doi: 10.7690/bgzdh.2016.05.006

风险理论在军工保密管理领域的应用

赵宝强
（中国飞行试验研究院保密办，西安 710089）

摘要：为主动防御，有针对性地防范泄密、窃密事件的发生，确保国家秘密安全，对风险理论在某军工单位保密管理领域的应用进行研究。从风险的识别、评估、分析、应对等环节全生命周期展现了保密风险的管控过程，列出了国家安全和利益价值、泄密风险来源和保密管理脆弱性等保密风险识别时应考虑的因素，给出了具有可操作性的分析评判标准及评估公式。应用结果表明：该研究具有一定的普遍性，对开拓军工保密管理思路具有较大的参考价值。

关键词：保密管理；风险管理；保密风险；军工
中图分类号：TJ03　　**文献标志码**：A

Application of Risk Theory in Field of Military Industrial Secrecy Management

Zhao Baoqiang
(*Security Management Office*, *Chinese Flight Test Establishment*, *Xi'an* 710089, *China*)

Abstract: As the active defense, for to prevent leak and stealing state secrets, ensure the security of state secrets, in this paper, the theory of risk in the field of military industrial secrecy management is studied. From risk identification, assessment, analysis, response and other aspects, the whole life cycle of security risk management and control processes are shown in this paper. The paper lists the national security and interests, the source of the risk of secrete leakage and the weakness of security management and other factors that should be considered in the identification of the security risks, the operable analysis and judgment criteria and evaluation formula are introduced. The application results show that this research has a certain universality, and has a great reference value for the development of military industrial security management ideas.

Keywords: security management; risk management; security risk; military industry

0　引言

风险是客观存在的，但在特定条件下是具有一定规律性的；因此，当不能或难以完全消除风险时，将风险影响控制在可接受的程度内就成为人们在特定条件下的最佳选择。风险管理就是系统识别、评估、分析和控制风险因素的过程[1]。

保密就是保护、严守秘密[2]，使之不被泄漏。保密是军工单位永恒的主题，关乎军工人的个人前途和家庭幸福，关乎单位的发展，关乎武器装备的威慑力，关乎军队的战斗力，关乎战争的成败，关乎国家利益。根据涉及内容的不同，秘密可分为国家秘密、工作秘密、商业秘密和个人隐私 4 类[3]。笔者所说的保密，是就保守国家秘密而言的，是指为维护国家安全和利益，将国家秘密控制在一定范围和时间内，防止泄露或被非法利用，由专门的组织和机构实施的活动[4]。

基于此，笔者通过科学、合理地利用风险理论和方法，对军工单位保密管理过程中存在的风险、不确定性因素进行有效识别和评估，并将产生的结果控制和处置在预期可接受的范围内。其目的就是主动防御，有针对性地防范泄密、窃密事件的发生，确保国家秘密安全。开展保密风险管理的研究与实践，意味着不再是被动地应对保密风险事件的发生，而是主动自觉地掌握和管理风险，通过逐步对风险的有效掌控和管理措施的不断完善，使员工在日常工作中积极主动地认识风险和把握风险，以最小的成本使泄密风险控制在可接受的水平，以最合理的代价获得最大的保密安全保障，杜绝失泄密事件和重大保密违规行为的发生。

1　研究方法

如图 1，笔者采用的研究方法分为以下环节。

1) 风险规划，包括可能性、危害性的评估标准以及风险等级的划分标准。风险规划应强调合理性和科学性。

2) 风险识别，包括国家安全和利益价值识别、泄密风险源识别和保密管理脆弱性识别 3 方面的内容，其中国家安全和利益价值是识别是否涉及国家秘密的前提，泄密风险源是具体业务中可能导致国

