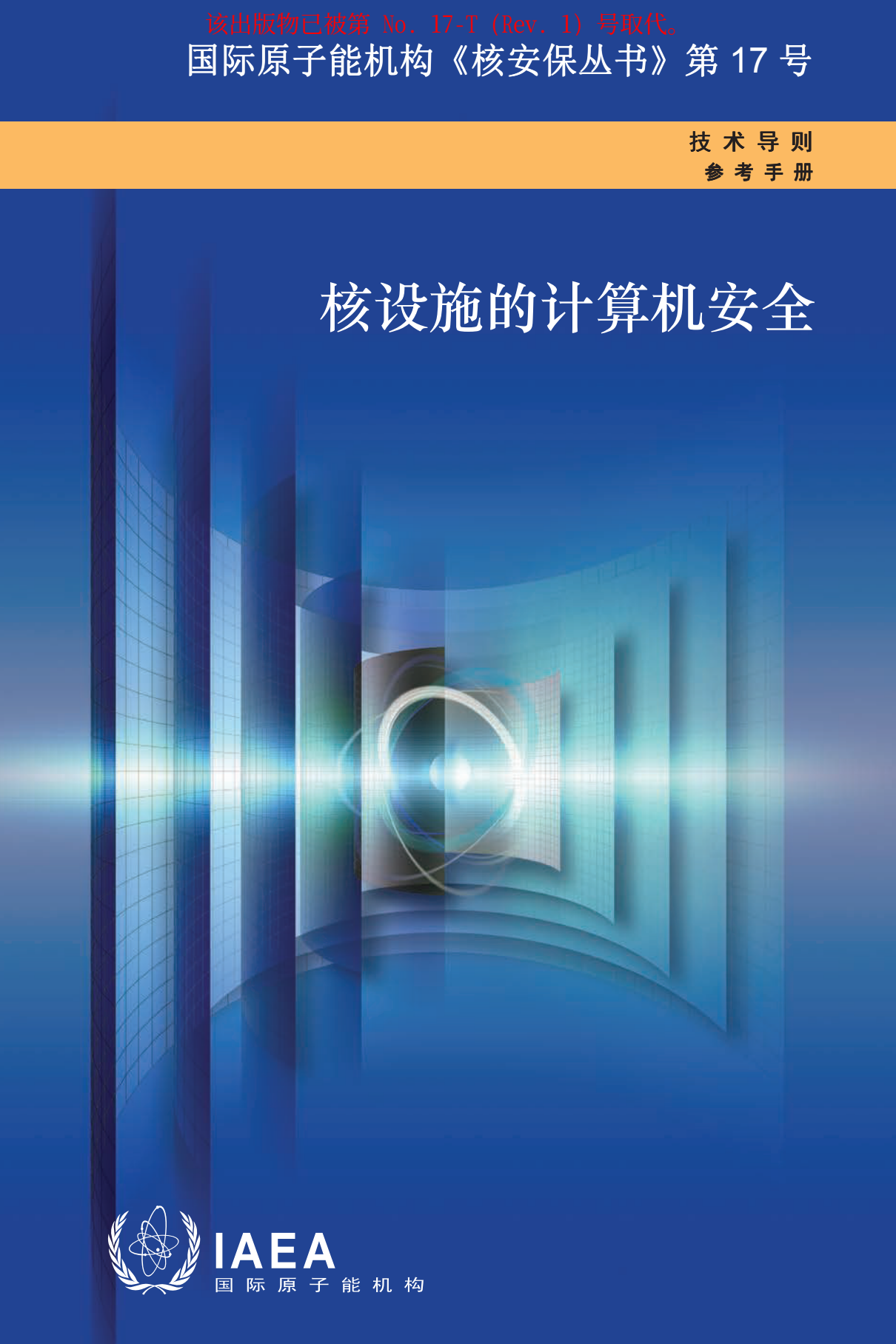
国际原子能机构《核安保丛书》第 17 号

技术导则
参考手册

核设施的计算机安全



IAEA
国际原子能机构

国际原子能机构《核安保丛书》

国际原子能机构《核安保丛书》出版物旨在处理与防止和侦查涉及核材料和其他放射性物质及其有关设施的盗窃、破坏、擅自接触和非法转移或其他恶意行为并做出响应有关的核安保问题。这些出版物符合并补充了国际核安保文书，例如经修订的《核材料实物保护公约》、《放射源安全和安保行为准则》、联合国安理会第 1373 号决议和第 1540 号决议以及《制止核恐怖主义行为国际公约》。

国际原子能机构《核安保丛书》的类别

原子能机构《核安保丛书》出版物按以下类别发行：

- **核安保法则**包含核安保的目标、概念和原则，并提供安保建议的基础。
- **建议**提出成员国在实施核安保法则时应当采用的最佳实践。
- **实施导则**进一步详细阐述这些广泛领域内的建议并提出其执行措施。
- **技术导则**出版物包括：**参考手册** — 在具体领域或活动中就如何适用实施导则提供详细措施和（或）指导；**培训导则** — 包括原子能机构在核安保方面的培训班教学大纲和（或）手册；以及**服务导则** — 在原子能机构核安保咨询工作组的行为和工作范围方面提供指导。

起草和审查

一些国际专家协助原子能机构秘书处起草这些出版物。对于核安保法则、建议和实施导则，原子能机构召开不限人数的技术会议，为感兴趣的成员国和相关国际组织提供适当的机会审查草案文本。此外，为确保高水平的国际审查和达成高度国际共识，秘书处向所有成员国提交草案文本，以供进行 120 天的正式审查。这使得成员国在文本印发以前有机会充分表示他们的意见。

技术导则出版物是与国际专家密切磋商后制订的。技术会议并非必需的，但为了广泛征求意见，也可以在认为必要时召开。

国际原子能机构《核安保丛书》出版物的起草和审查过程考虑到机密性，并且承认核安保与总体乃至具体国家的安全关切有着密不可分的联系。一个基本的考虑是在这些出版物的技术内容上应当虑及相关的原子能机构安全标准和保障活动。

核设施的计算机安全

下列国家是国际原子能机构的成员国：

阿富汗
伊斯兰共和国
阿尔巴尼亚
阿尔及利亚
安哥拉
阿根廷
亚美尼亚
澳大利亚
奥地利
阿塞拜疆
巴林
孟加拉国
白俄罗斯
比利时
伯利兹
贝宁
玻利维亚
波斯尼亚和黑塞哥维那
博茨瓦纳
巴西
保加利亚
布基纳法索
布隆迪
柬埔寨
喀麦隆
加拿大
中非共和国
乍得
智利
中国
哥伦比亚
刚果
哥斯达黎加
科特迪瓦
克罗地亚
古巴
塞浦路斯
捷克共和国
刚果民主共和国
丹麦
多米尼克
多米尼加共和国
厄瓜多尔
埃及
萨尔瓦多
厄立特里亚
爱沙尼亚
埃塞俄比亚
斐济
芬兰
法国
加蓬
格鲁吉亚
德国
加纳
希腊
危地马拉
海地
教廷
洪都拉斯
匈牙利
冰岛
印度
印度尼西亚
伊朗伊斯兰共和国
伊拉克
爱尔兰
以色列
意大利
牙买加
日本
约旦
哈萨克斯坦
肯尼亚
大韩民国
科威特
吉尔吉斯斯坦
老挝人民民主共和国
拉脱维亚
黎巴嫩
莱索托
利比里亚
利比亚
列支敦士登
立陶宛
卢森堡
马达加斯加
马拉维
马来西亚
马里
马耳他
马绍尔群岛
毛里塔尼亚伊斯兰共和国
毛里求斯
墨西哥
摩纳哥
蒙古
黑山
摩洛哥
莫桑比克
缅甸
纳米比亚
尼泊尔
荷兰
新西兰
尼加拉瓜
尼日尔
尼日利亚
挪威
阿曼
巴基斯坦
帕劳
巴拿马
巴布亚新几内亚
巴拉圭
秘鲁
菲律宾
波兰
葡萄牙
卡塔尔
摩尔多瓦共和国
罗马尼亚
俄罗斯联邦
卢旺达
沙特阿拉伯
塞内加尔
塞尔维亚
塞舌尔
塞拉利昂
新加坡
斯洛伐克
斯洛文尼亚
南非
西班牙
斯里兰卡
苏丹
瑞典
瑞士
阿拉伯叙利亚共和国
塔吉克斯坦
泰国
前南斯拉夫马其顿共和国
多哥
特立尼达和多巴哥
突尼斯
土耳其
乌干达
乌克兰
阿拉伯联合酋长国
大不列颠及北爱尔兰联合王国
坦桑尼亚联合共和国
美利坚合众国
乌拉圭
乌兹别克斯坦
委内瑞拉玻利瓦尔共和国
越南
也门
赞比亚
津巴布韦

《国际原子能机构规约》于 1956 年 10 月 23 日经在纽约联合国总部举行的国际原子能机构规约大会核准，1957 年 7 月 29 日生效。国际原子能机构总部设在维也纳，其主要目标是“加速和扩大原子能对全世界和平、健康及繁荣的贡献”。

国际原子能机构《核安保丛书》第 17 号
技术导则

核设施的计算机安全

参 考 手 册

国 际 原 子 能 机 构
2012 年·维也纳

版 权 说 明

Marketing and Sales Unit, Publishing Section
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 Vienna, Austria
传真：+43 1 2600 29302
电话：+43 1 2600 22417
电子信箱：sales.publications@iaea.org
http://www.iaea.org/books

国际原子能机构印制
2012 年 11 月 • 奥地利

核设施的计算机安全

国际原子能机构　奥地利 • 2012 年 11 月
STI/PUB/1527
ISBN 978-92-0-536110-9
ISSN 1816-9317

前　言

在全球目前的形势下无法排除核材料或其他放射性物质被用于恶意目的的可能性。各国对这种危险所作的响应是集体承诺加强对这种物质的保护和控制，并对核安保事件做出有效响应。为了加强全球核安保，各国已同意加强现有文书，并制订了新的国际法律文书。核安保对于核技术管理以及使用或运输核材料或其他放射性物质的应用至关重要。

国际原子能机构（原子能机构）通过“核安保计划”支持各国建立、维护和持久保持有效的核安保制度。原子能机构已经采用了一项综合性核安保方案。该方案承认有效的国家核安保制度建立在以下基础之上：执行相关国际法律文书、资料保护、实物保护、材料衡算和控制、侦查和应对贩卖这种物质的行为、国家响应计划以及应急措施。原子能机构编写《核安保丛书》，其目的在于协助各国协调一致地执行和保持该制度。

原子能机构《核安保丛书》包含“核安保法则”（该法则包括一国核安保制度的目标和基本要素）、“建议”、“实施导则”和“技术导则”。

各国承担对核安保的全部责任，特别是：提供对核材料和其他放射性物质及相关设施和活动的安保；确保这种物质在使用中、贮存中或运输中的安保；打击非法贩卖和防止因疏忽造成这种物质意外转移；以及做好应对核安保事件的准备。

本出版物属于“技术导则”类别的原子能机构《核安保丛书》，内容涉及核设施的计算机安全。本出版物基于各国的经验和实践以及计算机安全和核安保领域的出版物。提供本导则以供各国及其主管部门和营运者予以考虑。

正是因为有了来自原子能机构成员国的大量专家所作的贡献，才使得有可能将本出版物列入原子能机构的《核安保丛书》。与所有成员国广泛的磋商过程包括了顾问会议和不限人数的技术会议。随后向所有成员国分发了该草案，以供在 120 天内进一步征求意见和建议。对从成员国收到的意见进行了审查，并在本出版物的最终版本中考虑了这些意见。

编 者 按

本报告无论在法律方面还是在其他方面均不涉及因任何人的作为或不作为而引起的责任问题。

尽管在保持本出版物所载资料的准确性方面十分谨慎，但无论国际原子能机构还是其成员国均不对使用本出版物可能产生的后果承担任何责任。

国家或领土的特定称谓的使用并不意味着作为出版者的国际原子能机构对于该国家或领土、其当局和机构或其边界划定的法律地位做出任何判断。

提及具体公司或产品（不管是否已经载明为注册的公司或产品）名称并不意味着有任何侵犯所有权的意图，也不应当被解释为国际原子能机构方面的核可或推介。

目 录

该出版物已被第 No. 17-T (Rev. 1) 号取代。

1. 导 言

1.1. 背景

在过去的 10 年中，随着明显而又反复出现的计算机系统薄弱环节的证据逐步暴露出来，对计算机安全的关注一直不断加强。人们目睹这种薄弱环节被恶意利用的情况越来越频繁且影响越来越深刻。在一个越来越复杂的威胁假想方案中，出现作为针对一国关键基础设施攻击手段的网络恐怖主义的可能性已促使许多国家当局做好防御准备和发布新的条例。这种条例确定了在多个层面以及在各个运行阶段对核设施产生影响的计算机安全要求。与此同时，信息安全本身也一直在迅猛发展，结果创造出一系列丰富的国际最佳实践和标准文件，其中，国际标准化组织/国际电工技术委员会 27000 系列[1－5]正在迅速脱颖而出。

