doi: 10.7690/bgzdh.2020.08.007

兵器企业商密网规划思考

胡艳岭，沙金龙，姜鹏程
（中国兵器工业第二〇八研究所信息中心，北京 102202）

摘要：针对兵器行业战略转型发展需要，结合兵器企业基础网络现状及特点，系统分析企业在科研生产、销售经营和公共管理等方面的商密网建设需求。综合考虑发展趋势与需求导向，围绕业务剥离、系统定级、架构设计，提出规划建设要点及实施策略，可为兵器企业以及同类型军工企业信息化规划提供指导。

关键词：商密网；规划；等级保护
中图分类号：TJ0　　**文献标志码：**A

Thoughts on Planning of Business Secret Network of Weapon Enterprises

Hu Yanling, Sha Jinlong, Jiang Pengcheng
(*Information Center*, *No*. 208 *Research Institute of China Ordnance Industries*, *Beijing* 102202, *China*)

Abstract: Aims at the strategic transformation and development needs of weapons industry, combined with the current situation and characteristics of the basic network of ordnance enterprises, systematic analysis of the network construction needs of enterprises in scientific research, production, sales management, public management, etc. Considering the development trend and demand orientation comprehensively, puts forward the key points of planning and construction and implementation strategies around business separation, system grading and architecture design. It can provide guidance for information planning of weapon enterprises and the same type of military enterprises.

Keywords: business secret network; planning; classified protection

0　引言

商密网是承载企业商业秘密的网络环境。商业秘密是市场环境下，企业经营者和技术人员知识与智慧的结晶，产生、形成并应用于企业科研、生产、经营、管理等全过程，是企业重要的无形资产。随着 IT 技术发展，商业秘密的承载形式已经从纸介质、人脑中，演变为以数字化的形式存在于网络中，即商密网中。

近年来，随着全军实战化军事训练的大规模和从难从严开展，兵器行业作为各军兵种基础装备的供方，面临空前的发展机遇和严峻挑战。同时，伴随军民融合加快发展的态势，兵器行业作为准入门槛相对较低的军工行业，具备相关技术积累的民营高科技企业大量涌入，给传统兵器企业发展带来了前所未有的竞争压力。为了应对这些变化发展，兵器企业从传统科研型单位向科研产业型单位转型，正在打破壁垒、创建平台、建立机制，以开放包容的姿态，与市场充分接轨。IT 基础设施建设，是支撑兵器行业与市场接轨的基础工程。多数兵器企业原有“涉密网络为主+互联网集中接入”的网络基础设备及配套运行管理模式，已经无法适应当前形势变化，急需针对行业发展和企业转型需求进行商密网及配套基础设施的规划与建设。

1　业务驱动下的兵器企业网络建设情况

长期的军品科研背景下，兵器企业 IT 系统主要存在以下网络形式：1) 涉密信息系统，是兵器企业日常业务运行的主要 IT 运行模式。随着各企业信息化发展水平的不断提升，主要业务实现信息化的同时，按照国家分级保护对应等级标准，针对网络和应用，进行了 10 余年的安全防护体系建设及升级，基本涵盖了身份鉴别、访问控制、终端管理、主机审计、漏洞扫描、病毒防护、接入控制、输出监控和安全审计等方面，保障了兵器企业业务安全有效开展。2) 专用工控系统，是兵器企业在提升专业能力方面的 IT 运行模式，主要集中在生产、测试等方面。以商密局域网为支撑进行建设和使用，因设备的特殊性，一般按照等保标准建设，但在定级审查备案、安全防护体系建设等方面相对滞后。随着国家对信息安全的重视程度不断提升，以及等级保护 2.0 标准[1]的出台，在定级审查备案、安全防护建设

收稿日期：2020-03-20；**修回日期：**2020-04-06
作者简介：胡艳岭（1982—），女，河南人，硕士，高级工程师，从事数字化技术研究与应用、信息化规划与建设研究。E-mail: oil1999@163.com。

等方面有了契合实际的参照，兵器企业可望在近几年内逐步完善顶层架构并付诸实施。3) 互联网应用系统，是兵器企业与其他非涉密单位间信息交换的主要渠道，且根据国家针对军工企业涉密单位有关互联网接入的要求，实行最小化原则，对接入点数量进行了控制。随着兵器企业与民营企业间的共同合作交流迅速增多，以及自身非密公共管理业务从涉密网络中的剥离，兵器企业急需开展基于互联业务的商密网架构设计并及早落地。