收稿日期：2016-01-13；修回日期：2016-03-09
作者简介：赵宝强(1970—)，男，陕西人，硕士，高级工程师，从事信息安全及企业信息化研究。

家秘密泄露的环节和风险点，保密管理脆弱性是保密管理制度中不完善或难以监管的之处。风险识别应强调全面性、准确性和前瞻性。

3) 风险分析与风险评估，包括判断风险发生概率、风险发生造成的危害，并以此来确定风险的等级；在进行保密管理风险等级评估时，笔者采用了以下公式：

$$R=P\times S; \tag{1}$$

$$P=\text{Round}(\sqrt{P_1\times P_2},0); \tag{2}$$

$$S=\text{Round}(\sqrt{S_1\times S_2},0)。 \tag{3}$$

其中：R 为风险等级估值；P 为可能性综合分析估值(P_1 为行为可能性估值，P_2 为行为反复性分析估值，P 为对 P_1、P_2 乘积的平方根取整)；S 为危害性综合分析估值(S_1 为危害程度估值，S_2 为影响范围估值，S 为对 S_1、S_2 乘积的平方根取整)。P_1、P_2 和 S_1、S_2 的取值均为 1～5 之间(含)的整数。风险分析和评估应强调针对性、精确性。

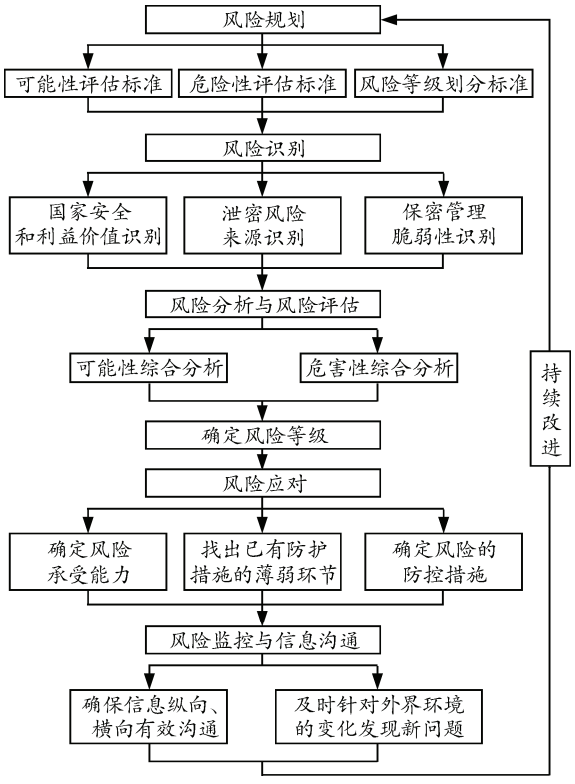

图 1　保密风险管理步骤示意图

4) 风险应对，包含确定风险的承受能力、找出已有防护措施的薄弱环节和确定风险的防控措施 3 个方面的内容。风险应强调有效性。

5) 风险监控与信息沟通，包括确保信息有效沟通、针对外部环境因素的变化发现新问题 2 方面的内容。风险监控与信息沟通应强调充分性。

6) 持续改进，是在迭代过程中对以上各个环节的不断优化和完善。持续改进应强调长效性。

2　保密风险管理研究

2.1　保密风险规划

为了深入开展保密风险理论的研究应用，笔者在中航工业试飞中心下属某单位开展了试点工作。该单位具有武器装备科研生产二级保密资质，有一定的保密管理基础，结合其保密管理实际，笔者确定了以下保密风险管理目标：

1) 构建以保密领导小组为决策机构，保密管理部门为核心，各部门为支撑的组织架构；

2) 建立保密风险管理流程和保密风险数据库，实现对保密风险管理的动态管控；

3) 将保密要求融入到具体的业务流程之中，不断优化保密管理流程、完善保密管理制度，形成保密风险管理长效机制。

2.2　风险评估指标与等级划分

对于公式 (2) 中 P 的取值，笔者从 2 个维度进行了评估标准的设计，即行为可能性维度和行为反复性维度，详见表 1。

表 1　保密管理风险可能性分值评估标准

可能性综合分析	行为可能性(P_1)	行为反复性(P_2)
1	基本不会发生	一年可能发生一次
2	发生的可能性较低	一季度可能发生一次
3	发生的可能性一般	每月可能发生一次
4	发生的可能性较高	每旬可能发生一次
5	发生的可能性很高	每旬可能发生多次