在承认标准化组织 27000 系列和工商业界其它标准的核心效力的同时，原子能机构希望将侧重于关注影响核设施计算机安全的具体条件。因此，对于认可和汇编相关导则和适当解决方案的出版物的需要便得到了确定。本出版物汇集了在核设施和其它关键基础设施范围内适用、测试和评审过计算机安全导则和标准的专家的知识和经验。本出版物汇编并叙述了适用于核学科的特别规定、最佳实践和经验教训，并将其放在与原子能机构其它导则和适用的工业标准相一致的安保计划的背景下进行阐述。

1.2. 目标

1.2.1. 核安保和计算机安全的目标

核安保包括预防、侦查和响应涉及或直接针对核材料、其他放射性物质、相关设施或相关活动的犯罪行为或未经授权的故意行为，以及可能直接或间接产生对人、财产、社会或环境的有害后果的其他故意行为。

计算机安全在确保实现这些目标方面发挥着越来越重要的作用。因此，本出版物将涉及制订和改进对设施的安全可靠运行和对预防偷窃、畜意破

坏和其他恶意行为至关重要的计算机系统、网络和其它数字系统的保护计划。

设施运行所需的所有其他系统或任何辅助或业务系统，凡对其擅自改动或修改可能损害其安保特征或可操作性的，均将通过把本出版物的规定扩大到适用于这些系统的方式予以涵盖。

因此，可将涉及计算机系统并与核安保有关的恶意行为归纳为以下几类：

— 旨在策划和实施进一步的恶意行为而通过对信息进行收集实施攻击；
— 瘫痪或损害对设施安保或安全至关重要的一台或若干台计算机属性的攻击；
— 结合其它同时攻击方式如实际侵入目标场所损害一台或若干台计算机。

计算机安全的目标通常被确定为保护电子数据或计算机系统和程序的机密性、完整性和可用性的属性。通过确定和保护数据或系统的这些属性以防止给核设施的安全和安保功能带来不利影响，就可以实现安保目标。

1.2.2. 范围

本出版物的主要目的是促进形成对增加计算机安全作为核设施总体安保计划一个基本部分之重要性的认识。

本出版物还旨在提供针对核设施执行计算机安全计划的导则。此点通过介绍为核设施制订的一些建议的方案、结构和执行程序来实现。这两方面结合起来对于实现和维护场址安保战略中规定的保护水平和遵守国家核安保目标至关重要。

本参考手册还旨在为提供关于评价现有计划、评定关键数字资产和确定以适当的方式降低风险措施的意见。

1.3. 核设施的特殊条件

对核设施计算机安全导则的需求是以带有核工业特征的特殊条件为依托的。以下列举了将在本出版物全面论述的这些条件的例子：

— 核设施必须遵守可能直接或间接监管计算机系统或确定导则的国家监管机构所规定的要求。
— 核设施可能不得不防止其它工业中通常不予考虑的更多威胁。这种威胁还可能是由于核工业的敏感性所引起的。
— 核设施的计算机安全要求可能不同于其它关切中的要求。一般业务活动仅涉及有限的要求。核设施则需要比电子商务、银行甚至军事应用具有更广泛的基础或一整套不同的考虑。第 7 章突出强调并详细说明了这种不同之处。

1.4. 结构

本出版物中的导则面向广大受众，其中包括决策者、核安保监管人员、设施管理层、负有安保职责的工作人员、技术人员、供应商和承包商。该导则适用于包括设计、开发、运行和维护在内的设施系统寿期的所有阶段。

本出版物分为两部分：

— 第一部分（第 2 章至第 4 章）旨在支持管理人员就设施内计算机安全的政策、设计和管理作出均衡的判断和知情的决定。该部分提供了关于计算机安全的监管和管理规定的导则。
— 第二部分（第 5 章至第 7 章）论述了关于执行计算机安全综合计划的技术和行政导则。

1.5. 基本方法

实施计算机安全所用的基本方法类似于确保核安保和核安全所用的方法。这凸显了从一开始就将计算机安全纳入设施安保综合计划的必要性和有利之处。

通过采用在更广泛的计算机安全界内开发的最佳实践方法和工具，同时考虑到核工业的特异性，就可以实现对计算机系统的成功保护。

第 5 章详细叙述的下列逻辑过程突出强调了核设施如何才能发展、实施、维护和改进计算机安全：

— 遵循国家法律和监管要求；
— 审查相关原子能机构导则和其他国际导则；
— 确保得到高管层支持和适当的资源；
— 确定计算机安全的范围；
— 确定计算机安全与设施运行、核安全和场址安全的其它方面之间的相互作用；
— 制订计算机安全政策；
— 开展风险评定；
— 选择、设计和实施计算机安全保护措施；
— 将计算机安全纳入设施管理系统；
— 定期审核、评审和改进系统。

本出版物将在对核设施作出具体规定的基本方法方面更详细地检查上述步骤。计算机安全基本方法其他阶段的实施工作可以直接参照现有国家和国际标准（见本出版物末尾的参考文献）进行。

1.6. 关键术语

由于词语在不同的实务界有着不同的含义，因此，本节对本出版物通篇使用的某些重要术语的含义作出阐释。

就本出版物而言，**计算机**和**计算机系统**系指构成核设施功能元素的计算、通讯、仪器仪表和控制装置。这不仅包括台式机算机、主机系统、服务器、网络装置，而且还包括嵌入式系统和可编程逻辑控制器等低层次部件。实际上，本出版物关切可能易受电子损害的所有部件。

在本出版物中，术语**计算机安全**将用于涵盖对以上定义的所有计算机和通过元件相加形成的所有互联系统和网络的安全。为本出版物的目的，

术语**信息技术安全**和**网络安全**被视为计算机安全的同义词，因此，将不在本出版物中使用。

本出版物定义的计算机安全属于（比如标准化组织/国际电工委 27000 [1]所定义的）**信息安全**的一部分，并与其有着同样的许多目标、基本方法和术语。

本手册末尾提供了本出版物所用的其他术语的定义。

该出版物已被第 No. 17-T (Rev. 1) 号取代。

第一部分

管 理 导 则

该出版物已被第 No. 17-T (Rev. 1) 号取代。

2. 监管和管理方面的考虑因素

本章突出强调高水平核设施计算机安全框架中的核心组成部分。本章将特别涉及与立法和监管机构以及与设施的管理和安保战略有关的各种问题。图 1 显示了与制订和实施核设施计算机安全计划有关的规范性文书层级的简化直观图。

2.1. 立法考虑因素

国家的关键作用在于建立核安保以及总体的计算机安全法律框架。这种框架如果实施得当，将对核设施的安全和安保产生很大的影响。国家法律制度应至少提供涵盖敏感资料保护和处理可能促成违反核安保规定的任何活动的法律和监管框架。

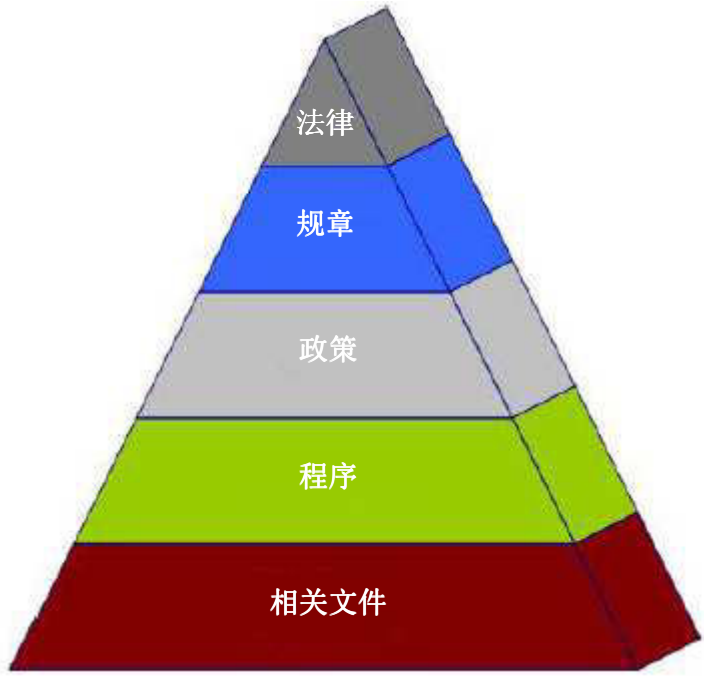


图 1. 相关规范性文书。

由于其问题的特殊性，计算机安全可能需要特别的法律规定，以考虑与计算机系统有关的独特犯罪行为和运作模式。国家应认真考虑其当前的法律是否充分涵盖了可能借助计算机实施的恶意行为。除其他外，可能影响计算机安全及其实施的重要法律包括：

— 有关计算机犯罪行为的法律；
— 有关恐怖主义行为的法律；
— 有关保护国家关键基础设施的法律；
— 授权披露信息的法律；
— 有关隐私和处理个人信息的法律。

重要的是对国家法律不断地进行审查和更新，以便对新的和正在出现的犯罪活动和对计算机安全潜在的其他威胁做出规定。

考虑到计算机网络的性质，敌手可能在一国境内但却身处该国实际边界之外从而有可能在该国法律制度管辖不到之地实施恶意行为。在编写本出版物之时，专门调整计算机犯罪国际合作问题的惟一相关国际法律文书是《欧洲理事会网络犯罪公约》[6]。

2.2. 监管考虑因素

监管机构应当在其导则中考虑相关法律并向营运者提供正确解释和实施法律义务的工具和手段。监管者还可以选择或指明相关参考导则，如标准化组织的标准或原子能机构的出版物。

监管者有关计算机安全的活动应明示确认防止偷窃核材料和导致可能的放射性释放的畜意破坏行为的目标。因此，在制定计算机安全法规时还应考虑促进核安保和核安全的法规。

可取的做法是国家监管机构（在涉及不止一个监管机构的情况下）开展合作，以便就拟规定的必要要求达成统一意见。

国家监管机构至少可以提供对计算机安全监管要求的高层次说明。更详细的监管要求还可以包括对于以下方面的规定：

— 管理层对计算机安全的承诺（第 4 章）。

— 计算机安全计划的所有权，包括计算机安全官员和团队职责的委任（第 4 章）。
— 计算机安全政策、实施计划和执法计划（第 5 章），包括：
  - 确定计算机安全范围；
  - 确定风险；
  - 风险管理战略；
  - 计算机安全培训和宣传计划；
  - 业务连续性计划。
— 审核和评审过程，无论内部的、外部的还是监管者自己进行的。

有关要求中不应规定详细的技术解决方案，因为技术发展可能使这种细节迅速变得过时。有关要求则可以侧重于预期成果，因为可以将这些成果写得不那么具有技术依赖性。

可以要求设施通过经核准的场址安保总计划或任何同等系列文件证明遵守了国家安保要求。**国家监管机构应将计算机安全要求作为场址安保计划要求的一部分予以颁布。**

2.3. 场址安保框架

场址安保主要是一种管理责任，特别是高管层的管理责任，其目的是通过实施场址安保计划确保充分实现法律和监管要求。

安保的所有领域（包括人员、实物、信息和计算机）应当相互作用和相互补充，共同促成可能在场址安保计划中定义的一座设施的安保特征（见图 2）。任何一个安保领域的失效都可能损害其他领域，并导致对其余安保领域提出额外的要求。计算机安全是与核设施安保所有其他领域相互作用的一个交叉领域。

本出版物的所有规定的实施应当始终顾及更大的场址安保计划框架。场址安保计划的制订同样也应从一开始就考虑到计算机安全。

管理层还有责任确保在适当级别妥善协调各个安保领域和纳入计算机安全。

图 2. 安保不同领域的相互作用。

2.3.1. 计算机安全政策

管理层应认识到计算机技术正越来越多地被用于完成核设施的许多关键功能。这种发展给运行安全和效率带来了多重好处。然而，为了确保正确发挥计算机系统的功能，必须要求计算机技术具有适当而均衡的安全屏障，以便在不必妨碍系统运行的情况下最大程度地防止恶意行为。

因此，所有核设施都应制订由场址最资深管理人核可和执行的计算机安全政策。该政策应具体规定设施的计算机安全总体目标。

计算机安全政策应成为场址安保总体政策的一部分，并应与其他相关安保职责一道经过谈判和协调。在制订计算机安全政策时，还应考虑到该政策对法律和人力资源的影响。

第 5 章对计算机安全政策和相关计划作了更详细的论述。

2.3.2. 核设施的计算机系统

支撑核设施运行的计算机系统和网络就结构、配置或性能要求而言包括许多非标准信息技术计算机系统。这种系统可能包括专业化工业控制系统、访问控制系统、警报和跟踪系统以及与安全和安保及应急响应有关的信息系统。尽管工业控制系统已从严格的专有实施发展为更为主流的计算机结构，但工业控制系统与标准信息技术系统之间仍存在显著的区别，因此，在制订场址安保计划时必须对此加以考虑。第 7 章对与核设施有关的计算机系统的独特性作了全面论述。