2　商密网建设的必要性分析

从网络建设情况分析中可以看出，在专用工控系统和互联网应用的推动下，兵器企业商密网建设需求日趋明显。同时，从国内大背景来看，随着智能制造技术发展，工业和信息化深度融合成为传统制造业的发展方向[2]。兵器行业作为传统制造业的一员，信息化发展较之民口企业差距较大，但随着军工融合的加速，数字化、智能化广泛应用，物联网、数字孪生、大数据、云服务、云平台等技术正向兵器装备的科研试制、生产物流、销售经营、公共管理等业务领域迁移渗透。各兵器企业也在谋求自身发展的过程中，不断催生出新的更为便捷和高效的工作模式，以市场化融合为导向的新一轮 IT 基础设施规划建设需求逐渐显现。兵器企业涉及科研试制、生产交付、测试试验、供应管理、销售经营和综合管理等主要领域。笔者从业务板块共性需求出发，结合关键技术发展趋势，分析兵器企业商密网建设需求。

2.1　工业互联技术推动企业技术革新

工业互联技术是新一代信息技术与工业经济深度融合的全新产业生态[2]，在工业感知、工业通信、工业控制和大数据等技术驱动下，生产、测试、交付过程的网络化和工业设备的互联化成为提升产业创新能力的重要赋能手段。将技术人员、专用设备、过程数据和管理技术等全面互联，构建一种新型工业生产制造和服务运行模式，通过网络中的数据流推动供应链、服务链、物流链等在企业内外部的拉通，实现企业内、上下游企业间生产资源全局配置与管理。

近年来，在国家的扶持下，兵器企业在业务上虽有不同或侧重，但在科研试制、生产交付和测试试验等业务板块，引进了中试、生产、总装、测试和试验等专用设备，建立了专业的生产线、装配线和总装线等。随着工业互联技术逐步成熟，以及配套安全防护设备商用化，借助数控设备组网、测试设备组网、配送设备组网等一体化解决方案的应用，可迅速提升企业生产效率和产能。

2.2　云计算技术刺激企业管理提升

云计算技术凭借其易用、灵活、高可用和易扩展等特点，成为 IT 技术应用的主流方向之一[3]。越来越多的企业开始引入云计算，将传统的 IT 架构逐步转变成云计算架构，国内 IT 产品供应商的主流产品都在向云服务模式转变，涌现出了公有云、私有云、混合云等各种各样的云服务产品和解决方案。华为等企业更是推出了从芯片到服务器到云平台的全栈式云服务解决方案。云服务模式的蜂拥而至加速了企业关键应用系统上云的节奏，同时，海量的移动应用也推动了云计算架构在不同客户不同场景下瞬息万变的业务应用扩展。当前，互联网用户中，近三成的企业已经开始采用云服务模式，企业业务上云已经成为不可逆转的趋势。

兵器企业因涉密业务属性，长期以来，以涉密网络架构为主进行应用系统的建设与部署。其中，不乏基于多重考虑，将处理非涉密业务的信息系统部署在涉密网络中的现象。这种物理隔离的网络形式，极大地限制了业务效率的进一步提升，尤其是在与上下游的开放型企业合作过程中，限制了供应商管理、销售经营及综合办公效率，远远落后于民口企业在 IT 应用方面的发展，影响竞争力提升。随着移动办公、网络协同、资源共享的需求快速增长，改变现有主流网络模式，系统性地建设商密网，剥离原有的非涉密业务应用，进行移动化及云化改造，将会成为未来几年兵器企业信息化建设的重点之一[4]。

3　兵器企业商密网规划与建设要点

通过对兵器行业商密网建设需求分析可以看出，内外部形势均指向了商密网规划与建设。如何使企业商密网规划与建设的方向、重点、步骤更科学合理，又在资金投入、人员投入、资源整合、资源共享等方面实现最优配置，需要从业务剥离、安全防护定级、体系建立与运营等 3 方面理清思路。

3.1　业务剥离

现有涉密信息中有非密业务剥离到商密网，关键是在准确定密定级的前提下，把握好拟剥离业务与涉密应用间信息交换时效性对业务的影响程度，

以及剥离后业务效率提高带来的收益与投资成本的平衡。笔者以兵器行业业务领域覆盖相对较多的某研究所为例，进行商密业务剥离分析。该研究所涉及装备研发、试制、试验、测试、生产、销售、服务等业务板块。近年来，产业领域快速拓展，随之而来的是生产任务总量、经营规模急剧增加，业务协同已经从设计制造一体化、设计仿真一体化、设计测试一体化等逐步拓展到了客户关系管理、外部供应商管理、内外部物流管理、生产交付管控等生产交付和对外经营的多个方面，新的产业增值点已经给企业商密网规划提供了明确输入，同时随着无线互联技术、移动办公方式的普及应用，对业务需求的实现方式也提出要求。如表 1 所示，根据研究所战略方向，从业务维度进行了需求梳理。

