DOI:10.16080/j.issn1671-833x.2010.22.024

数字化制造企业的信息安全体系及实施方案

Information Security System and Executive Plan of Digitization Manufacturing Enterprise

昌河飞机工业(集团)有限责任公司技术管理中心　吴建香

[摘要] 根据数字化制造企业的安全需求特点,系统构建了数字化企业信息安全体系,并将多种安全方案纳入到该体系中。针对数字化企业数据及资料安全问题,提出了一套综合解决方案,该方案实现了身份鉴别、设备集中控制、文档权限管理、文档加密、安全审计,大大提高了企业内部数据及资料的安全性。提出了一种典型数字化企业的信息安全实施方案,保障了内部业务应用系统的信息安全。

关键词:数字化　信息　安全　网络　防火墙　访问控制　备份

[ABSTRACT] Based on the safety requirement characteristics of digitization manufacturing enterprise, security system for digitization enterprise information is built systematically, and many security plans are incorporated into the system. A set of integrated solutions plan is forwarded for digitization enterprise data and information security issues, which achieve figure identification, equipment centralized control, document authority management, document encryption, security audit, and greatly improve the security for the internal data and information of enterprise. A type of information security executive plan for digitization enterprise is presented, which ensures the information security of internal business applications system.

Keywords: Digitalization Information Security Network Firewall Access control Backup

数字化制造企业将信息技术、现代化管理技术和制造技术相结合并应用到企业产品生命周期全过程和企业运行管理的各个环节,实现产品设计制造、企业管理、生产控制过程以及制造装备的数字化和集成化,提升了企业产品开发能力、经营管理水平和生产制造能力,从而提高了企业综合竞争能力。随着企业数字化建设的深入,企业对信息化建设的要求越来越高,建设全面集成的数字化制造企业成为企业信息化工作的目标。

1　信息安全问题分类

在企业信息化工作的开展中,信息安全问题是必须要考虑的首要问题。数字化企业信息安全问题总体上分为信息泄露问题和信息丢失问题。

1.1　信息泄露问题

数字化企业信息系统覆盖面广,不仅涉及到企业内部设计和管理层信息化系统,而且向下延伸到企业生产设备网络化运行系统。可见信息安全涉及人员和环节多,稍有不慎就会出现信息泄露事件,一旦信息泄露将会对企业造成极大危害。

1.2　信息丢失问题

数字化企业信息化程度高,一旦出现信息丢失,将可能影响整个企业的运行,使企业处于瘫痪状态。同时由于对信息的依赖程度高,使得安全问题的“水桶效应”更加明显,单点的安全问题可能会对企业带来很大的危害。

2　安全体系

针对数字化企业的总体信息安全需求,遵循安全性、可行性、效率性、可承担性的设计原则,数字化企业的信息安全体系可从物理安全、网络安全、信息化数据及资料安全、制度约束几方面进行设计。

2.1　物理安全

物理安全的目的是保证数据库服务器、应用服务器、计算机系统、网络交换机、通讯链路以及其他重点生产设备的企业级信息安全,物理安全措施主要包括以下方面。

(1)建立不同安全区域标志实施不同区域隔离。

特别是服务器存放的中心机房、涉及企业级保密数据的单位。具体设计中考虑门禁系统,建立出入审查和登记管理制度,对出入活动进行不间断实时监视记录。

(2)抑制和防止电磁泄漏(即 TEMPEST 技术)。

目前主要防护措施有 2 类:一类是对传导发射的防护,主要采取对电源线和信号线加装性能良好的滤波器,减小传输阻抗和导线间的交叉耦合。另一类是对辐射的防护,这类防护措施又可分为以下 2 种:一是采用各种电磁屏蔽措施,如对设备的金属屏蔽和各种接插件的屏蔽,同时对中心机房的下水管、暖气管和金属门窗进行屏蔽和隔离;二是干扰的防护措施,即在计算机系

统工作的同时，利用干扰装置产生一种与计算机系统辐射相关的伪噪声向空间辐射来掩盖计算机系统的工作频率和信息特征[1]。

2.2 网络安全

2.2.1 网络结构安全

通过层次设计和分区设计实现网络之间的访问控制，网络结构设计时需要对网络地址资源分配、VLAN划分、路由协议选择、QoS配置等方面进行合理规划。通过VPN加密信道保障企业分支机构、合作伙伴与总部之间信息传输的安全性；通过布置防火墙系统加强了网络层的安全性；通过在入口防火墙上布置入侵检测系统动态保护网络；通过布置访问控制系统、基于主机的入侵检测系统，进一步保障关键服务器的安全[2]。