2.3.3. 纵深防御

保护要求应反映敌手要想达到目的必须克服或绕过的（结构、技术、人员和组织方面的）多层和多种方法保护的概念。

防止和减轻安保破坏行为后果的主要手段是“纵深防御”。纵深防御主要通过将必须在计算机系统损害发生前失效或使之失效的一系列连续而独立的保护层次结合起来的方式实施。如果某一层保护或屏障失效，后续保护层或屏障就会起作用。在实施得当时，纵深防御能够确保任何单一的技术性故障、人为故障或组织上的失误都不会导致计算机系统损害，并确保可能引起计算机事件叠加失误的概率非常低。不同防御层的独立有效性是纵深防御的一个必要组成部分。

2.4. 评定威胁环境

计算机安全威胁环境系指一种快速变化和不断演进的情形。尽管适宜的计算机安全计划将确保计划本身的持久性，但为防止现时最普遍的威胁而采取的具体控制措施并不能保证防止明天的威胁。

国家主管当局应定期发布威胁评价报告，包括对计算机系统安全的威胁和关于与核设施所用计算机系统的安全有关的当前攻击途径的资料。用于确定威胁级别并作为安保特征发展基础的典型工具是“设计基准威胁”（见第 6.3.1 节）。

设施保持有效且持续不断的威胁评定并向管理层和业务部门定期简报这种评定状况至关重要。

第 6 章详细但并非无遗地叙述了与核设施有关的潜在攻击来源和相关攻击手法以及评价和确定威胁所用的基本方法。

3. 管理系统

管理系统负责制订政策和目标并促使能以高效和有效的方式实现这些目标。管理系统是核安保文化的一个极为重要的辅助要素。核设施的许多活动都由管理系统进行控制。这些活动将安保、安全、健康、环境、质量

和经济各要素理想地融合在一个单一的管理工具或一套相互增强的综合系统之中[7、8]。

必须对管理系统进行审查，以确保完整性和遵守场址安保政策。更概括地说，管理系统就其本质而言具有动态性，必须适应设施和环境不断变化的状况，不能作为一次性措施执行，而是需要不断地接受评定和改进。图 3 说明了管理过程的周期。

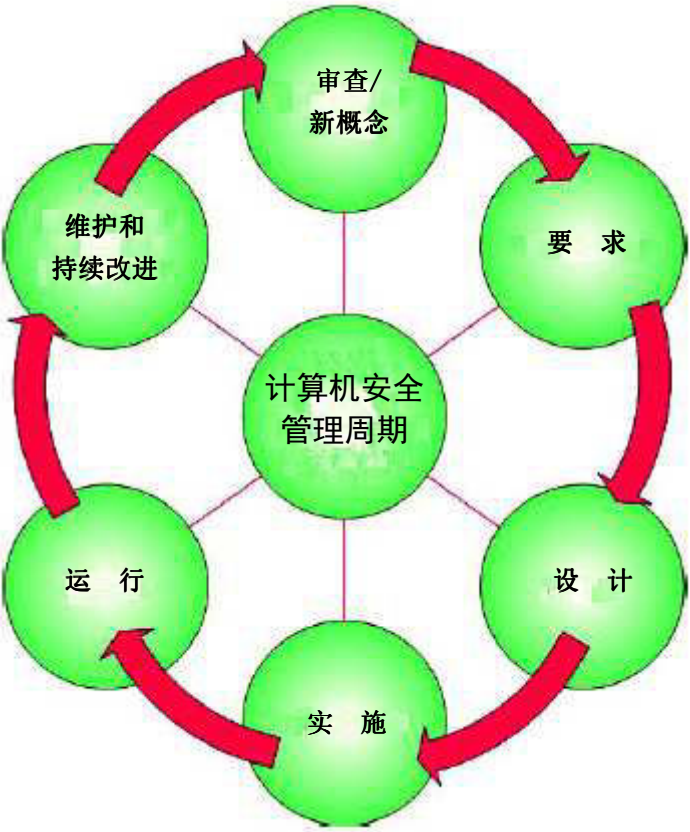


图 3. 安保管理周期。

本章旨在以计算机安全管理的必要细节补充现有的管理系统导则。要纳入所需的计算机安全规定，应当审查或增加的关键要素有：

— 信息资产确认和分类；
— 正式风险分析；

— 符合法律和监管要求；
— 业务运作要求；
— 关键人员能力要求；
— 业务连续性；
— 逻辑访问管理；
— 系统寿期安全；
— 配置管理；
— 修订和核准计算机安全措施；
— 执行已确定的计算机安全措施；
— 接受已实施的计算机安全措施；
— 遵守已核准的计算机安全措施；
— 即时分析计算机安全事件并酌情报告；
— 定期报告遵守情况；
— 内部和外部各方定期审查已实施的安全措施（审核）；
— 提高认识的培训；
— 新风险和已确定风险的变化；
— 法律和监管要求的改变；
— 信息安全中期计划。

上述过程应被视为贯穿系统寿期所有阶段不断进行中的活动。具体实施细节将在第 5 章所述计算机安全计划中详细论述。

4. 组织问题

4.1. 权力和职责

以下各节详细阐述了成功制订和保持计算机安全计划所需的对管理层和专家工作人员的最低要求。

4.1.1. 管理层

设施的高管层通过建立一个适当的过程和支持组织的方式启动计算机安全。为了实现此目的，管理层应当：

— 承担对计算机安全所有方面的全部责任；
— 制订设施的安全目标；
— 确保遵守法律和规章；
— 设定设施的风险接受水平；
— 分配组织的计算机安全责任；
— 确保在安全的不同方面之间进行充分沟通；
— 确保制订一项可执行的计算机安全政策；
— 提供实施可行的计算机安全计划所需的充足资源；
— 确保定期审核和更新计算机安全政策和程序；
— 确保对培训和宣传计划提供支持。

计算机安全的长期过程一般委托给组织内部的专家实施。

4.1.2. 计算机安全官员

计算机安全关乎几乎所有的设施活动。因此，将总体计算机安全监督工作交给一个明确界定的机构便十分重要。本出版物中使用了“计算机安全官员”的头衔；在其他情况下，该职能可以被称为“信息技术安全官员”或“信息安全官员”，也可以指派给多个角色。无论采取何种方案，这一职能都应当在全设施经过密切协调，保持始终独立于执行部门，并具有明确可及的与高管层的统属关系。

计算机安全官员应深入了解计算机安全并熟练掌握核设施安保其他方面的知识。进一步的要求有：了解核安全和项目管理，并有能力将不同学科的人员融入一个高效率的团队。

计算机安全官员或同等职位者的典型职责包括：

— 就计算机安全问题向公司管理层提供咨询意见。
— 领导计算机安全团队。
— 协调和控制计算机安全活动发展工作（如执行安全政策、指令、程序、导则、措施）。
— 与实物安保以及其他安保和安全学科协调，以便对安全措施和安全事件响应制订预案。

— 确定对设施内计算机安全至关重要的制度（即计算机安全基准）。应随时向资产所有者通报其设备在计算机安全中的作用。
— 定期开展计算机安全风险评定。
— 对计算机安全基准进行定期检查、审核和审查，并向最高管理层提供状况报告。
— 拟订和实施计算机安全培训和评价活动。
— 拟订并领导相关计算机安全应急响应活动，包括与内外部相关组织进行协调。
— 调查计算机安全事件，并拟订事件后程序和预防行动。
— 参与场址安保评定活动。
— 参与新系统采购/开发需求分析。

4.1.3. 计算机安全团队

计算机安全官员必须有权利用与计算机安全、设施安全和电厂运行以及实物安保和人员安全有关的适当跨学科专门知识。这可以包括一支专门的计算机安全团队或特别利用组织内部特定的专门知识。该团队的目的是支持计算机安全官员履行职责。

4.1.4. 其他管理职责

组织内部各管理层必须确保各自职责范围内的计算机安全达到适当的水平。典型的职责包括：

— 在场址计算机安全计划的指导下开展工作；
— 向计算机安全官员提供与计算机安全有关的运作要求和反馈，并解决运作要求、安保要求和安全要求之间的潜在冲突；
— 向计算机安全官员通报可能导致改变计算机安保特征的任何状况，如人事变动、设备变更或程序变更；
— 确保工作人员得到关于与其职责有关的计算机安全问题的充分培训和简况介绍；
— 确保分包商和为承包单位工作的第三方供应商在场址安保计划的范围内开展工作；

— 跟踪、监测和报告具有安全意义的事件；
— 执行人员安全措施。

4.1.5. 个人职责

组织内的每个人都有责任执行计算机安全计划。具体职责包括：

— 了解基本计算机安全程序；
— 了解岗位特定的计算机安全程序；
— 在计算机安全政策的范围内开展工作；
— 向管理层通报可能导致计算机安保特征弱化的任何变化；
— 向管理层通报涉及损害计算机安全的任何事件或可能的事件；
— 定期参加安全方面的初始和进修培训。

4.2. 计算机安全文化

健全的计算机安全文化是任何有效安保计划的必要组成部分。管理层必须确保将计算机安全意识充分纳入总体场址安保文化之中。核安保文化的特点是信念、态度、行为和管理系统，将这些组合起来就产生了有效的核安保计划。核安保文化的基础是可以在监管、管理或运行核设施或开展核活动方面发挥作用的人甚至可能受这些活动影响的人承认，存在可信的威胁，而且核安保十分重要。（关于核安保文化的更多资料，见参考文献[9]。）计算机安全文化是总体安保文化的一个子集，其基础是将上述特点适用于计算机安全意识。

经验已经表明，大多数计算机安全事件都与人有关，任何计算机系统的安全在很大程度上取决于其全部使用者的行为。附件三提供了可能导致产生安全损害的人为失误的例子。计算机安全文化通过旨在向工作人员通报情况和增强计算机安全意识的一系列活动（如招贴画、通告、管理层讨论、培训、测试等）发展起来。应定期衡量、审查和不断改进计算机安全文化的特性。可用下列指标来评价一个组织内的计算机安全文化：

— 计算机安全要求被以文件形式明确记载，并为工作人员所充分理解。

— 存在组织内外部计算机系统运行所用的明确而有效的程序和规程。
— 工作人员理解并认识到遵守计算机安全计划范围内的控制措施的重要性。
— 对计算机系统进行维护，以确保其安全可靠并按照计算机安全基准和程序运行。
— 管理层充分致力于并支持安全举措。

4.2.1. 计算机安全培训计划

强有力的培训计划是计算机安全文化的一个基石。至关重要的是教育工作人员、承包商和第三方供应商认识到遵守安全程序和维护安全文化的重要性。

提高认识计划应包括下列要求：

— 成功地完成计算机安全培训和（或）提高认识计划应成为进入计算机系统的一个先决条件。培训应与系统安全级别和使用者的预期作用相适应。
— 应向负有关键安全职责的人（如计算机安全官员、计算机安全团队、项目管理人员、信息技术行政官员）提供强化培训/资格认证。
— 培训应对所有工作人员定期反复进行，以包括新的程序和新现威胁。
— 应要求工作人员确认其了解各自的安全职责。

培训计划应包括评价计算机安全意识、培训有效性和促进持续改进或再培训的程序的衡量标准。

该出版物已被第 No. 17-T (Rev. 1) 号取代。

第二部分

实 施 导 则

该出版物已被第 No. 17-T (Rev. 1) 号取代。

5. 实施计算机安全

本出版物不确定可接受风险的最低标准或可以采用的系列具体缓减措施。任何系列具体标准都会随着数字系统的变更、新威胁的出现、新缓减工具的提供以及监管要求的变化而迅速变得过时。本出版物第二部分侧重于汇编一套支持和指导实施核设施计算机安全的具体的方法学建议。

这些建议既非规定性的，也非确定性的，而应作为导则采用。在适当情况下，可以采用替代措施来实现预期的纵深防御和其他基本核安保目标[10－12]。

5.1. 计算机安全计划和政策

5.1.1. 计算机安全政策

正如第 2.3.1 节所介绍的那样，计算机安全政策规定一个组织的高水平计算机安全目标。该政策必须达到适当的监管要求。计算机安全政策要求应当纳入作为将用于执行和控制政策的较低层级文件中的考虑因素。此外，该政策还必须：