表 1 某兵器研究所商密网建设需求分析

领域	业务需求	IT 应用	网络类型
科研试制	情报查询、检索	各类智库、各类知识服务平台	互联网
	业务交流与对接	互联网邮件系统	互联网+应用
	试制设备组网管理	DNC、MDC 等	工控网-局域网
	测试设备组网管理	测试设备管理平台	工控网-局域网
生产物流	制造-财务-库房拉通管理；批产订单到交付全过程管理；供应链管理、制造资源管理、生产过程管理、精准交付管理等	ERP、财务、WMS、供应商管理等	商密网-局域网+应用
销售经营	产品销售	产品销售服务平台	互联网+应用、APP
	新媒体	新媒体平台	互联网+网站、公众号
	测试经营	测试经营管理平台	互联网+应用、APP
公共管理	移动办公	移动办公平台	互联网+应用、APP
	对外宣传	宣传平台	互联网+门户、公众号
	人力资源管理(招聘等)	HR 平台	互联网+应用、APP
	集团业务对接	集团专网应用	集团专网+应用

科研领域，依据承担任务类型，将仍以开展涉密网络为主支撑业务，但考虑到国内外情报信息以及各类高端智库对企业战略调整、技术创新等的影响，可考虑引入高端权威的知识网络平台，并进行相关商密网络基础设施的改造建设。该所已经实现了数控机床组网应用，设计制造一体化对研制数据的实时性要求，则须在做好机床网络安全防护建设的同时，与涉密网络联接。随着工控信息安全设备的商用化，测试设备组网将会成为测试效率提升的突破口，可择机规划测试专网的建设并捋顺一体化测试思路。生产物流领域，面向精准高效交付的基础管理能力提升是整个生产网络建设的巨大驱动力，目前已经建成的专业化生产线以及其设备的通信方式，将作为生产网络建设的考虑因素，以现有标准建设的网络很难适应精准高效生产交付的发展趋势；因此，生产网络需要在准确定密定级的基础上，大胆探索新的安全防护方式，同时理顺 BOM 转化、财务、库房等业务对接方式，提高管理效率。销售经营领域，在产品销售、特色经营、测试经营和轻兵器新媒体等方面，正在尝试适合自身当前发展的 IT 平台或应用，整合销售经营平台之下的网络平台，将有利于网络安全的统一管理和一致性管理。公共管理方面，在业务需求明确的基础上，优先引用成熟商用 APP 应用，可适度降低投入成本和运维费用。

分析结果显示：生产、物流、测试等业务板块因其信息资源敏感性和业务应用系统定制化程度高等特点，从自建的角度进行商密网络的规划更符合研究所自身业务特点和监管要求；销售、经营、公共管理、供方管理等业务板块以商用 IT 系统、APP 应用为主，在资源和业务整合的基础上，可探索云服务的方式委托建设及运维管理。商密网规划的初步构想如图 1 所示。

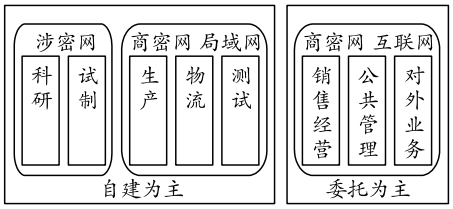

图 1 兵器企业商密网规划

3.2 系统定级

定级是所有商密网络建设的起始点，影响到架构设计、防护体系设计、运行维护方式和资金投入，是商密网规划和建设的关键点之一。定级工作包括确定定级对象、初步定级、专家评审、主管部门审核和公安机关备案审查 5 个环节[5]。备案后将直接纳入公安机关监管范围，是公安部门对网络运营单