2.2.2 访问控制策略

访问控制是网络安全防范和保护的主要策略，是保证网络安全最重要的核心策略之一，它的主要任务是保证网络资源不被非法使用和非常访问。访问控制也是维护网络系统安全、保护网络资源的重要手段[3]。

访问控制采用防火墙(Firewall)对服务器的网络访问进行控制，同时对重要服务器安装专门的访问控制软件，对登陆操作系统进行身份识别和审计。

各种策略必须相互配合才能真正起到保护作用。

(1)入网访问控制。

入网访问控制为网络访问提供了第一层访问控制。它控制哪些用户能够登录并获取网络资源，用户的入网访问控制可分为3个步骤：用户名的识别与验证、用户口令的识别与验证、用户帐号的默认限制检查。3道关卡中只要任何一关未过，该用户便不能进入该网络。

对网络用户的用户名和口令进行验证是防止非法访问的第一道防线。用户注册时首先输入用户名和口令，服务器将验证所输入的用户名是否合法。如果验证合法，才继续验证用户输入的口令，否则用户将被拒之网络之外。网络管理员可以控制和限制普通用户的帐号使用、访问网络的时间、方式。用户名或用户帐号是所有计算机系统中最基本的安全形式。用户帐号只有系统管理员才能建立。

(2)网络的权限控制。

网络的权限控制是针对网络非法操作所提出的一种安全保护措施。用户和用户组被赋予一定的权限。网络控制用户和用户组可以访问哪些目录、子目录、文件和其他资源。可以指定用户对这些文件、目录、设备能够执行哪些操作。根据访问权限将用户分为以下几类：

a. 特殊用户(即系统管理员)；

b. 一般用户，系统管理员根据他们的实际需要为他们分配操作权限；

c. 审计用户，负责网络的安全控制与资源使用情况的审计。

用户对网络资源的访问权限可以用一个访问控制表来描述。

(3)目录级安全控制。

网络应控制用户对目录、文件、设备的访问。用户在目录一级指定的权限对所有文件和子目录有效，用户还可进一步指定对目录下的子目录和文件的权限。对目录和文件的访问权限一般有8种：系统管理员权限(Supervisor)、读权限(Read)、写权限(Write)、创建权限(Create)、删除权限(Erase)、修改权限(Modify)、文件查找权限(File Scan)、存取控制权限(Access Control)。网络系统管理员为用户指定适当的访问权限，这些访问权限控制着用户对服务器的访问。8种访问权限的有效组合可以让用户有效完成工作，同时又能有效控制用户对服务器资源的访问，从而加强了网络和服务器的安全性。

(4)属性安全控制。

当用文件、目录和网络设备时，网络系统管理员给文件、目录等指定访问属性。属性安全控制可以将给定的属性与网络服务器的文件、目录和网络设备联系起来。属性安全在权限安全的基础上提供更进一步的安全性。网络上的资源都应预先标出一组安全属性。用户对网络资源的访问权限对应一张访问控制表，用以表明用户对网络资源的访问能力。属性设置可以覆盖已经指定的任何受托者指派和有效权限。属性往往能控制以下几个方面的权限：向某个文件写数据、拷贝一个文件、删除目录或文件、查看目录和文件、执行文件、隐含文件、共享、系统属性等。网络的属性可以保护重要的目录和文件，防止用户对目录和文件的误删除、执行修改、显示等。

(5)防火墙控制。

防火墙作为近期发展起来的一种保护计算机网络安全的技术性措施，是一个用以阻止网络中的黑客访问某个机构网络的屏障，也可称之为控制进/出2个方向通信的门槛。在网络边界上通过多级防火墙建立起来的相应网络通信监控系统来隔离内部和外部网络、内网不同区域的访问，对网络中重要网段加以保护，以阻档外部网络的侵入。目前的防火墙主要有以下2种类型[4]。

a. 包过滤防火墙：

包过滤防火墙设置在网络层，可以在路由器上实现包过滤。首先应建立一定数量的信息过滤表，信息过滤表是以其收到的数据包头信息为基础而建成的。信息包头含有数据包源IP地址、目的IP地址、传输协议类

型(TCP、UDP、ICMP 等)、协议源端口号、协议目的端口号、连接请求方向、ICMP 报文类型等。当一个数据包满足过滤表中的规则时,则允许数据包通过,否则禁止通过。这种防火墙可以用于禁止外部不合法用户对内部的访问,也可以用来禁止访问某些服务类型。但包过滤技术不能识别有危险的信息包,无法实施对应用级协议的处理,也无法处理 UDP、RPC 或动态的协议。

b. 代理防火墙:

代理防火墙又称应用层网关级防火墙,由代理服务器和过滤路由器组成,是目前较流行的一种防火墙。它将过滤路由器和软件代理技术结合在一起。过滤路由器负责网络互连,并对数据进行严格选择,然后将筛选过的数据传送给代理服务器。代理服务器起到外部网络申请访问内部网络的中间转接作用,其功能类似于一个数据转发器,主要控制哪些用户能访问哪些服务类型。当外部网络向内部网络申请某种网络服务时,代理服务器接受申请,然后根据其服务类型、服务内容、被服务的对象、服务者申请的时间、申请者的域名范围等来决定是否接受此项服务,如果接受,它就向内部网络转发这项请求。代理防火墙无法快速支持一些新出现的业务(如多媒体)。现要较为流行的代理服务器软件是 Win Gate 和 Proxy Server。

2.2.3 应用层系统安全策略

(1)应用层系统安全一方面需要对应用系统进行检测和修补。

通过扫描软件对重要网段内的所有提供网络服务的设备进行漏洞扫描和修补,在条件具备时扫描范围应该扩大到网络的所有设备。

加强应用层系统安全主要可采取 3 种措施,一是通过基于网络的扫描软件对重要主机系统进行定期漏洞扫描评估,发现漏洞后对系统及时进行修补;二是通过在重要的主机上(如应用服务器、WEB 服务器、数据库服务器等)安装基于主机的实时入侵检测系统防范各类攻击;三是建立基于网络的防病毒系统。

(2)应用层系统安全的另一方面是用户口令的安全策略。

用户口令是用户入网的关键所在。为保证口令的安全性,用户口令不能显示在显示屏上,口令长度应不少于 10 个字符,口令字符最好是数字、字母和其他字符的混合。用户口令应是每用户访问网络所必须提交的"证件"、用户可以修改自己的口令,但系统管理员应控制口令的以下几个方面的限制:最小口令长度、强制修改口令的时间间隔、口令的唯一性、口令过期失效后允许入网的宽限次数。

(3)应用层系统安全的再一方面是设备集中控制策略。

设备集中控制采用基于网络的设备集中控制系统对受限机器的对外复制渠道进行控制。中心控制台接管所有受限机器的系统资源,对受限机器的终端输出设备(USB、软盘、串并口、红外接口等)、网络文件共享进行监管。每个内部员工分配 1 个固定、唯一的 IP 地址,并在网络安全设备中将其与 MAC 地址捆绑起来,则该计算机所产生的所有行为视为该员工的行为。

2.3 信息化数据及资料安全

企业需要存储海量的生产数据信息,更需要保证信息系统的永不停顿以及系统的安全。意外断电、系统或服务器崩溃、用户失误、磁盘损坏甚至数据中心的灾难性丢失都可能造成数据库文件的破坏或丢失。而这些文件往往包含着珍贵的数据,经不得任何损失。数据库管理员必须对此有所准备。在这种情况下,数据库备份占了举足轻重的位置。数据库备份几乎是任何计算机系统中绝对必需的组成部分。

数据备份主要通过双机热备、数据灾难备份、存储磁盘阵列等方式共同组成一套企业级存储服务系统,采用双机热备技术保证重点服务器的不间断运行,采用磁盘阵列技术对重要数据进行实时备份,采用磁带机对重要数据进行灾难备份。再结合各主机系统内含的数据备份程序或各类专业级数据备份软件为网内的各异构系统的计算机系统(包括 UNIX 和 Windows 系统)的关键应用提供数据库的集中式存储与管理,增强稳定性、可用性、安全性,减少由于硬件或其他安全问题带来的损失。企业的核心交换机也采用备份机制。

数据备份系统在工作的时候,所有客户端的数据库备份任务都是由主备份服务器按策略自动发起。针对不同客户端服务器上需要备份数据库的不同,系统管理员在主备份服务器上制定每台客户端服务器不同的数据库备份运行方式,将启动的时间,备份任务发生的时间间隔等都设置好。整个备份网络的存储设备集中连接到主备份服务器上。存储设备里的存储介质(磁带)也都由主备份服务器统一分配使用,备份数据流将通过网络等方式传到主服务器上并最终写入存储设备。目前使用的数据库备份方案是完全备份和增量备份相结合的备份方式,通过自动化带库及集中的运行管理。定期工作人员通过使用备份软件对写入磁带的数据库数据进行校验以保证数据的完整性及有效性。

2.4 制度约束

无论信息泄露的表现形式如何,这类安全违规事件追究到最后大部分都是由企业内部人员所造成的。因此,解决来自企业内部的信息安全问题应以人为核心要解决以上的企业内部信息安全问题,一方面要加强技术