— 可以执行；
— 可以实现；
— 可以审核。

5.1.2. 计算机安全计划

计算机安全计划就是以组织角色、责任和程序的形式实施上述政策。该计划规定并详细说明实现设施的计算机安全目标的途径，而且是场址安保总体计划的一部分或与其有联系。

该计划应列入易受攻击性、保护措施、后果分析和缓减措施方面的主要行动，以确定和保持核设施可接受的网络风险，并促进恢复到安全运行状态。

5.1.3. 计算机安全计划的组成部分

在既定计算机安全政策的基础上，计划的各个组成部分都应尽量实现各自不同的目的和目标。以下各分节提出了关于计算机安全计划最低内容和项目的建议：

(a) 组织和责任：
  (1) 组织系统图；
  (2) 负责人和报告责任；
  (3) 定期审查和批准程序。
(b) 资产管理：
  (1) 所有计算机系统清单；
  (2) 所有计算机系统应用程序清单；
  (3) 网络图，包括与外部计算机系统的所有连接情况。
(c) 风险、漏洞和遵守情况评定：
  (1) 安全计划审查和再评定周期；
  (2) 自评定（包括侵入性测试程序）；
  (3) 审核程序和缺陷跟踪与纠正；
  (4) 监管和法律遵守情况。
(d) 系统安全设计和配置管理：
  (1) 基本结构和设计原则；
  (2) 涉及不同安全级别的要求；
  (3) 制订对供应商和卖方的计算机安全要求；
  (4) 全寿期安全。
(e) 运行安全程序：
  (1) 访问控制；
  (2) 数据安全；
  (3) 通讯安全；
  (4) 平台和应用程序安全（如硬化）；
  (5) 系统监测；
  (6) 计算机安全维护；

(7) 事件处理；
(8) 业务连续性；
(9) 系统备份。

(f) 人员管理：
(1) 忠贞度调查；
(2) 培训；
(3) 资格认证；
(4) 终止/调离。

以上提供的是制订计算机安全计划所用的框架。可以利用许多参考文献来填充这一框架，主要的国际参考文献有关于信息安全管理系统的标准化组织/国际电工委 27001[2]和关于实施建议的标准化组织/国际电工委 27002[3]。

尽管上述大多数组成部分在任何商业或工业计算机安全计划中具有一致性，但其在核设施范围内实施却确实存在某些细微差别。计算机安全计划的这些组成部分在第 7 章作了更详细的阐述。风险、漏洞和遵守情况评定在第 6 章作了阐述。资产分析则在第 5.3 节作了进一步详细阐述。

5.2. 与其他安保领域的相互作用

如第 2.3 节所述，计算机安全计划的运作和维护应当在设施总体保护计划的框架内进行。设施特定的计算机安全计划应在与实物保护、安全和信息技术专家密切磋商后拟订。计算机安全计划必须经过定期审查和更新，以反映来自任何安保领域的安保事件和来自场址安保系统的运作经验。

5.2.1. 实物安保

实物安保计划与计算机安全计划应相互补充。计算机化的资产具有实际接触控制要求，同样，电子损害可能导致某些实物保护功能下降或失效。攻击假想方案完全可以纳入对电子攻击和实际攻击的协调。负责实物安保计划的团队与计算机安全计划的团队应相互通报情况并协调各自的工作，以确保计划在制订和审查过程中的一致性。

5.2.2. 人员安全

除了宣传和培训外，通常在人员安全领域范围内处理的安保的其他方面对于建立一致的计算机安全也必不可少。应与计算机安全管理部门和人员安全管理部门进行协调，以便对建立适当的忠贞调查、保密承诺和终止程序水平以及对确定必要的岗位胜任力做出必要的规定。特别是负有关键安全职责的工作人员可能需要接受更高水平的忠贞度。

5.3. 资产分析和管理

核设施计算机系统之间的相互作用可能以非显性的方式影响安保。因此，安全计划必须**查明所有资产**并**较为全面地盘点对设施安保和安全功能至关重要的资产**。盘点的内容可以包括数据、计算机系统及其接口和所有者。

以下方法可以满足上述需求：

(a) 应汇编关于现有计算机系统的相关信息，以制作一份完整的资产清单；
(b) 应绘图标明已确定资产之间的互连情况；
(c) 应确定和评价与安全功能和已确定的安全系统、安全相关系统和安保系统的相关性。

每个步骤的完整性是开始后续步骤的至关重要的先决条件。

对核设施计算机系统的全面分析包括：

— 全部现有计算机化系统的功能/任务和运行模式；
— 确定相关互连情况，包括电源；
— 数据流分析，以确定何者与何者相通以及如何相通和为什么相通；
— 发起通讯的程序、通讯频率和规程；
— 计算机系统和设备位置；
— 用户群组分析；
— 对数据和计算机化系统而言的所有权；
— 相应的安全级别（见第 5.5 节，分级方案）。

设想这种分析所需的许多信息都可以获得，但却应当加以核验和组织。相关信息来源包括系统技术规格和文献。

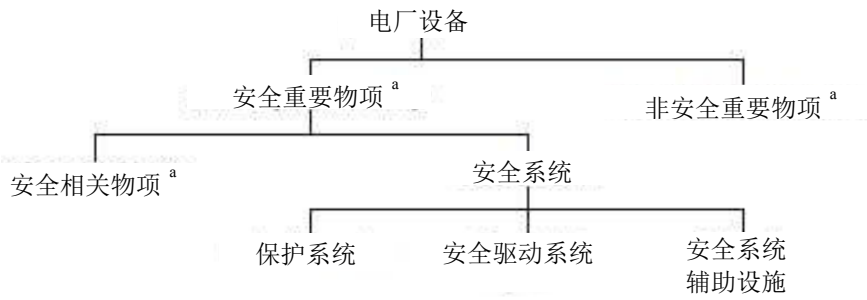
5.4. 计算机系统分类

就本出版物而言，正如第 1.6 节所定义的那样，计算机和计算机系统系指构成核设施功能元素的计算、通讯、仪器仪表和传感装置。属于主要关切的计算机功能是与安全和安保有关的控制和数据程序。就对这些功能提供支持、通过次级或间接效应对安保可能造成的损害以及电厂的总体生产率而言，其他计算机功能可能成为一个关切事项。

以下非详尽无遗地列出了在核设施可以找到并与本导则的目标相关的计算机系统。根据其安全重要性和安保重要性分别对其进行了分类。在确定所适用的适当安全级别（第 5.5 节）时以及在风险评定分析（第 6.2 节）中应考虑到这两种分类。还要注意就安全和安保而言，有些功能是明显重叠的。

5.4.1. 安全重要性

如图 4 所示，原子能机构安全标准（如参考文献[13－15]）按功能对核设施设备进行了分类。



[a] 在此范畴内，“物项”系指结构、系统或部件。

图 4. 就安全功能而言的电厂设备。

电厂设备

— 安全重要系统
  - 安全系统
    — 保护系统：自动启动的反应堆和电厂保护行动所用的仪器仪表和控制系统。
    — 安全驱动系统：由保护系统和通过手动方式启动的用于完成安全行动的仪器仪表和控制系统。
    — 安全系统辅助设施：应急供电系统所用的仪器仪表和控制系统。
  - 安全相关系统
    — 过程控制系统：电厂控制所用的仪器仪表和控制系统。
    — 控制室仪器仪表和控制系统，包括警报系统。
    — 为控制室收集和准备信息的过程计算机系统。
    — 燃料处理和贮存仪器仪表和控制系统。
    — 消防系统。
    — 出入控制系统。
    — 语音和数据通讯基础设施。

— 非安全重要系统
  - 非安全重要功能（如除盐）控制系统。

还应考虑不一定属于电厂设备范围但却可能影响安全的计算机系统。

非电厂设备

— 办公自动化
  - 作业许可和作业指令系统：对工作活动进行协调以提供良好工作环境的系统。
  - 工程和维护系统：处理电厂运行、维护和技术支持细节的系统。
  - 配置管理系统：旨在跟踪电厂配置包括在核设施安装的型号、版本和部件的系统。

- 文件管理系统：用于存储和检索电厂信息如图纸、会议记录的系统。
- 内联网：允许在“需要知晓”基础上访问电厂所有技术性和行政性文件的系统。这种访问通常为只读式。

— 外部连接性
- 电子邮件：用于向外部方传输信息的系统。
- 公共网站：用于向因特网用户提供设施信息的系统。
- 远程访问/第三方访问：允许从外部对场址内某些功能进行严格控制的访问系统。

5.4.2. 安保或安保相关系统

就安保系统而言，尚不存在类似于安全分类的成熟的安保分类。但对设施内的这类系统进行这种分类应成为资产分析的一个重要部分。以下列表可以辅助进行这种分类：

— 实际出入控制系统：用于确保仅有获得批准的人员才能进入场址内与他们行使的职能相适应的区域；
— 语音和数据通讯基础设施；
— 安全许可数据库：用于确保人员持有适当的安全许可方可获准进入场址的一部分或接触场址上的资料；
— 安保警报监测和控制系统：用于监测场址上的所有安保警报并辅助评定警报；
— 计算机和网络安全组成部分；
— 核材料衡算和控制系统。

5.5. 计算机安全分级方案

计算机系统安全应以分级方案为基础，根据分级方案，适用的安全措施要与攻击的潜在后果成比例。执行分级方案的一种实用方法是对计算机系统进行区位分类，并根据为各区位指定的安全要求的级别对其实行分级保护原则。应根据计算机系统与安全和安保的相关性为其指定不同的级别和区位。但是，**应允许风险评定过程反馈于分级方案并影响分级方案**。

5.5.1. 安全级别

安全级别是规定设施内各种计算机系统所需安全保护程度的一种抽象概念。分级方案中的每个级别都需要有一套不同的保护措施，这样才能满足该级别的安全要求。一些保护措施适用于所有级别的所有计算机系统，而另一些保护措施则专门针对某些级别。

安全级别模式使得能够在对各种计算机系统进行分类（为系统指定一个级别）并确定适合于该级别的一套保护措施的基础上更容易地指定对各系统的保护措施。

各级别及其相关的保护措施应在计算机安全计划中适当加以规定。

5.5.2. 区位

区位是为行政管理、通讯和实施保护措施的目的将计算机系统进行分组的一种逻辑和物理概念。区位模式使得能够为行政管理和实施保护措施的目的将对电厂安全可靠运行具有同样或类似重要性的计算机系统组合在一起。

区位模式的采用应遵守下列导则：

— 每个区位均由对设施的安保和安全具有同样或类似重要性的系统组成；

— 属于一个区位的系统对保护措施具有类似的需求；

— 属于一个区位的不同计算机系统均建立一个该区位内部通讯所用的可信区；

— 区位边缘需要有以区位依赖政策为基础的数据流解耦机制；

— 区位可以为改进配置的目的划分为分区位。

由于区位由对设施的安全和安保具有同样或类似重要性的系统组成，因此，每个区位都可以被指定一个级别，以指明对该区位的所有计算机系统适用的保护措施。然而，区位与级别之间的关系不是一对一的关系；在多个区位需要同等程度保护时，可以对多个区位指定一个级别。区位是计算机系统的逻辑和物理分组，而级别则代表着所需的保护程度。

区位模式应在计算机安全计划中适当加以规定，以提供关于所有计算机系统、所有相关通讯线路、所有区位交叉点和所有外部连接的概览。

5.5.3. 实施安全级别模式的例子

以下介绍了按不同级别实施安全措施的例子。这只是分级方案的一种可能的实施方法；对级别及其基本安全措施的确切选择应根据纳入考虑的环境、设施的具体情况和专门的安全风险分析作出。

在实施中：

— 通用级别的措施应适用于所有计算机系统。

— 如图 5 所示，安全级别由 5 级（需最少保护）至 1 级（需最多保护）构成。

— 与每一级别相应的措施不是累积性的（因此，可能会出现重复）。

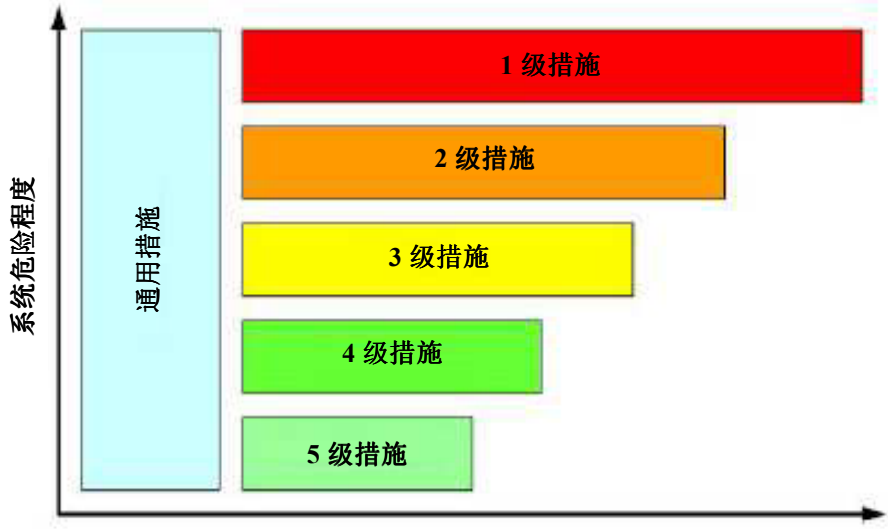


图 5. 安全级别/措施强度。

通用级别

对于适用的系统和级别而言，应采用以下通用措施：

— 规定适合于每一级别的政策和做法。

— 为所有使用者编写安全操作程序并使其为他们所理解。
— 获准接触该系统的工作人员必须具备适当的资格和经验，并在必要时经过安全审批。
— 使用者只能获准接触其开展工作所需的系统上的功能。
— 建立适当的接触控制和使用者验证过程。
— 建立异常现象探测制度或程序。
— 对应用程序和系统薄弱环节进行监测，并采取适当的措施。
— 定期进行系统薄弱环节评定。
— 必须按照安全操作程序对可移动介质进行控制。
— 应对计算机和网络安保组成部分进行严格的维护。
— 对计算机和网络安全组成部分（如安全门户、侵入探测系统、侵入预防系统、虚拟个人网络[1]服务器）进行严格的登记和监测。
— 建立适当的备份/恢复程序。
— 按照部件和系统的功能对其实际接触进行限制。

