很难保障其安全性，网络攻击者很有可能会利用一些工程自动化软件的安全漏洞获取现场生产设备的控制权。

2.3 网络安全设备局限性

民机中的大客生产系统的边界防护主要是部署防火墙设备，然而作为一种被动防御手段，防火墙本身也存在着应用上的不足：防火墙只是一个策略执行机构，它并不区分所执行安全策略的对错，更无法判别出一条合法策略是否满足安全管理者的本意；防火墙的防范策略是在该攻击方式经过分析后设置的，这种防御的滞后性对于新出现的攻击方式将失去作用。所以从防火墙的实际使用情况来看，很难完全杜绝生产控制区的网络边界安全威胁。

网络安全设备的应用的确可以很大程度地增加系统的安全性，但是仅依赖于安全设备的部署或堆叠也是不够的。要做到对生产系统的全方位保护，更重要的是整体系统防护的安全策略和安全风险评估。基于安全风险评估的结果，企业可以更加了解系统的脆弱性和威胁源并制定相应的安全策略，控制风险从而保证系统的可靠性。

2.4 网络攻击与入侵

由于公司网络并不是完全隔离于外网，内部的主机或服务也就有可能成为网络攻击的目标。对于网络中传播的病毒、网页中挂载的木马等，一旦进入了公司内网，将威胁到生产系统从而导致不可估计的后果。同时，网络中从来不乏有目的的黑客行为，他们利用系统或者软件漏洞入侵目标，从而达成获取机密或者破坏系统的任务。

2.5 通信协议漏洞

民机的装配过程涉及平尾自动化装配线、机身对接及全机对接装配线等 5 条自动化装配生产线，其中的自动化设备需要相互协调与统筹管理，所以针对不同的设备和控制器所采集的数据传输需要制定相应的通信协议。这些专用的工业通信协议在设计过程中往往都不会考虑安全防护问题，所以其中的漏洞也就成为了潜在的威胁。

3 民用飞机生产控制系统的信息安全策略

由于民用飞机生产控制系统的复杂性和特殊性，以及前文对信息安全隐患的分析，需要从主动和被动两个方向同时建立安全策略，才能够有效保障其有效工作。结合工业控制系统网络与系统信息的安全标准[2]，构建民用飞机生产控制系统安全策略的逻辑结构（如图 2 所示）。

3.1 建立主动安全策略

（1）设立安全管理机构。

飞机生产系统需要多个部门协同合作，而各个部门的信息既有联系又有相对的独立性，信息的流通与审批、安全措施的实施与维护，都需要一个组织机构来进行统筹管理。该机构的主要职责就是安全策略的制定与执行、事故的处理等方面。信息安全是所有管理层成员所共有的责任，而且每个部门都必须配合此机构做好信息安全防护工作。

（2）人员安全意识培训。

系统即使拥有再好的安全策略，如果其中的人员并未按照策略进行事件处理，或者企业未按照策略进行管理，那么终会导致系统的安全措施形同虚设。上文提及

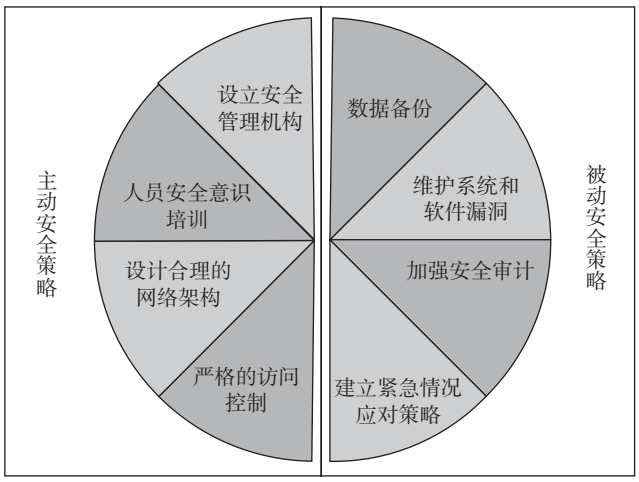

图2 民用飞机生产控制系统的信息安全策略逻辑结构

Fig.2 Logical structure of information security policy for civil aircraft production control system

的所有威胁中往往出现最多的就是由人员导致的，为了防止或降低此事件出现的可能性，对人员的安全意识培训是非常有必要的。

（3）设计合理的网络架构。

类似大客数字车间的成型系统一旦建成，后期如果还想对其进行调整，将变得异常困难。网络架构的总体设计必须考虑的一个重要因素就是信息安全问题。根据安全管理机构制定的安全策略，部署相应的安全设施以及安全技术到相应的系统模块中，这是系统中的重要环节。