注：可能性分析应基于现有制度、人员素质、技术保障条件下。

对于式 (3) 中 S 的取值，笔者也从 2 个维度进行了评估标准的设计，即危害程度维度和影响范围维度，详见表 2。

表 2　保密管理风险危害程度评估标准

危害程度综合分析	危害程度(P_1)	影响范围(P_2)
1	一般扣分项，扣分在 2 分以内(含)。	部门内
2	一般扣分项，扣分在 5 分以内(含)。	单位内
3	A. 一般扣分项，扣 5～10 分(含 10 分)； B. 重点扣分项，扣分在 5 分以内(含)； C. 存在较大泄密隐患。	区域内
4	A. 一般扣分项，扣 10～15 分(含 15 分)； B. 重点扣分项，扣分在 5 分以上； C. 存在重大泄密隐患。	行业内
5	A. 一般或重点扣分项，累计分数超过 15 分； B. 中止项； C. 发生印证性或其他泄密事件。	全国

对识别出来的保密风险，按照式 (1) 计算出来的 R 值，笔者根据数值大小将保密风险划分为 4 个等级(参见表 3)。

表3 保密风险等级的划分标准

风险等级	风险说明	计算数值
A级(小)	可以接受	1～5
B级(较大)	有控制接受	6～10
C级(大)	不期望发	11～20
D级(重大)	不能接受	20～25

3 保密管理风险应用

3.1 风险识别

试点选定的单位曾在2014年梳理出了20多个保密管理的风险，但未系统性地按照风险理论开展相应的评估工作，也未针对性地制定相应的控制措施。2015年5月下旬，笔者与其保密管理部门一起确定了本次工作的目标，设计了评估标准，较为系统地开展了保密风险管理工作。

同年5月底，笔者对该单位的保密管理人员(包括各部门保密员和主管保密的领导)进行了风险理论培训；6月初，结合全国每年的“保密月”活动，笔者在该单位发布了保密管理风险可能性分值评估标准和风险危害程度评估标准，同时制定了统一的填报表格以便于事后统计汇总，并给出了相应的填报案例以方便参照填写；该单位各部门通过全面梳理各自的业务流程，找出了每个业务环节中的保密管理风险；6月中旬，笔者对回收到的20多个部门的保密管理风险源调查问卷进行了汇总分析，对相近风险进行归一化处理后，共形成178个保密管理风险。

依据《军工单位保密资格审查认证工作指导手册》中的相关要求，笔者又将这些风险源划分为：定密管理、涉密人员管理、涉密载体管理、要害部门部位管理、计算机和信息系统管理、通信及办公自动化管理、宣传报道管理、涉密会议管理、外场试验管理、协作配套管理、保密检查共11大类[5]，分类后分别占总数的比例参见表4和图2。

表4 风险分类统计

序号	类别	类别编号	风险数量	所占比例/%
1	定密管理	A	3	2
2	涉密人员管理	B	35	19
3	涉密载体管理	C	39	22
4	要害部门部位管理	D	18	10
5	计算机和信息系统管理	E	48	27
6	通信及办公自动化管理	F	3	2
7	宣传报道管理	G	5	3
8	涉密会议管理	H	5	3
9	外场试验管理	I	13	7
10	协作配套管理	J	7	4
11	保密检查	K	2	1
	合计		178	100