1 级

除通用措施外，还应将 1 级保护措施适用于对设施至关重要并需要最高水平安保的系统，如保护系统。这种措施可以包括以下内容：

— 不得授权安全级别较弱系统的任何类型网络数据流（如确认，信号通知）进入 1 级系统。只应允许严格的向外通讯。注意这种严格的单向通讯不天然确保可靠性和完整性（可以考虑冗余/纠错手段）。还注意这样做排除了任何类型的“握手”协议（包括 TCP/IP[2]），甚至是采用控制连接指示的协议。强烈劝阻规定例外，而且只有在严格的逐案基础上并在得到完全的正当理由和安全风险分析支持的情况下才能考虑规定例外。[3]

[1] “虚拟个人网络”是利用公共通讯手段建设的一种网络，其目的是利用加密和其他安全机制连接各个节点，以确保仅有授权的用户可以进入该网络，而且数据不会被拦截。

[2] 传输控制协议/因特网协议 — 数据传输协议。

[3] 一些成员国强烈认为在任何情况下都不应允许有例外。

— 确保系统完整性和可用性的措施一般解释为属于安全论证文件的一部分。
— 不允许远程维护访问。
— 严格控制对系统的实际接触。
— 获准接触系统的工作人员的数量限于绝对的最少量。
— 双人规则适用于在计算机系统范围内所作的经核准的任何修改。
— 对所有活动都应进行登记和监测。
— 在逐案基础上对系统的每一次数据输入进行批准和验证。
— 对任何修改都应适用严格的组织和行政程序，包括对硬件进行维护和更新以及对软件进行修改。

2 级

除通用措施外，还应将 2 级保护措施适用于需要高水平安全的系统，如运行控制系统。这种措施可以包括以下内容：

— 只允许 2 级和 3 级系统的外向单向网络数据流。相反（内向）方向只能允许接收必要的确认信息或受控信号信息（如适合于 TCP/IP 的信息）。
— 可以允许在逐案基础上并在限定的工作期内进行远程维护访问。远程维护访问在使用时必须要有强力措施的保护，使用者必须遵守通过合同规定的既定的安全政策。
— 将获准接触该系统的工作人员的数量保持在最低限度，并对使用者和行政管理人员精确地加以区分。
— 应严格控制与系统实际连接。
— 已经采取了一切合理措施来确保系统的完整性和可用性。
— 涉及对系统采取行动的薄弱环节评定可能导致电厂或程序不稳定，因此，只应考虑在工厂验收测试或长期计划停堆期间利用试验台架、备用系统进行。

3 级

除通用措施外，还应将 3 级保护措施适用于对运行非必要的实时监视系统，如控制室中的实时过程监视系统，3 级措施属于防范各种网络威胁的

中等严厉程度措施。这种保护措施可以包括以下内容：

— 不允许从 3 级系统访问因特网。
— 对登录和关键资源的审核跟踪情况进行监测。
— 实施安全门户，以保护本级系统不受控制地接收来自 4 级系统的通讯量，并且只允许特定的限量活动。
— 应控制与系统实际连接。
— 在严密控制的情况下逐案允许远程维护访问；远程计算机和使用者必须遵守通过合同具体规定的既定的安全政策。
— 通过访问控制机制并根据“需要知晓”原则对使用者可利用的系统功能进行控制。必须对这一原则的任何例外进行认真的研究，并应通过其它手段（如实际接触）确保提供保护。

4 级

除通用措施外，还应将 4 级措施适用于与运行技术规格要求的部件或系统有关的维护或运行活动管理所用的技术数据管理系统（如作业许可、作业指令、安全标签、文件管理），4 级措施属于防范各种网络威胁的中等严厉程度措施。4 级措施包括以下内容：

— 仅允许获得批准的合格使用者对系统进行修改。
— 可以准许从 4 级系统访问因特网，但条件是要采取适当的保护措施。
— 实施安全门户，以保护本级系统不受控制地接收来自外部公司或场址网络的通信量，并且允许受到控制的特定活动。
— 应控制与系统实际连接。
— 允许并控制远程维护访问；远程计算机和使用者必须遵守通过合同具体规定和控制的既定安全政策。
— 通过访问控制机制对使用者可利用的系统功能进行控制。必须对这一原则的任何例外进行认真的研究，并应通过其它手段确保提供保护。
— 允许获得批准的使用者进行远程外部访问，但条件是建立适当的访问控制机制。

5 级

5 级措施应适用于同技术控制或运行目的没有直接重要性的系统，如办公自动化系统，5 级措施属于防范各种网络威胁的低等严厉程度措施。5 级措施包括以下内容：

— 仅允许获得批准的合格使用者对系统进行修改。
— 允许从 5 级系统访问因特网，但条件是要采取适当的保护措施。
— 允许获得授权的使用者进行远程外部访问，但条件是建立适当的控制。

5.5.4. 解耦区位

区位边缘需要有数据流解耦机制，以防止未经授权的访问，并防止错误从保护要求较低的区位向较高的区位蔓延。

确保区位解耦的技术和行政措施必须适合各保护级别的具体要求。不应允许存在通过若干区位的直接连接通道。

6. 威胁、薄弱环节和风险管理

下节介绍计算机系统风险管理所采用的基本概念。风险管理在包括设计、开发、运行和维护在内的设施系统寿期的所有阶段都具有相关性。第 6.2 节概述了全面风险管理方法所需的步骤。第 6.3 节和第 6.4 节侧重叙述了核工业各个阶段所具有的具体特点。

6.1. 基本概念和关系

计算机安全背景下的风险系指特定威胁利用一项资产或一组资产的薄弱环节从而给组织造成损害的可能性。衡量这种风险是要将发生事件的可能性与其后果的严重程度结合起来进行。

图 6 是显示威胁、薄弱环节和风险概念之间多种相互联系的流程图[16]。

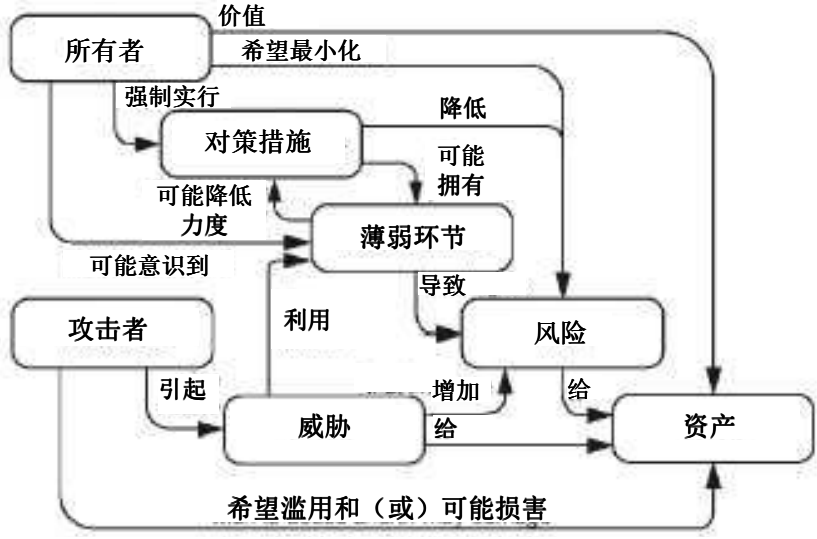


图 6. 安全概念和关系（根据标准化组织 13335-1 2004 [16]改编）。

6.2. 风险评定和管理

风险评定是在处理薄弱环节和其被利用的可能性中用于确定分配资源和工作量的最佳场所的一个重要手段。

这是一个确定并记录威胁、薄弱环节和影响三者之间特定结合方式并设计出适当的保护控制措施的过程。威胁和薄弱环节评定奠定了制订防止对计算机系统的攻击或缓减其后果所需的对策措施的基础。

风险评定和管理方法学的基本步骤如下：

— 确定范围和背景；
— 确定和表征威胁；
— 薄弱环节评定；
— 制订攻击假想方案；
— 成功利用的可能性；
— 评价风险级别；
— 确定对策措施。

为了开展系统而连贯的风险分析和评定，必须采用一种遵守被明确定义的现有标准的过程。许多风险评定或管理方法学和工具已臻成熟，可以高效构建这一过程，并因此获得了广大受众的认可。其中大多数基于共同的概念和逻辑。现行国际标准是标准化组织/国际电工委 27005 —《信息安全风险管理》[4]。附件二给出了方法学的另一个具体例子。国家当局可能要求采用具体的风险评定方法学或政策，而设施则可能额外拥有自己的方法学或政策。

欧洲网络和信息安全机构对风险评定方法和工具作了有意义的概述，并专辟了一个特别网页进行这方面的调查[17]。

评价系统的必要性、评定的深度以及更新风险分析的频率都取决于系统就其安全和安保功能而言的重要性。在对系统进行修改时必须考虑进行一次新的分析或至少进行一次审查。引进新设备、新软件和新程序或者营运者技能组合的重大变化都可能满足这一条件。潜在威胁和薄弱环节的数量通常随着从独立系统向互联系统的进步而增加。

在开展针对特定威胁的风险分析不切实际时，建议采用最佳实践和良好的工程原则。

6.3. 确定和表征威胁

图 7 强调说明了攻击越来越复杂而发动这种攻击所需的知识逐步减少的持续趋势。计算机安全计划应力争保持一定的评定水平，以涵盖很广泛的可能的攻击假想方案。

在发生主要黑客入侵事件的场合经常可以找到关于工业控制系统薄弱环节的出版物。考虑到这种出版物所描述的一般是真实黑客技能和兴趣发展水平的一种滞后的状况，这应当成为一种额外的提高认识因素。此外，交互式通讯软件的薄弱环节最近已开始由各国家计算机应急响应小组进行公布，这一做法增强了对公众舆论和计算机安全界的曝光度，并将兴趣集中在薄弱环节解决方案和产品缺陷上。

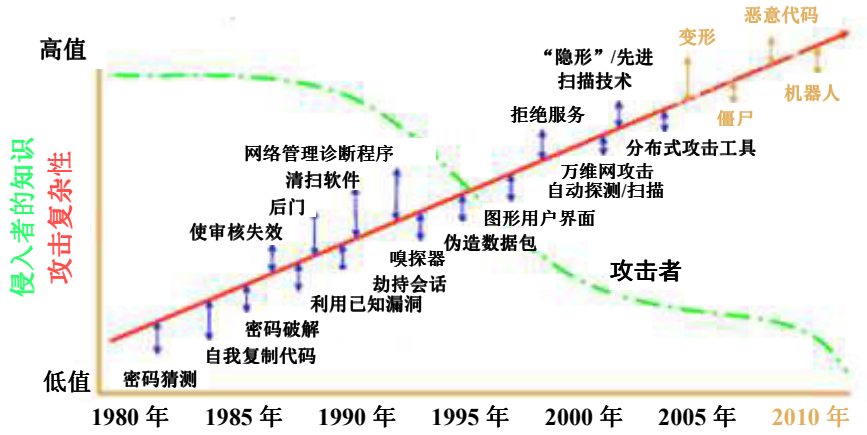


图 7. 威胁随着攻击者的激增而越来越复杂。[4]

因此，在确定了适当的支持和资源后，制订计算机安全计划的最初步骤应当侧重于了解基于可信的攻击者概貌和攻击假想方案的潜在威胁。可能的第一步将是创建列出可信攻击者、动机和潜在目标的攻击者概貌矩阵。然后，可以将攻击者概貌矩阵用于建立看似可行的攻击假想方案；以下分节更详细地研究了这一过程。

6.3.1. 设计基准威胁

通常用于确定威胁级别并作为安保特征发展基础的一个重要工具是“设计基准威胁”。设计基准威胁是关于潜在（内部和（或）外部）敌手特性和特征的一种表述。设计基准威胁源于可靠情报信息，但却并未打算使之成为关于实际主要威胁的表述。根据当前威胁环境，设计基准威胁代表着设施预期防御的最大合理威胁。各国在监管体系中利用设计基准威胁来确定进行适当的资源分配，以防止核材料和核设施免于敌对行动。（关于设计基准威胁的更多资料，见参考文献[18]。）