（4）严格的访问控制。

在企业内部，每个人员扮演着不同的角色，每个角色拥有着不同的权限。对于系统而言，未经授权的用户进行的越权操作都属于违规操作，视为无效。控制未经授权用户进行访问可以通过多种手段，如通过有效的密码和完善的身份认证制度。而有效的密码至少需要满足以下要求：用户不能使用生日、电话号码等别人容易猜出的密码；密码应该输入至少 8 位字符，建议混合使用数字、大写、小写和特殊的字符。另外一种硬件加密锁的方式更为有效：使用一个 USB 硬件设备，里面存放登陆者的认证信息，当登陆时，必须插上钥匙才能进行密码的验证。在企业内部实施 UKey 认证制度，可从物理上阻止未经授权人员进行访问 [3]。

（5）主动安全防御的一体化防护技术。

民机生产系统是一个复杂的工业控制系统，企业在对其部署安全防护之前，需要先进行安全风险评估，充分了解系统的脆弱性和潜在的威胁，有针对性地建立安全防御一体化防护技术，如身份认证、入侵检测等。通过一体化的防护，可以让企业在统一的安全策略下实现完整的安全管理，为企业的运行提供可靠的运行环境，保证安全防护的最大化。以下针对民机生产系统的一体化防护提出一些可行性建议。

在关键网络与其他网络的连接处设置安全网关设备。民机生产系统的网络分为工业网络与公司网络，为了防止公司网络对工业网络入侵的可能，可以设置防火墙控制访问，如图 1 所示；在公司网络上部署入侵检测系统，检测网络中的行为异常；由于工业网络中只有工业通信，且与公司网络被防火墙隔离，所以需要建立严格的访问控制，而在工业网络中部署入侵检测的需求还有待于风险评估的结果。

3.2 建立被动防御策略

（1）数据备份。

数据备份及灾难恢复是信息安全的重要组成部分。理想的备份系统应该是全方位、多层次的，硬件系统备份用来防止硬件系统故障，使用网络存储备份系统和硬件容错相结合的方式，可用来防止软件故障或人为误操作造成的数据逻辑损坏。这种对系统的多重保护措施不仅能防止物理损坏，还能有效地防止逻辑损坏。

数据备份方式按其备份地域一般划分为本地备份和异地备份两种，一是系统的业务数据由于系统或人为误操作造成损坏或丢失后，可及时在生产本地实现数据的恢复；二是发生地域性灾难（地震、火灾、机器毁坏等）时，可及时在本地或异地实现数据及整个系统的灾难恢复。对于大客生产系统而言，无论是哪种数据损坏都是致命的，所以数据备份显得尤为重要 [4]。

（2）维护系统和软件漏洞。

对于 Windows 通用操作系统，在局域网内部署一台微软的 SUS（Software Update Service 软件升级服务器），通过 SUS 可以在局域网中建立一个 Windows 升级服务器，以后局域网中的电脑就可以通过这个服务器来自动升级。

对于专用控制操作系统和第三方应用软件，需要有完整的技术支持，保证在出问题时可以获得帮助 [5]。而对于此大客车间专属的工业应用软件，在开发初期就需要有完整的测试支持，投入使用后依然需要有技术支持团队对相关软件进行维护，从而保证系统运行的可靠性。

（3）加强安全审计。

安全审计作为企业安全管理、信息系统等级保护、风险控制的关键手段，在现代化系统中已不可或缺。审计策略也应该由安全管理机构制定，保证审计的范围能够覆盖到系统的每个用户，不出现盲区就可以最大程度保证系统安全。审计的对象包括用户的行为、系统资源的使用状况、发生的所有事件等，同时审计记录应该也得到保护 [6]。当有安全事件发生时，如果入侵者没有清

除入侵记录，那么通过审查系统日志文件就可以了解入侵过程，从而进行修护和下一步的防护。

（4）建立紧急情况应对策略。

基于网络控制的大客生产线，由于不确定因素而导致的系统问题随时都有可能发生，为了保证经济、声誉、人员损失最小化，制定相应的紧急情况应对策略是非常有必要的。该响应策略需要在业务中断、系统宕机、网络瘫痪等事件触发后快速有效地恢复系统运行，而由于突发事件的不确定性和多样性，应急策略往往需要在弹性和通用性之间寻求平衡点[7]。针对特定的信息安全事件制定相应的通用的应对策略，如在日常维护级别中，可以通过数据冗余来达到存储介质损坏而不丢失数据的目的，设置备用的控制服务器来确保生产线不会停滞太久等[8]。