位的监管重点。

兵器企业商密网定级的对象一般主要包括科技情报网、生产/测试设备专网、生产物流网、销售经营网和公共管理网 5 类。对其进行系统定级时，可参考 GAT1389－2017《信息安全技术 网络安全等级保护定级指南》进行定级，需要明确受侵害的客体以及对客体的侵害程度。首先，这些对象受到破坏时，其所侵害的客体主要涉及 2 类：1) 侵害法人的合法权益；2) 侵害社会秩序，即影响兵器行业的科研、生产秩序。其次，需要从业务信息安全和系统服务安全 2 个维度进行客体受侵害程度的初定[5](如表 2 所示)，且采取孰高原则。如图 2 所示，分别从业务信息安全角度和系统服务安全角度，对兵器企业主要定级对象受侵害的客体和侵害程度进行分类。生产/测试设备专网、生产物流专网的业务信息安全程度初定在三级为合适；销售经营、公共管理类业务从业务信息范围初定二级为宜。定级的合理性须由企业定密责任部门初定后，经专家评审并报主管部门审核通过后方可作为建设依据。

表 2　业务信息安全和系统服务安全等级对应

受侵害的客体	对客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	一级	二级	三级
社会秩序、公共利益	二级	三级	四级
国家安全	三级	四级	五级

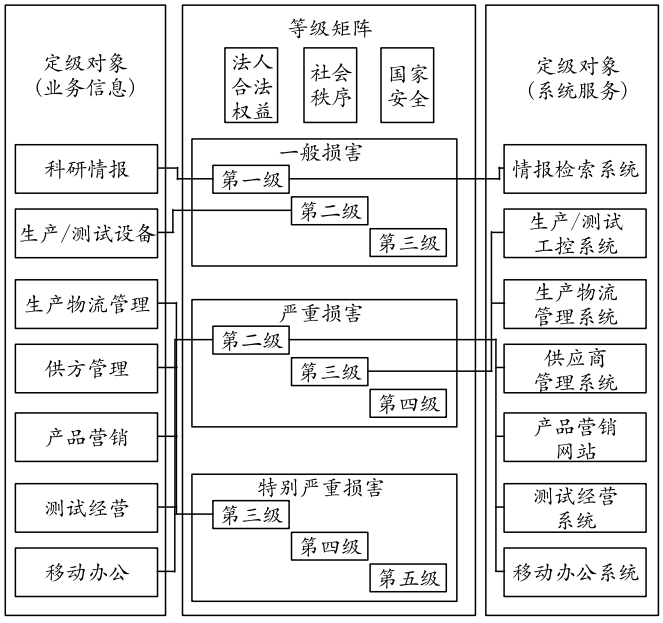

图 2　兵器企业主要业务信息与系统服务安全等级初步划分

3.3　架构设计

对典型兵器研究所业务应用需求分析结果显示：架构设计时，既要考虑引入无线设备和非/低定制化应用的情况，又要考虑移动互联和高定制化应用的情况；既要兼顾高安全性，又要兼顾经济性；既要考虑合理适度冗余，又要具备快速扩展能力。我国网络安全等级保护制度 2.0 系列标准中的《信息安全技术 网络安全等级保护安全设计技术要求》，明确了包含云计算、移动互联、物联网和工业控制等在内的主要网络环境设计的技术要求，可以作为指导兵器企业开展商密网网络架构设计的依据[6-8]。在网络架构设计时，可在对业务信息安全合理定级的基础上，对所承载业务应用按照等级进行分类。针对二级及以下级别系统，可采用公有云为基础的网络架构；针对三级及以上级别系统，可采用私有云为基础的网络架构，进行如图 3 所示的网络层、平台层、应用层和安全防护体系整体设计，以降低 IT 采购成本、推动 IT 架构敏捷，为应用快速拓展预留一定空间。

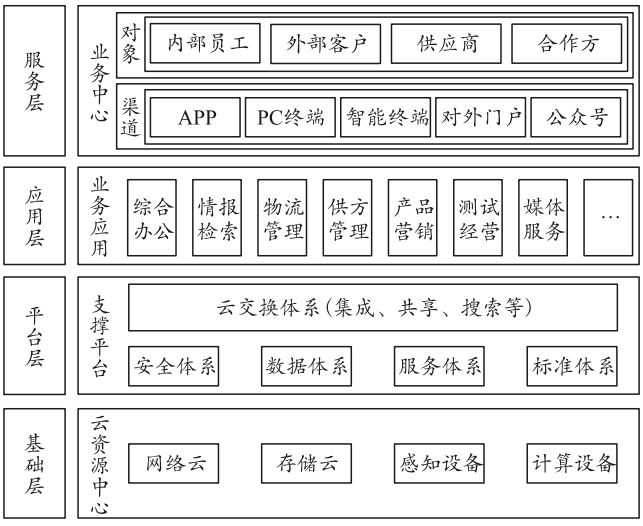

图 3　兵器企业商密应用服务平台架构

4　结束语

笔者以支撑兵器企业战略转型为切入点，对兵器企业科研试制、生产物流、销售经营、公共管理等主要商密业务需求进行了全面梳理，重点分析了等级保护制度 2.0 标准下，兵器企业商密网规划与建设中业务剥离、系统定级、架构设计等方面的技术策略，可为兵器企业十四五信息化规划提供支撑。

参考文献：

[1] 公安部网络安全等级保护中心. 网络安全等级保护制度 2. 0 标准正式发布[S]. 2019.