应当考虑将利用/针对计算机系统的单独攻击威胁或协同攻击（包括利用计算机系统）威胁纳入这种假想方案。

---

[4] H.F.利普森，《跟踪和追踪网络攻击者：技术挑战和全球政策问题》，特别报告 CMS/SEI-2002-SR-009（2000）10。

6.3.2. 攻击者概貌

表 1 和表 2 说明了一系列可能的攻击者概貌。表 1 侧重于内部威胁（关于内部威胁的论述，另见参考文献[19]），表 2 则确定了一些可能的外部威胁。两表均将一般类型攻击者与其资源、攻击的时间跨度、可能使用的工具以及攻击者的动机联系起来。需要对概貌进行修改，以适应具体设施的情况。因此，需要有适当的情报收集过程，才能确保每一设施的攻击者矩阵的完整性和相关性。

6.3.3. 攻击假想方案

在制订攻击假想方案的过程中，可以辨别若干可能性。对核设施的攻击可能抱有以下目的：

— 逐步形成随后旨在破坏电厂和（或）移走核材料的协同攻击；
— 危及人类或环境安全；
— 发动对另一场址的攻击；
— 造成混乱和恐慌；
— 为犯罪团伙获取金钱利益；
— 造成市场严重不稳并为选定的市场参与者创造获利机会。

取决于攻击的目标或目的，攻击者会试图利用不同的系统薄弱环节。这种攻击可能导致：

— 未经授权获取信息（丧失机密性）；
— 拦截和修改信息、软件、硬件等（丧失完整性）；

表 1. 内部威胁

攻击者	资源	持续时间	工具	动机
密探	推动“社交工程”。 一定程度上进入系统。 可获取系统文件和专门知识。	不等，但一般不能长时间逗留。	现有的访问，对编程和系统结构的了解： — 可能知道现行密码； — 能够插入专门制作的后门和（或）木马； — 可能有外部专家支持。	偷窃商业信息、技术秘密、个人信息。 经济上获利（向竞争对手出售信息）。 敲诈。
心怀不满的雇员/使用者	中等/雄厚资源。 一定程度上进入系统。 可获取关于具体业务和运行系统的系统文件和专门知识。	不等，但一般不能长时间逗留。	现有的访问，了解编程和系统结构。 可能知道现行密码。 能插入“kiddie（小子）”工具或脚本(如果其掌握特定的计算机技能，有可能做得更精巧)。	报复、破坏、制造混乱。 偷窃商业信息。 让雇主/其他雇员难堪。 降低公众形象或信誉。

表 2. 外部威胁

攻击者	资源	持续时间	工具	动机
娱乐性黑客	各种技能，但一般有限。 很少了解公众信息以外的系统。	时间很多，但却不是很有耐心。	一般可获得脚本和工具。 可能进行一些工具开发工作。	娱乐，地位。 机会目标。 利用“可轻易实现的攻击目标”。
核电站的激进反对者	资源有限，但可通过秘密渠道获得财政支持。 有机会获得网络社区的工具。 很少了解公众信息以外的系统。	攻击可能针对某些以往知晓的活动（如庆典、选举）。 时间很多，有耐心，也有积极性。	可获得计算机技能。 可能有来自黑客群体的支持。 “社交工程”。	确信能拯救世界。 改变有关特定问题的公众舆论。 妨碍业务活动。
心怀不满的雇员/使用者（不再受雇）	如果不参与较大的群体，资源有限。 可能仍拥有系统文件。 可能利用未加管理的以往访问手段。 与设施工作人员可能有联系。	不等，取决于相关人群。	可能知道现行密码。 可能利用未加管理的以往访问手段。 可能在仍为雇员时创建了系统后门。 “社交工程”。	报复、破坏、制造混乱。 偷窃商业信息。 让雇主/其他雇员难堪。 降低公众形象或信誉。

表 2. 外部威胁（续）

攻击者	资源	持续时间	工具	动机
有组织犯罪	雄厚的资源。 聘请网络专才。	不等，但大多短期。	脚本，自作工具。 可能聘请“待聘黑客”。 可能聘请前/现雇员。 “社交工程”。	敲诈。 偷窃核材料。 勒索（获利）。 利用企业在财务上和认识上的担忧。 获取（技术性、商业性或个人的）信息以便出售。
民族国家	雄厚的资源和专门知识。 情报收集活动。 可能的培训/系统操作经验。	不等。	接受过培训的网络专家组。 尖端工具。 可能聘请前/现雇员。 “社交工程”。	情报收集。 为以后的行动建立接入点。 偷窃技术。
恐怖分子	各种技能。 可能的培训/系统操作经验。	时间很多，很有耐心。	脚本，自作工具。 可能聘请“待聘黑客”。 可能聘请前/现雇员。 “社交工程”。	情报收集。 为以后的行动建立接入点。 制造混乱。 报复。 影响公众舆论（恐慌）。

— 数据传输线路阻塞和（或）系统关闭（丧失可用性）；
— 未经授权侵入数据通讯系统或计算机（丧失可靠性）。

所有这些方面均可能对计算机系统的功能带来重大后果和影响，从而对设施的安全和安保造成直接或间接的损害。在逐步建立攻击假想方案的过程中，应当考虑技术的趋势和攻击技术的轻松获取性。附件一列出了一些假想方案，以说明对核设施的虚拟且现实的攻击情况。

6.4. 风险评定的简化结果

表 3 仅为说明的目的列举了可能在核设施发现的系统的例子。该表确定了成功攻击对被考虑系统的潜在影响、对设施的相应影响以及适当的对策措施的一般例子。

该表未考虑对风险评价具有重要性的可能性概念。成功攻击的可能性以及潜在后果取决于所考虑的范围和设施。此外，就风险评定中所考虑的每个系统而言，还应当对机密性、完整性和可用性要求进行较为全面的评定。

7. 对核设施的特殊考虑

鉴于核工业的独特性，核设施的计算机安全必须解决对核工业以外的企业信息技术网络甚至类似过程控制系统的计算机安全关切之外的关切。以下各节叙述了与核工业相关的其中一些关切。

表 3. 核设施的典型系统

系统	对计算机安全的影响	对设施的潜在影响	建议的对策措施
反应堆保护系统	丧失安全关键软件/数据的完整性。 丧失功能可用性。	**决定性** 电厂安全受损，放射性释放。	1 级安全措施
过程控制系统	丧失控制软件/数据的完整性。 丧失功能可用性。	**高** 电厂运行受损。	2 级安全措施
作业许可和作业指令系统	丧失数据的完整性和系统的可用性。	**中** 对部件采取错误的行动。 正常运行和维护中断。	4 级安全措施
实际出入控制系统	丧失场址进入控制系统的可用性和完整性。 丧失场址进入数据的机密性。	**高** 使未授权人员有机可乘。 受权人员被阻止进入需要进入的区域。	2 级安全措施
文件管理系统	丧失机密性、可用性和数据完整性。	**中** 信息被用于策划更严重的攻击。	4 级安全措施
电子邮件	丧失机密性、完整性和可用性。	**低** 行政负担。 日常运行变得更加困难。	5 级安全措施

7.1. 设施寿期阶段和运行模式

核设施具有各种广泛的设计和运行特点。它们拥有多个寿期阶段和运行模式，其中包括：

— 设计、建造和调试。
— 运行：
  - 功率运行；
  - 机组启动；
  - 热停堆；
  - 冷停堆；
  - 换料和维护。
— 退役。

这些多个寿期阶段和运行模式可能涉及不同的系统以及同样不同的运行环境。例如，密集维护期常常涉及设备更换、改造和测试，或者可能要求额外的工作人员和第三方/承包商进入。在计算机安全计划中应考虑到这种多样性。特别是不同的寿期阶段可能意味着对计算机安全计划做出很大的修改。

7.2. 信息技术系统与工业控制系统之间的区别

就结构、配置或性能要求而言，支持核电厂运行的计算机系统和网络结构并不是标准计算机系统。这种系统可以归于专业化工业控制系统一类。尽管工业控制系统已从严格的专有实施发展为更为主流的计算机结构，但工业控制系统与标准信息技术系统之间仍存在显著的区别，因此，在任何场址安保计划中都必须对此加以考虑。

表 4 基于国家标准和技术研究所提供的资料拟订[20]，对工业控制系统与传统的信息技术系统之间的主要区别作了介绍。

表 4. 信息技术系统与工业控制系统之间的区别[20]

类别	信息技术系统	工业控制系统
性能要求	非实时 响应必须一致 需要高通过量 可以接受高延迟和抖动	实时 响应时间关键 适中的通过量可以接受 高延迟和（或）抖动属于严重关切的问题
可用性要求	重新启动等响应可以接受 可用性缺陷常常可以忍受，取决于系统的运行要求	由于过程可用性要求，重新启动等响应不可接受 中断必须提前数天/数周计划并列入时间表 高可用性要求进行彻底的部署前测试
风险管理要求	数据机密性和完整性至高重要 容错不那么重要 — 短暂停机不属于主要风险 主要风险影响是业务活动延迟	人的安全最为重要，其次是保护过程 容错是必需的，即使短暂停机也是不可接受的 主要风险影响是违反监管规定以及生命、设备或生产损失
结构安保重点	最重要的是保护信息技术资产以及这些资产所储存的或在相互之间传输的信息 中央服务器可能需要更多的保护	首要目的是保护边缘客户端（如过程控制器等现场装置） 中央服务器的保护仍很重要
不希望的后果	安全解决方案围绕典型的信息技术系统设计	必须对安全工具进行测试，以确保其不损害正常的工业控制系统运行
时间紧迫的互动	应急互动不那么关键 可以实施必要程度的有严格限制的访问控制	对人员和其他应急互动的响应十分关键 进入工业控制系统应严格加以限制，但不应妨碍人机互动
系统运行	系统系为与典型的运行系统一同使用而设计的 有自动化部署工具便可直接进行升级	不同的定制运行系统，常常不具备安全能力 软件修改必须仔细进行，而且通常由软件供应商进行，因为有专门的控制算法，也许还涉及同时修改硬件和软件
资源制约	系统被规定拥有足够的资源，以支持增加第三方应用程序，如安全解决方案	系统的设计旨在以最少的记忆和计算资源支撑预期的工业过程，从而为增加安全技术提供支持
通讯	标准通讯协议 主要是具有某些本地化无线能力的有线网络 典型的信息技术组网实践	许多专有和标准通讯协议 使用了若干种通讯介质，包括专用有线和无线介质（无线电和卫星） 网络颇为复杂，有时需要控制工程师的专门知识
修改管理	按照良好安全政策和程序及时进行软件修改。程序常常是自动化的	软件修改后必须经过全面测试，并在整个系统内逐步加大部署力度，以确保控制系统的完整性得以保持工业控制系统中断常常必须提前数天/数周计划并列入时间表
管理支持	允许多样化的支持方式	服务支持通常通过单一卖方提供
部件寿命	寿命大约在 3－5 年之间	寿命大约在 15－20 年之间
部件供应	部件通常为本地部件，且易于获得	部件可能是被隔离的、远距离的，需要做出广泛的实际努力才能取得

7.3. 对额外连接性的要求和相关后果

工业控制系统越来越令人关切的一个领域是人们越来越希望运行系统的商务系统与工程系统之间互联互通。在公司总部、规划者和工程师获取实时电厂数据愿望的驱动下，正在受严格限制的电厂运行控制网络与供企业接入的无限数据网络之间架设桥梁。该桥梁可能成为一个网络侵入的途径。

另一个独特的结构特点是远程应急操作中心的存在。这种应急操作中心提供了一个远距离场所，以便在事件使得主站无法使用的情况下对电厂进行监测和应急操作。对电厂控制的某些要素进行监测/维护的要求造就了对某种通讯介质上的数据流的需求。该介质提供了损害和进入主系统的潜在途径。此外，对复制功能的要求还造就了对两个系统保持一致的安全要求的需要。保持单一系统的失败可能形成侵入和利用式注入的途径。

对远程分析、维护或升级的需求还可能产生类似的漏洞。在就这种额外的连接性达成一致之前，必须开展全面的风险分析。

7.4. 对软件升级的考虑

现行有关验证或鉴定核电厂设备的许多规章都是在考虑到模拟设备的情况下制定的。这些规章不会很快过时。另一方面，信息技术安全计划和最佳实践意味着软件和数字部件的定期升级和修补，因为这些部件的过时要比规章快得多。

因此，必须要在数字核控制或监测系统中考虑软件修补和升级所构成的挑战。在最坏情形假想方案中，每一次软件修改或修订均可以被视为一次系统修改，并可能导致进行一次特定的系统验证甚至对某些关键系统进行重新鉴定。由于这一方案十分麻烦，其结果可能是补丁实施工作出现积压，或者有意识地决定延后进行软件升级。为了限制这种后果，应当将避免上述过程的正常维修与需要重新测试甚至重新鉴定关键系统的系统修改区分开来。在所有情况下，对安全或安全相关系统以及对安保系统的任何修改都必须按照商定的程序进行。

7.5. 计算机系统的安全设计和技术规格

在许多现有过程控制和工业控制系统和仪器仪表的最初设计和开发过程中，计算机安全并不是一项主要考虑。最近对系统和过程间连接性的推动、商业现货计算机系统的一体化和恶意计算机活动（如黑客行为）的出现已使得有必要考虑将计算机安全作为新设备采购中的一个核心要求。

因此，作为与供应商合同谈判的一部分，应当完成安全要求的正规化。标准化组织文件“通用标准”（ISO 15408）[21]是将这种安全要求正规化的一种可能的工具。在美国国土安全部制订“控制系统采购用语”[22]的尝试中可以找到另一个例子，该部出版了关于规定网络安全要求以及控制系统专用采购用语的导则和建议。

7.6. 第三方/卖方访问控制程序

必须考虑到任何第三方和卖方的安全水平。最重要的是安全部门要与合同部门密切合作，以确保安全条款纳入每份合同。

合同常常由核工业中的组织授予外部实体；其中一些合同将必然导致签约公司在其公司所在地持有带防护标识的信息或资产。除非这种合同的授予及其随后的管理遵循严格的规则，否则，与合同有关的这种带防护标识的信息或资产就可能冒着受损害或未经授权公开的危险。

考虑到上述因素，核工业的每个场址/组织的主管管理层必须与签约公司保持密切的工作关系，以确保重要的安全问题在合同的拟定和实施过程中以及在最后移交期间得到处理。

如果认为必要，应当进行检查和审核，以确保签约组织的管理系统适当处理安全问题，并确保该组织的实践和措施符合该系统的规定。

参 考 文 献

[1] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology — Security Techniques — Information Security Management Systems — Overview and Vocabulary, ISO/IEC 27000:2009, ISO, Geneva (2009).