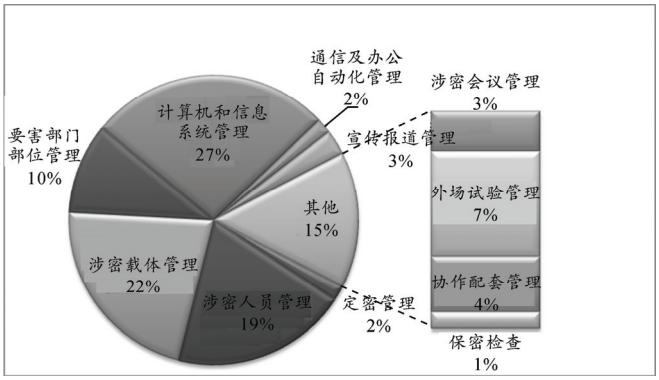

图2 不同类别风险所占比例

对比后笔者发现，计算机和信息系统管理类、涉密载体管理、涉密人员管理、要害部门部位和外场试验管理等6个面方面存在的问题占了全部风险的85%，统计结果也基本与军工单位保密资格审查认证过程中的主要扣分项以及日常保密检查中的薄弱环节相一致，这6个方面同时也是保密管理的难点和重点。

3.2 风险评估

为了更有针对性地协助单位对识别出来的风险进行管控，笔者又对识别出来的风险进行统计分析。笔者以可能性P为横轴、以危害性S为纵轴，将所有的保密管理风险按其危害性评估取值和可能性评估取值进行分布区取点(参见图3)，图中各点右边数值的含义为：可能性取值和危害性取值，中间以逗号隔开。笔者将保密管理的重点放在图3中标有A、B、C、E、F、I、J、K、N、O的10类风险上。

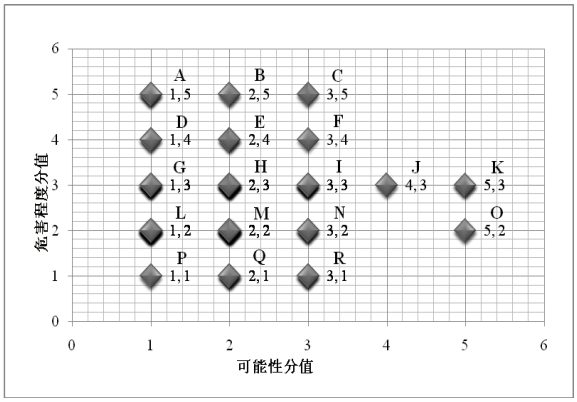

图3 保密管理风险分布图

经统计，以上10类风险共有35个，笔者又根据风险整改的迫切性[6]、投入费用大小以及难易程度对这些风险的行了排序。下面选取排名最前的10个风险进行详细说明(参见表5)，表5中的风险编号首位字母为风险分类号(参见表4)，后3位为风险流水号。

表 5　重点保密管理风险列表

风险编号	风险描述	风险等级
C-01	外出携带涉密载体丢失	D
E-01	涉密计算机硬盘损坏，数据恢复时被拷贝留存	D
E-02	外场试验使用的计算机在涉密文档打印、涉密光盘刻录环节存在不足	D
B-01	新来员违反保密管理规定	C
D-01	无关人员进入要害部门部位	B
D-02	安装有行车记录仪的外来车辆进入控制区域	B
B-02	未及时将新增涉密人员在出入境管理部门备案	B
H-01	召开涉密会时，无关人员可能会知悉会议内容	B
F-01	涉密场所、活动、会议，存在手机泄密隐患	B
J-01	设备采购、引进时，存在安全隐患	B

3.3　风险应对

针对以上重点风险，笔者组织了相关业部门开展，从风险产生和演变的整个过程进行了讨论，对些风险的传递链进行了认真研究，并有针对性地制定了相应的管控措施[7-8](参见表 6)。