手段，另一方面要完善企业关于信息安全问题的相关管理制度，加强对员工安全意识的培训和安全行为的管理。

在网络安全中，除了采用技术措施之外，还应加强网络的安全管理，制定有关网络操作使用规程和人员出入机房管理制度；制定网络系统的维护制度和应急措施等规章制度，这对于确保网络的安全、可靠地运行，将起到非常有效的作用。

3 结束语

数字化化制造企业由于信息系统覆盖面更广、集成度更高，解决面临的信息安全问题显得更为棘手。要解决企业内部信息安全问题，一方面要加强技术手段，另一方面要完善企业关于信息安全问题的相关管理制度，加强对员工安全意识的培训和安全行为的管理。在数字化企业信息安全模型中，通过采取合理的安全策略、建立专门的安全组织机构、完善安全制度来建立保障数字化企业信息安全的长效机制；通过加强定期的安全评估，发现信息系统中潜在的安全漏洞，以便及时弥补和修复；通过安全审计工作，及时发现潜在的安全事件，以便及时进行处理，同时对安全违规行为起到威慑作用，减少安全违规事件。

参 考 文 献

[1] 张杰，沈精虎 .Internet/Intranet 环境下的工程设计 . 北京：人民邮电出版社，2000.

[2] 冯登国 . 计算机通信网络安全 . 北京：清华大学出版社，2001.

[3] 唐正军 . 网络入侵检测系统的设计与实现 . 北京：电子工业出版社，2002.

[4] 唐博 . Windows Internet 黑客防范与安全策略 . 北京：清华大学出版社，2002.

（责编 良辰）

（上转第 122 页）

的制造精度并选用较紧的配合。

设计固定导套时，主要应当从上述 2 个方面入手，来提高钻孔的位置精度。其中导套的长度 l_1、导套至工件端面的距离 l_2 及钻孔的直径 d 和钻孔深度 l 的关系如表 1 所示。

表1 钻孔时l_1和l_2同d的关系式

l_1	$l<d$ 时	$(0.5\sim1.8)d$
	$l>2d$ 时	$(1.2\sim2)d$
l_1	钻钢	$(0.5\sim1.8)d$
	钻铸铁	$(0.5\sim1.8)d$

3 夹具设计总体方案

定位方式：采用一面两销的定位方式，详见图 5。

夹紧方式：采用 FESTO 公司的摆角气缸气压夹紧，结构紧凑，夹紧可靠。

导向装置：为保证刀具相对于工件的正确位置、提高刀具系统的支承刚性，在夹具上设置了钻模套（图 7），夹具的外观如图 8 所示。

4 结束语

该套夹具经使用后检测工件得知，不仅符合计算分析结果和使用要求，还具有以下特点：结构简单，对夹具加工精度要求不十分高，动作灵活可靠；夹紧可靠，刚性好；利用机床现有动力源，对机床主体结构无影响，缩短制造周期，成本低；为夹具的结构设计提供参考。

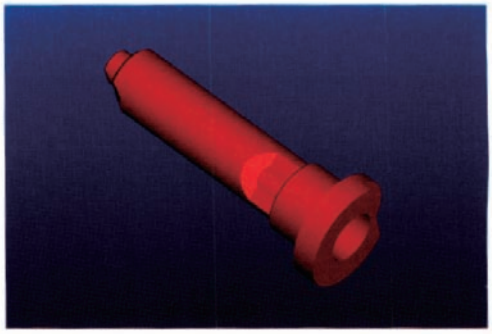
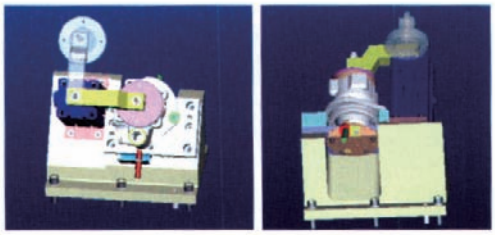


图7 钻模套

Fig.7 Oriented device



（a）前面 （b）后面

图8 夹具简图

Fig.8 Diagram of Clamp

参 考 文 献

[1] 龚定安，赵孝昶，高化 . 机床夹具设计 . 西安：西安交通大学出版社，2000.

[2] 组合机床讲义，《组合机床》编写小组 . 北京：国防工业出版社，1972.

[3] 组合机床设计手册 . 大连组合机床研究所，1998.

[4] 金振华 . 组合机床及其调整与使用 . 北京：机械工业出版社，1984.

（责编 侧卫）