[2] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology — Information Security Management Systems — Requirements, ISO/IEC 27001:2005, ISO, Geneva (2005).

[3] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology — Code of Practice for Information Security Management, ISO/IEC 27002:2005, ISO, Geneva (2005).

[4] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology — Security Techniques — Information Security Risk Management, ISO/IEC 27005:2008, ISO, Geneva (2008).

[5] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology— Security Techniques — Requirements for Bodies Providing Audit and Certification of Information Security Management Systems, ISO/IEC 27006:2007, ISO, Geneva (2007).

[6] COUNCIL OF EUROPE, Convention on Cybercrime, ETS No. 185, COE, Strasbourg (2001).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, The Management System for Facilities and Activities, IAEA Safety Standards Series No. GS-R-3, IAEA, Vienna (2002).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Application of the Management System for Facilities and Activities, IAEA Safety Standards Series No. GS-G-3.1, IAEA, Vienna (2006).

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Culture, IAEA Nuclear Security Series No. 7, IAEA, Vienna (2008).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Physical Protection Objectives and Fundamental Principles, Resolution GOV/2001/41, IAEA, Vienna (2001).

[11] The Physical Protection of Nuclear Material and Nuclear Facilities, INFCIRC/225/Rev.4 (Corrected), IAEA, Vienna (1999).

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Guidance and Considerations for the Implementation of INFCIRC/225/Rev.4, The Physical Protection of Nuclear Material and Nuclear Facilities, IAEA-TECDOC-967 (Rev.1), IAEA, Vienna (2000).

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Instrumentation and Control Systems Important to Safety in Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.3, IAEA, Vienna (2002).

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Software for Computer Based Systems Important to Safety in Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.1, IAEA, Vienna (2000).

[15] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Safety Glossary: Terminology Used in Nuclear Safety and Radiation Protection — 2007 Edition, IAEA, Vienna (2007).

[16] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology — Security Techniques — Management of Information and Communications Technology Security — Part 1: Concepts and Models for Information and Communications Technology Security Management, ISO/IEC 13335-1:2004, ISO, Geneva (2004).

[17] EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY, Inventory of Risk Management/Risk Assessment Methods and Tools, http://www.enisa.europa.eu/act/rm/cr/risk-management-inventory/rm-ra-tools.

[18] INTERNATIONAL ATOMIC ENERGY AGENCY, Development, Use and Maintenance of the Design Basis Threat, IAEA Nuclear Security Series No. 10, IAEA, Vienna (2009).

[19] INTERNATIONAL ATOMIC ENERGY AGENCY, Preventive and Protective Measures Against Insider Threats, IAEA Nuclear Security Series No. 8, IAEA, Vienna (2008).

[20] STOUFFER, K.A., FALCO, J.A., SCARFONE, K., Guide to Industrial Control Systems (ICS) Security — Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations such as Programmable Logic Controllers (PLC), Rep. NIST SP-800-82, National Institute of Standards and Technology, Chicago (2011).

[21] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Information Technology — Security Techniques — Evaluation Criteria for IT Security, ISO/IEC 15408:2008, ISO, Geneva (2008).

[22] UNITED STATES DEPARTMENT OF HOMELAND SECURITY, Cyber Security Procurement Language for Control Systems, September (2009), http://www.us-cert.gov/control_systems/pdf/FINAL-Procurement_ Language_Rev4_ 100809.pdf

[23] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Risk Management — Vocabulary, ISO/IEC Guide 73:2009, ISO/IEC, Geneva (2009).

该出版物已被第 No. 17-T (Rev. 1) 号取代。

文 献 目 录

AMERICAN NATIONAL STANDARDS INSTITUTE, INTERNATIONAL SOCIETY FOR AUTOMATION, Security Technologies for Industrial Automation and Control System, ANSI/ISA-TR99.00.01-2007, ANSI, Washington DC, (2007).

FEDERAL MINISTRY OF THE INTERIOR, National Plan for Information Infrastructure Protection, BMI, Berlin (2005).

INTERNATIONAL ATOMIC ENERGY AGENCY, Physical Protection Objectives and Fundamental Principles, Resolution GOV/2001/41, IAEA, Vienna (2001).

INTERNATIONAL SOCIETY FOR AUTOMATION, Integrating Electronic Security into the Manufacturing and Control Systems Environment, Instrumentation, Systems and Automation Society, ISA-TR99.00.02-2004, ISA, Research Triangle Park, NC (2004).

KOREA INSTITUTE OF NUCLEAR SAFETY, Cyber Security of Digital Instrumentation and Control Systems in Nuclear Facilities, KINS/GT-N09-DR, KINS, Seoul (2007).

NATIONAL INFRASTRUCTURE SECURITY CO-ORDINATION CENTRE, Good Practice Guide: Process Control and SCADA Security, Version 2.0, NISCC, November (2006).

NUCLEAR ENERGY INSTITUTE, Cyber Security Plan for Nuclear Power Reactors, NEI 08¬09 (Rev. 5), NEI, Washington DC (2010).

NUCLEAR REGULATORY COMMISSION, Cyber Security Programs for Nuclear Facilities, Regulatory Guide 5.71, NRC, Rockville, MD (2010).

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, OECD, Paris (2002).

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, Implementation Plan for the OECD Guidelines for the Security of Information Systems and Networks-Towards a Culture of Security, DSTI/ICCP/REG (2003) 5/REV1, OECD, Paris (2003).

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, The Promotion of a Culture of Security for Information Systems and Networks in OECD Countries, DSTI/ICCP/REG (2005) 1/FINAL, OECD, Paris (2005).

附件一

攻击核设施系统的假想方案

如第 6.3 节所述，基于计算机的攻击的性质和形式可能有很大差别，但都必须加以防范。尽管这种攻击可能有不同的类型，但其严重的后果包括：

— 未经授权获取或拦截信息（丧失机密性）；
— 未经授权修改信息、软件、硬件等（丧失完整性）；
— 数据传输线路阻塞和（或）系统关闭（丧失可用性）。

在制订防范计算机攻击的预防措施时，必须了解攻击的性质和攻击或攻击者可能用来获取相关信息和进入目标计算机系统的潜在地点。**以下仅是用于鼓励读者在更多地了解威胁之后反思自己所在的组织/系统并在必要时对安保特征作出相应改变的例子。**所描述的攻击尽管属于虚构，但却与根据在其他行业所见类似攻击拟订的看似合理的假想方案有关。对于确保安全计划涉及不断变化的威胁环境背后的力度而言，仔细思考这种假想方案直至得出结论是一种很好的方法。

一次精心策划的计算机攻击由多个阶段组成。这些阶段包括：

— 确定目标；
— 侦察；
— 进入/损害系统；
— 执行攻击；
— 掩盖痕迹，以保持可否认性。

以下分节列举了三种虚构的计算机攻击假想方案。第一种假想方案将信息收集作为目标之一，可以作为前奏适用于后面两个假想方案。

假想方案 1 — 收集信息以支持恶意行为

攻击目的 — 取得对设施控制（有限进入）区的实际进入，以支持后续攻击。

感兴趣的目标是管理出入证和分配进入特权的人。取得对限制区的实际进入的内容包括损害出入证管理人的计算机和损害进入密码系统。攻击者选择伪装成供应设备零件的分包商。

收集信息以支持攻击的可能的目标包括：

— 用于可能的勒索或“社交工程”的人员信息；
— 出入控制系统的设计文件；
— 电厂安保系统或其他相关方面的政策和工程计划；
— 工作计划表 — 工厂调度表、作息表、谁正在工作、什么时候工作、谁在休假、什么时候出现了某些改变；
— 供应商名单和它们什么时候在为设备进行工作；
— 设备和零件库存；
— 密码和出入控制措施；
— 出入控制的行政和技术措施；
— 软件开发者和当前项目信息；
— 网络结构；
— 电信结构。

收集这种信息的潜在方法包括：

— “社交工程”；
— 公开信息网上搜索；
— 垃圾搜寻；
— 战争拨号，战争驾驶；

— 电子邮件攻击 —“钓鱼”[1] 以取得网络进入，键盘记录器；

— 在主机上通过磁盘、记忆卡或光盘安装软件或装置；

— 窃听密码输入或进入代码输入（人工、音频或视频监视）。

攻击的组成部分可能包括：

— 取得出入证（磁卡）和代码；

— 偷窃/复制现有出入证；

— 利用卡片机制作新证；

— 创建新的雇员条目；

— 假冒新近解聘雇员的身份；

— 给予希望的访问级别。

一旦取得卡和代码，攻击者便利用所取得的信息开展组织活动，以便作为提供设备零件的人不引人注目地进入设施。

假想方案 2 — 瘫痪或损害一个或若干个计算机系统的攻击

攻击目的 — 破坏核电厂和防止电厂立即重新启动。

在本例子中，在电厂关闭期间，分承包商正在进行给水控制系统测试。该承包商安装了从其办公室监测和测试该系统所用的远程接入点。在该承包商完成工作后，该接入点仍错误地存在。

攻击者收集了确定该分承包商为该厂以前的工作人员和有关该厂信息的首要目标的电厂信息。攻击者针对该分承包商的办公室进行电子邮件“钓鱼”攻击，并在该系统中植入了一个根工具包，以进行行政控制。攻击者因此取得了对该承包商计算机网络的进入，并发现了该厂的测试计划以及尚未被该厂去功能化的远程接入端口。

[1] “钓鱼”系指在电子信函中通过伪装成值得信赖实体的方式欺诈性地获取敏感信息如用户名、密码和信用卡资料的企图。

有了这一信息，攻击者便可以通过使网络涌入造成系统故障的流量的方式对给水控制系统进行拒绝服务[2]攻击。系统被设计成仅处理最低流量负载。

一旦攻击者取得进入、绘制网络图谱并确定通讯协议，他便开始攻击。攻击将导致给水控制系统失去响应，从而造成电厂手动紧急停堆。给水控制系统故障的原因不能立即得到确定，电厂仍被关闭，以接受调查。

假想方案 3 — 损害计算机系统作为一种协同攻击手段

攻击目的 — 偷窃在贮存设施之间运输的核材料。计算机攻击将被用于修改库存和跟踪系统，以隐瞒被盗材料丢失情况。

侦察和情报收集确定贮存设施之间放射性物质运输的标记和跟踪过程。这包括描述组成部分和列出内容物的各物项的射频识别[3]标签。

攻击计划包括内线协助搬运在途物质。攻击阶段包括：

— 拦截在途运输；
— 搬走少量运输中的放射性物质；
— 对射频识别芯片进行重新编程，以反映所剩的实际数量；
— 修改库存跟踪系统，以反映正在运输的新数量，而被盗的数量仍贮存在原设施中。

计算机攻击的重点是取得对存量数据库的网络进入并修改存量和转运记录。

---

[2] “拒绝服务”就是防止未经授权利用系统资源或延迟系统运行和功能。

[3] 射频识别：利用无线电波进行识别和跟踪的技术。

附件二

确定计算机安全要求的基本方法

应当按照现行标准以系统化和一致的方式实施确定、控制、消除或最大程度减少可能影响核设施计算机安全的威胁的过程。本附件对一种具体的方法学做了较深入的考察。选择该方法而不是许多其他可利用的方法并不意味着原子能机构认可该方法，而应仅被视为一个详细的例子。关于风险评定的一般介绍，请参见第 6.1 节。