4 结束语

民机生产系统是现代化工控系统，虽有别于普通 IT 系统，但其信息安全的防范措施与传统网络安全存在较多的共性。本文结合民机生产系统网络结构和安全需求，针对其潜在的威胁，包括人员安全意识、软件漏洞、设备局限性等，提出了相应的安全策略。但是由于安全防范存在的滞后性，所以并不存在能够防范所有安全威胁的策略，企业的信息安全仍需其中的安全部门进一步维护。值得强调的是，建立安全策略与流程是其中很重要的一个环节，用“三分技术，七分管理”来形容工业控制系统信息安全不无道理，所以在企业创建初期设立合理的管理策略是非常有必要的。

参 考 文 献

[1] 张克伟，曹兴强，刘贵阳．烟草工业控制系统安全防护分析与对策．电子测试，2014(2):144-145.

[2] 岳妍瑛，王彬．油田工业控制系统信息安全浅析．自动化博览，2013(3):38-42.

[3] 潘明惠，偏瑞琪，李志民．电力系统信息安全应用研究．中国电力，2001(S):46-49.

[4] 欧阳劲松，丁露．IEC62443 工控网络与系统信息安全标准综述．信息技术与标准化，2012(3):24-27.

[5] 唐文．工业自动化控制系统信息安全研究．计算机安全，2012(4):2-7.

[6] 仇伟．现代化制造企业信息安全及其应对策略．科技创业家，2012(12):128-130.

[7] Holečko P, Krbilová I. IT security aspects of industrial control systems. Advances in Electrical and Electronic Engineering, 2006(5):1336-1376.

[8] Stouffer K, Falco J, Scarfone K. SP800-82 “Guide to industrial control systems (ICS) security”. Gaithersburg: NIST Special Publication, 2011: 55-62.

（责编 深蓝）

（上接第 119 页）

表3 航空企业复合材料制件验收标准应用概况（以层压板制件为例）

公司	质量等级（分区域）	孔隙率要求	检测起始灵敏度当量缺陷 /mm	多个缺陷缺陷尺寸	缺陷间距离限制 /mm
SR	ϕ 6~40mm 9 个等级	5MHz/9.5mm 探头，超声底波衰减不超过 75%	6.3	6.3~38mm	87~100
BE	A 区，关键结构； B 区，梁 / 肋 / 框； C 区，非承力区	A 区 1.0%； B 区 1.5%； C 区 2.0%	6	A 区 < 9mm； B 区 < 12mm； C 区 < 15mm	A 区 > 180； B 区 > 100； C 区 > 100
GN	一级：ϕ 6mm； 二级：ϕ 10mm； 三级：ϕ 12mm	5MHz/9.5mm 探头，超声底波衰减不超过 75%	6	500mm 内累计面积： 一级：10%； 二级：15%； 三级：25%	100
AZ	关键 重要 一般	高应力区 < 5%； 中应力区 < 8%； 低应力区查制件表面	5	零件各异 ϕ 9~30mm	按零件特定间距为 100~300

法和标准的发展。随着飞机复合材料用量的增大，尤其是在翼梁、机身、直升机旋翼、机翼、方向舵等承力结构上的应用，促进了检测标准的进一步精细化，使主承力构件检测要求更加严格，质量分等级、检测区域更加具有针对性。大飞机研制与生产几乎对每一制件都有单独的验收要求。纵观其发展趋势，呈现出如下特点：一是特定的专用型，二是可广泛适用的通用型。有的型号飞机主承力结构处于应力区，其损伤容限与其他型号飞机差别明显，要求严格，尤其在研制早期，对各制件要求针对性强。另外，对主要部件均有特定标准，需在图纸上一一标明，检测程序和操作方法也要具体。普通的标准适用范围小，而通用型标准可用于生产阶段的质量控制、优化产品检验，也可用于在役检测。另外，通用型标准对质量分级、检测分区、单个 / 多个缺陷、缺陷间距限制等都有规范性描述，使用者可“对号入座”，即按照被检件损伤容限和使用寿命，选择标准中对应的质量控制等级和检测评定方法。

参 考 文 献

[1] 张丽华，范玉青．复合材料在飞机上应用评述．航空制造技术，2006(3): 64-66.

[2] 包建文．高效低成本复合材料及其制造技术．北京：国防工业出版社，2012.

（责编 谷雨）