表 6　重点风险源和相应的控制措施

风险编号	应对措施
C-01	A. 外出携带涉密载体履行审批手续，并对外出人员进行保密提醒； B. 外出携带绝密级、机密级 1 份(含)以上，秘密级 3 份(含)以上的两人同行护送，并确保随身携带； C. 携带涉密载体外出时，不去与工作无关的场所； D. 使用涉密载体外带专用袋或专用箱，中途密封携带； E. 离开交通工具前，应及时检查所携带涉密载体是否完好； F. 携带涉密载体外出及返回，尽量乘坐专车； G. 外带涉密载体现场移交，当面清点并签字留证； H. 制定涉密载体丢失后的应急预案，并定期演练。
E-01	A. 选择具有数据恢复资质的单位对存储介质进行数据恢复； B. 对重要数据可靠备份，确保数据安全。
E-02	A. 加强外场试验人员的保密教育； B. 严格履行打印、刻录审批、登记制度； C. 打印的文件和刻录的光盘按规则进行编号； D. 从技术和管理 2 个方面完善外场计算机和信息系统管理； E. 加强返回后的检查，并对违规行为进行处罚。
B-01	A. 加强新员工上岗前的保密教育，考试合格后方能上岗； B. 为新员工指定“保密师傅”，开展“传帮带”活动。
D-01	A. 办理人员证件严格履行审批手续； B. 加强门卫验证环节的管理； C. 对外部人员证件使用防伪标志，并实行年审制度。
D-02	A. 办理车辆证件严格履行审批手续，确认有无形成记录仪； B. 加强验证管理，禁止装有行车记录仪的车辆进入控制区域； C. 对车辆证件使用防伪标志，并实行年审制度。
B-02	A. 指定专人每半年在出入境管理处对涉密人员报备更新； B. 保密管理部门将此项工作纳入年考核指标和检查内容。
H-01	A. 选择符合保密管理要求的场所召开涉密会议； B. 如果参会人员较多，为参会人员发放证件； C. 安排人员专门负责阻止位佩戴证件的人员进入会场； D. 会议服务人员由本单位人员担任。
F-01	A. 配备手机屏蔽柜，召开涉密会议时防止手机带入； B. 定期对手机信号屏蔽仪检查，确保召开正常使用； C. 增购手机信号屏蔽器，用于临时召开涉密会时借用。
J-01	A. 选择具有相应资质的供货商或合作伙伴； B. 引进的设备在投入使用前，请安全部门进行技术检测。

3.4　风险应对策略

在以上重点保密管理风险的应对过程中，笔者应用到了预防风险、减轻风险、回避风险、转移风险、储备风险和接受风险等多个策略[1]。以下，笔者以实际案例逐个对以上风险应对策略总结说明(详表 7)。

表 7　风险应对策略应用情况说明

序号	应对策略	应用情况说明	案例
1	预防风险	A. 有形手段：对人员证件使用防伪标志并年审； B. 无形手段：对新来员工进行保密知识培训。	D-01 B-01
2	减轻风险	为新员工指定“保密师傅”。	B-01
3	回避风险	安排专人阻止位佩戴证件的人员进入会场。	H-01
4	转移风险	选择具有存储介质数据恢复资质的单位进行数据恢复。	E-01
5	储备风险	制定涉密载体丢失后的应急预案，并定期演练。	C-01
6	接受风险	未采取应对措施的评估值很低的风险	—

3.5　风险监控

为了加强对重点保密管理风险的管控，便于实际操作和过程留证[9]，笔者设计了保密风险管控卡，从风险名称、风险分类、风险编号、风险策略等方面做出了规范性要求，参见图 4。

保密管理风险管控卡

部门名称		(填写风险所在部门的名称)	风险名称	(填写该风险的名称)
风险分类		(填写该风险的类别)	风险编号	(填写该风险的编号)
风险策略		(填写本部门针对该风险的管理策略，说明通过何种手段将风险控制在什么样的水平)		
风险诊断		(说明针对该风险在管理环节上存在的主要问题和缺陷，包括制度、流程、控制措施的设计和执行中存在的问题)		
解决措施	责任主体	(说明该风险的牵头业务部门及责任分配)		
	整改方案	(说明为降低该风险的低风险等级，拟开展的管理改进工作及资源投入计划，并说明各项管理改进工作的实施计划)		

填报人：　　填报时间：

图 4　保密管理风险管控卡

3.6　持续优化

风险不是一成不变的，随着管理要求和外部环境的不断变化，必然会出现新情况和新问题。所以，保密风险管理不可能一蹴而就，存在一个螺旋式发展的过程[10]，需要多轮迭代，持续改进、不断完善，并建立相应的长效管理机制。