一般而言，为了了解特定计算机化系统的威胁和薄弱环节，首先必须对该系统进行功能和技术上的分析，并确定需要加以保持的相关依赖性因素。接下来有必要确定和分析与这些因素有关的风险。

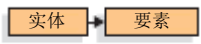
以下段落对“表达需求和确定安保目标”作了概述。“EBIOS（表达需求和确定安保目标）”是代表 *expression des besoins et identification des objectifs de sécurité* 的一个法文首字母缩略词。该词是由法国信息安全中央办公室设计的。[1]

EBIOS 提供了评定和处理信息系统安全领域风险（包括签约当局所用的辅助工具）、起草文件和提高认识的正规方案。

本附件仅提供了根据法国信息安全中央办公室辅助网站上提供的文件改编的该方案的各项基本原则。

EBIOS 方法的各项原则

研究背景和确定范围



第一步是概述这项研究的技术、业务和监管背景。特别是信息系统以构成组织内部信息系统附加值的**基本要素**、功能和信息为基础。

[1] 实现信息系统安全的方法：http://www.ssi.gouv.fr/site_rubrique113.html。

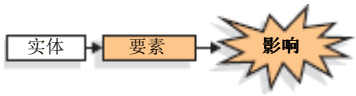
例如，电厂冷却系统的监测系统依靠措施、参数和计算结果等各种信息项目以及允许进行这种计算的各种功能。

这些基本要素与各种类型的一系列**实体**相联系：硬件、软件、网络、组织、人力资源和场址。

以触发冷却系统特定循环泵启动所用的参数为例。与其有联系的有监测计算机、处理软件、营运者、冷源状态、电厂状态、适用的规章等。

产出：研究目标（背景+要素+实体）。

敏感性表述



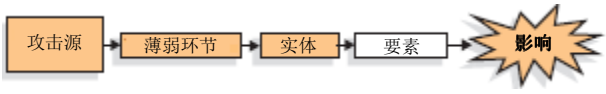
为了保证业务的正确进行，必须对每一基本要素的**敏感性**做出表述。

这种表述基于各种**安全标准**，如可用性、完整性和机密性。如果不将这种敏感性包含在内，就会给组织带来**影响**，而这种影响可能呈现各种形式，如违反核安保、损害安全、对活动运行造成损害、失去客户信任或经济损失。

回到电厂冷却系统循环泵启动参数的例子，对这种信息的可用性和完整性应有很高的要求，以避免对材料、环境或人员以及电厂可利用率带来不利影响。

产出：敏感性。

威胁研究



每个组织都通过其自然环境、文化、形象、活动领域等暴露在各种威胁因素之下。可以通过威胁因素的类型（自然的、人为的或环境的）和起因（意外的或故意的）对其进行表征。

威胁因素可以采用因此需要加以确定的各种**攻击方法**。攻击方法通过

其可能侵犯的安全属性（如可用性、完整性、机密性）和可能的威胁因素进行表征。

回到例子，核电厂必须考虑第 6.3 节所阐述的大量威胁因素：

- 间谍行为/偷窃技术；
- 心怀不满的雇员/使用者（内部或外部）；
- 娱乐性黑客；
- 网上活跃分子；
- 有组织犯罪；
- 民族国家；
- 恐怖分子。

还有攻击方法：

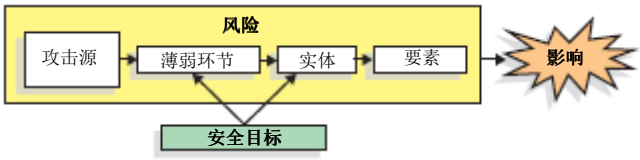
- 窃听；
- 灌水/拒绝服务；
- 软件诱骗/后门；
- 登录/密码攻击（蛮力攻击，词典攻击等）。

每个实体都有威胁因素可以通过利用相关攻击方法加以利用的**薄弱环节**。因此，我们可以突出强调与核电厂冷却系统有关联的若干薄弱环节：

- 可能存在在设计和开发阶段加入的隐藏功能（软件）；
- 使用未经评定的设备（硬件）；
- 在线创建或修改系统命令的可能性（网络）；
- 可能被用于窜改系统资源软件的网络（网络）；
- 很容易通过间接接入路径侵入场址（工作场所）；
- 操纵员不遵守指令（工作人员）；
- 设计、安装和运行阶段没有安保措施（组织）。

产出：威胁正式化（包括假想方案）。

安全目标的表述



现在确定基本要素如何受威胁因素及其攻击方法的影响：这就是**风险**。

这种风险代表着可能的损害。它产生于这样一个事实，即威胁因素可以通过采用特定攻击方法来利用基本要素所依赖的实体的薄弱环节的方式对基本要素产生影响。

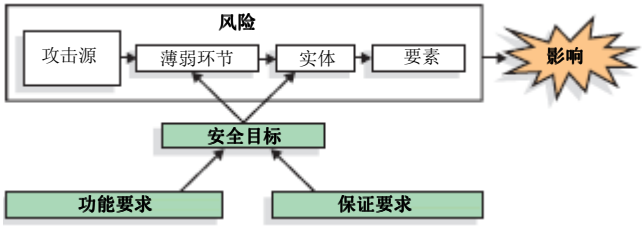
在本例子中，存在着由创建或修改与网络有联系的系统命令的可能性所引起的敏感信息被通过软件诱骗方式损害的风险，这种风险可能对材料、环境、人员安全、电厂可利用率和公众信任产生影响。

安全目标主要在于弥补实体存在的代表了所有保留风险的薄弱环节。对尚未暴露出来的风险提供保护显然没有任何作用。但随着风险潜力的上升，安全目标的强度也必须随之增加。这些目标因此构成一套完全适应的技术规格。

例子中的核电厂安全目标之一是就创建和修改冷却系统中与网络有联系的系统命令提供保护。

产出：安全目标。

确定安全要求



负责方案实施的团队随后必须拟订必要安全功能的确切技术规格。此后，该团队还必须证明这些**功能要求**完全覆盖了安全目标。

在本例中，就创建和修改与网络有联系的系统命令提供保护的功能要求包括：

— 系统在正常运行期间按定期间隔进行一系列自我测试，以证明其正在正确运行；

— 物理和逻辑访问控制。

最后，该负责团队必须具体列出**保证要求**，以促使达到并随后展现必要的置信任度。

保证要求之一可以是开发者必须按必要的阻力水平对系统安全功能进行阻力分析。

产出：功能要求和保证要求。

附件三

人为失误在计算机安全中的作用

本附件考察与计算机安全有关的人员绩效问题，并特别审视人员绩效如何影响一个组织抵御攻击、确认攻击、恢复基本数据/服务以及适应正在出现的威胁的能力。研究工作继续力争制订技术解决方案，如安全监测软件、侵入探测/预防计划、更强有力的验证系统以及更有抵抗力的加密方法，但却常常忽视了作为原因和作为计算机安全防范措施的人为因素。

多份报告已将人为失误确定为计算机安全破坏行为的主因。最新的估计是人为失误相关破坏行为的数量在 60－80%之间。大多数失误本可以通过加大对宣传的投入和在运行和监督方面更加勤勉而得以避免。

系统/运行可存活性是计算机安全计划的目的之一。系统可存活性的要素有：

— 系统抗攻击性；
— 确认攻击和损害评定；
— 基本服务和服务全面恢复；
— 作为未来攻击防御手段的系统适应和发展。

表 3-1 举例说明了这些重点领域，并尝试对过程和应用中常见类型的人为失误进行了归类。捕捉的人为失误既有系统管理者的，也有系统使用者的。该清单并未打算做到详尽无遗，但却旨在举例说明与这些系统和过程的实施有关的人际互动水平。

尽管该表侧重于人员绩效的消极方面，但还必须注意人员绩效的积极影响。人操作者即雇员有时属于链条中最弱的一环，但却可能是防止系统故障或受损的闸门。技术永远不会是彻底的解决方案。雇员是确保系统安全/可存活性的纵深防御战略中的一个层级。调查经常发现，最重要的安全问题是计算机安全宣传和培训不足。

表 3-1. 常见人为失误

过程/应用	常见人为失误
抗攻击性	
进入限制（系统管理）	— 文件权限不足。 — 设置了多余服务。 — 打开了易受攻击端口。 — 准许实际进入。 — 未采用带密码的屏幕保护程序。 — 未安装系统补丁。 — 未了解安装补丁的意义。 — 下载/安装恶意/损坏的软件。
密码生成/使用	— 写下了密码。 — 密码效力弱。 — 使用缺省密码。 — 密码被披露。 — 不使用密码。 — 在安全和非安全系统上使用同样的密码。
确认攻击和损害	
侵入探测系统	— 配置不当（规则集）。 — 不做系统升级。 — 登录审查方面缺乏警惕。
登录审核	— 登录审查不勤。 — 未注意多个登录期的趋势。

表 3-1. 常见人为失误（续）

过程/应用	常见人为失误
系统恢复	
备份和恢复	— 未做备份。 — 未及时备份。 — 配置不当。 — 给备份介质造成实际损害。 — 意外删除数据。 — 将备份介质储存在未实施安全/未予保护的场所。 — 使用有缺陷的介质。 — 给介质贴上错误标签。 — 对介质造成实际破坏。 — 未测试恢复程序。 — 未制作多份关键系统信息。 — 未将备份介质储存在场外地点。
适应新威胁	
公司程序	— 不知晓公司政策。 — 违反公司政策。 — 缺乏公司恢复政策。 — 采用过时的政策。 — 未核实政策/程序工作。 — 未执行政策。

雇员要想作为计算机安全系统可存活性方面有价值的人充分发挥作用，就需要：

— 充分了解其在总体计算机安全计划中的作用；
— 履行职责所需的计算机安全知识和技能；
— 理解有效的安全文化从他们开始。

定　义

为本出版物的目的，以下术语具有术语之后所给定的含义。这些定义可能不同于其他学科中的用法。定义尽可能取自原子能机构现有出版物，但本出版物中的若干术语是在计算机安全的具体背景下使用的。其他定义来自国际标准（如本出版物参考文献[1、15、23]）。

出入控制　意在确保对资产的接触得到授权并根据商业和安保要求加以限制（标准化组织）。

攻击　摧毁、暴露、改变、瘫痪、偷窃或未经授权接触或使用资产（标准化组织）。

验证　提供关于所称实体的特点是正确的保证（标准化组织）。

可用性　可应受权实体的要求而获得和使用的特性（标准化组织）。

计算机安全　信息安全中与基于计算机的系统、网络和数字系统有关的特定方面。

计算机安全事件　实际或潜在危及基于计算机的、网络化的或数字的信息系统的机密性、完整性或可用性或危及系统处理、储存或传送的信息或构成对安全政策、安全程序或可接受的使用政策的违反或即将发生的违反危险之信息的事件。

计算机安全范围　关键资产与之相联系且其接触受到控制的网络的逻辑边界。

计算机安全政策　规定一个组织如何管理和保护计算机和计算机系统的指令、规章、规则和实践的集合。

机密性　不向未得到授权的个人、实体或过程提供或披露信息的特性（标准化组织）。

对策措施 为抵消威胁或消除或减少薄弱环节所采取的行动。

纵深防御 用于保护核安保威胁目标的连续多层系统和措施的组合。

信息安全 保护信息的机密性、完整性和可用性。

注：此外，还可以包括真实性、可说明性、不可否认性和可靠性等其他特性（标准化组织）。

完整性 保护资产精确性和完全性的特性（标准化组织）。

需要知晓 使用者、过程和系统被准许仅接触执行受权职能所需的信息、能力和资产的原则。

核设施 生产、加工、使用、处理、贮存或处置核材料且需要批准书或许可证的设施，包括相关建筑物和设备。

风险 某一威胁利用一项资产或一组资产的薄弱环节从而给组织造成损害的可能性。对这种风险要将发生事件的可能性与其后果的严重程度结合起来进行衡量。

风险评定 系统地确定、估计、分析和评价风险的总体过程。

社交工程 依靠人际交往来操纵个人非故意地违反安全程序（如披露信息或开展有安全影响的其他行动）的一种非技术形式的信息收集或攻击手段。

威胁 可能导致危害系统或组织的有害事件的潜在原因（标准化组织）。

注：在原子能机构其他《核安保丛书》出版物中，“威胁”一般被定义为“具有实施恶意行为的动机、意图和能力的个人或团伙”。但本出版物在其威胁不一定是人的计算机安全的范围内使用这一术语。

薄弱环节（漏洞） 资产或控制中可以被威胁加以利用的弱点（标准化组织）。

该出版物已被第 No. 17-T (Rev. 1) 号取代。

12-12795

本出版物旨在形成对将计算机安全纳入作为核设施总体安保计划一个基本部分的重要性的认识。本出版物还旨在为核设施提供关于实施计算机安全计划的导则，并提供关于评价现有计划、评定关键数字资产和确定以适当的方式降低风险措施的意见。

国际原子能机构
维也纳
ISBN 978–92–0–536110–9
ISSN 1816–9317