[2] 何积丰. 从工业互联网到工业软件服务[OL]. 科技创新咨询平台微信公众号, 2019.

[3] 廖飞, 陈捷, 肖云峰. 云计算安全架构及防护机制研究[J]. 通信技术, 2019, 52(10): 2472−2482.
[4] 习阳, 李凯, 王潇. 军工行业工业控制系统信息安全风险与对策[J]. 兵工自动化, 2019, 38(9): 13−15.
[5] 李明, 曲洁. 《信息系统安全等级保护定级指南》修订要点解析[J]. 信息网络安全 2016(S1): 19−21.
[6] 马力, 祝国邦, 陆磊. 《网络安全等级保护基本要求》(GB/T 22239−2019) 标准解读[J]. 信息网络安全, 2019(2): 77−84.
[7] 国家市场监督管理总局, 中国国家标准化管理委员会. 信息安全技术 网络安全等级保护基本要求: GB/T 22239−2019[S]. 北京: 中国标准出版社, 2019.
[8] 国家市场监督管理总局, 中国国家标准化管理委员会. 信息安全技术 网络安全等级保护安全设计技术要求: GB/T 25070−2019[S]. 北京: 中国标准出版社, 2019.

****

（上接第 21 页）

[10] ZHAO H P, FU X G, GAO M G, et al. Research on the visibility of low-orbit debris using space-borne radar[J]. IET Radar, Sonar & Navigation, 2015, 9(1): 31−37.
[11] OLIVER M, EBERHARD G. 卫星轨道−模型、方法和应用[M]. 北京: 国防工业出版社, 2012: 34−35.
[12] MERRILL I. Skolnik. 雷达手册 [M]. 3 版. 北京: 电子工业出版社, 2010: 1069.
[13] Wikipedia. North American Aerospace Defense Command [OL]. (2018−07−09)[2019−10−25]. https://en.wikipedia.org/wiki/North_American_Aerospace_Defense_Command.
[14] 刘兴. 防空防天信息系统及其一体化技术[M]. 北京: 国防工业出版社, 2009: 81−90.
[15] Wikipedia. Boeing E-3 Sentry [OL]. (2018−06−01)[2019−10−25]. https: // en. wikipedia. org/ wiki/ Talk: Boeing_E-3_Sentry.
[16] 王群. 美国新一代导弹预警卫星系统及其能力分析[J]. 国防科技, 2012(2): 7−12.

****

（上接第 31 页）

参考文献:

[1] 刘佩. 空战机动飞行仿真研究[C]. 中国自动化学会控制理论专业委员会, 第 37 届中国控制会议论文集, 中国自动化学会控制理论专业委员会: 中国自动化学会控制理论专业委员会, 2018: 5.
[2] 陈向, 王维嘉, 魏文领, 等. 基于蒙特卡罗搜索树的自动飞行机动[C]//2016 年航空科学与技术全国博士生学术论坛, 西安: 西北工业大学研究生院, 2016.
[3] 林清, 梁争争, 许少尉. 基于自主可控的机载嵌入式计算机现状与展望[J]. 航空计算技术, 2018(5): 2−4.
[4] 牛文生, 王乐. 机载计算技术的新进展[J]. 航空科学技术, 2012(4): 1−4.
[5] "Nvidia Workstation Products" [Z]. Nvidia.com.Retrieved October 2, 2007.
[6] 薛杨, 孙永荣, 赵科东, 等. 基准地图测绘下的视觉导航算法[J]. 兵工自动化, 2019, 38(10): 22−27.
[7] LIU Y, JIAO S, WU W, et al. GPU accelerated fast FEM deformation simulation[C]//IEEE Asia Pacific Conference on Circuits & Systems. IEEE, 2008.
[8] PIRJAN A. Improving Software Performance in the Compute Unified Device Architecture[J]. Informatica Economica, 2010, 14(4): 2−3.
[9] CHU A, FU C W, HANSON A, et al. GL4D: A GPU-based Architecture for Interactive 4D Visualization[J]. IEEE Transactions on Visualization & Computer Graphics, 2009, 15(6): 1587−1594.