4 结束语

通过风险理论在某单位保密管理领域的应用，笔者有效筛选出了该单位的保密管理要点。所筛选的保密管理风险也与日常保密检查过程中发现的主要问题大体一致，同时也暴露出了一些日常保密检查过程中未曾关注过的问题。风险理论的应用，是笔者在保密管理方面的一次尝试，也是对该单位内部干部职工在保密管理方面意见和建议的汇总与整理。虽然取得了一定的效果，但也存在调查不够深入，对风险理论的理解程度不深入，风险源判别不够准确，评估不够精确，措施不够有效，针对性不强等问题，还需要在下一轮应用过程中加强研究、宣传和培训，通过建立相应的激励机制，促进保密风险管理的持续完善。

参考文献：

[1] 沈建明. 项目风险管理[M]. 北京: 机械工业出版社, 2003: 1-10.
[2] 国家保密局编写组. 中华人民共和国保守国家秘密法释义[M]. 北京: 金城出版社, 2010: 4-7.
[3] 陕西省保密委教材编写组. 保密工作实用指南[M]. 西安: 陕西省保密局, 2013: 1-4.
[4] 国家保密局培训教材编写组. 保密工作概论[M]. 北京: 金城出版社, 2013: 6-7.
[5] 国家军工单位保密资格认证办公室. 军工保密资格审查认证工作指导手册[M]. 北京: 金城出版社, 2009: 245-275.
[6] 王少刚, 吴金秋, 李险峰. 企业保密风险管理的应用与研究[J]. 保密科学技术, 2014(11): 21-26.
[7] 国家国防科技工业局. 军工涉密信息系统安全保密管理人员工作务实[M]. 北京: 北京航空航天大学出版社, 2011: 43-140.
[8] 国家国防科技工业局. 军工单位涉密信息系统安全保密管理人员工作务实[M]. 北京: 北京航空航天大学出版社, 2011: 116-248.
[9] 中航工业集团公司经理部. 保密风险指南[Z]. 北京: 中航工业集团公司, 2014: 10.
[10] 柳立强, 刘清, 武瑞凯. 浅谈部队信息安全保密风险管理[J]. 科技风, 2013(9): 261.

****

（上接第 14 页）

表 1 鱼雷保障性参数体系

参数类型	参数名称
顶层参数	效能 寿命周期费用
综合特性参数	战备完好率 使用可用度 任务成功度
保障系统及资源参数	战备转级时间 保障设备满足率 保障设备利用率 备件满足率 备件利用率
保障性主要相关特性参数	平均故障间隔贮存时间 贮存可靠度 平均修复时间 维修度 故障检测率 故障隔离率 虚警率 总寿命 实航使用寿命 储存寿命

5 结束语

笔者建立了较为完整的鱼雷保障性参数体系，可用于确定相应指标。下一步，笔者将对各参数对应的定量指标的验证评估方法进行研究。

参考文献：

[1] 王树宗, 李宗吉, 严海峰. 国外鱼雷技术保障现状及我国应采取的技术途径[J]. 鱼雷技术, 1999, 7(4): 32-35.
[2] 徐廷学. 浅谈导弹武器系统保障性参数体系[J]. 飞航导弹, 1999(7): 1-3.
[3] 吴涛, 杨晶, 张正勇. 舰船装备保障性评估指标体系研究[J]. 舰船电子工程, 2012, 32(7): 104-106.
[4] 王喆峰, 薛霞. 雷达系统可靠性参数选择与指标确定的探讨[J]. 雷达与对抗, 2006(3): 66-69.
[5] 陈圣斌. 现代武装直升机可靠性维修性的参数选择和指标确定[J]. 直升机技术, 2001, 125(1): 25-32.
[6] 王自力. 可靠性维修性保障性要求论证[M]. 北京: 国防工业出版社, 2011: 18-20.
[7] 孟庆玉, 张静远, 严海峰. 鱼雷作战效能分析[M]. 北京: 国防工业出版社, 2003: 115-118.
[8] 毛丁辉, 邱建琪, 史涔溦. 基于转动惯量的异步电机参数自整定系统研究[J]. 机电工程, 2015, 32(6): 830-835.