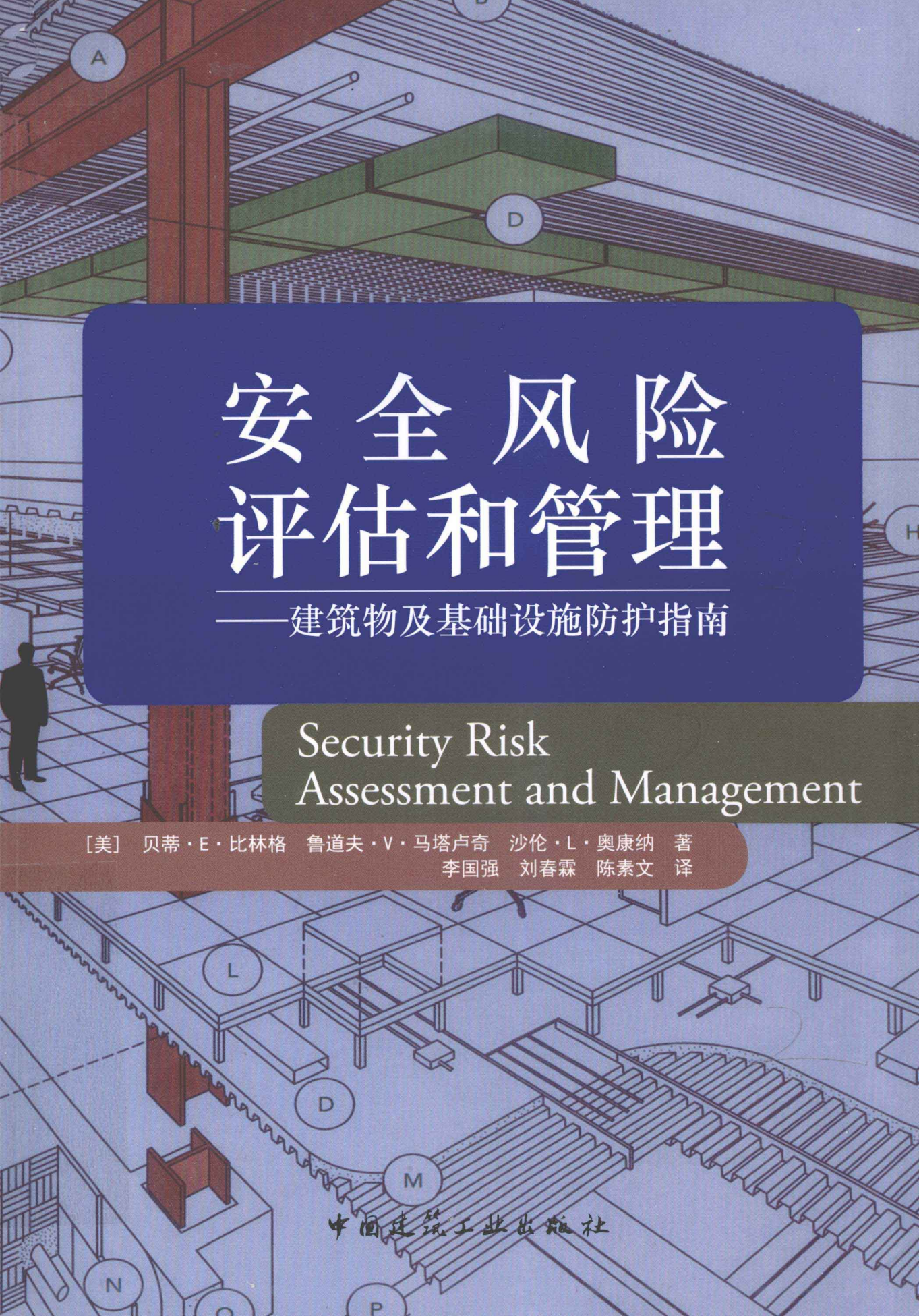

安全风险评估和管理

——建筑物及基础设施防护指南

Security Risk Assessment and Management

[美] 贝蒂·E·比林格 鲁道夫·V·马塔卢奇 沙伦·L·奥康纳 著
李国强 刘春霖 陈素文 译

中国建筑工业出版社

安全风险评估和管理

——建筑物及基础设施防护指南

贝蒂·E·比林格
[美] 鲁道夫·V·马塔卢奇 著
沙伦·L·奥康纳

李国强 刘春霖 陈素文 译

中国建筑工业出版社

著作权合同登记图字：01-2009-2085号

图书在版编目(CIP)数据

安全风险评估和管理——建筑物及基础设施防护指南 /（美）比林格，马塔卢奇，奥康纳著；李国强，刘春霖，陈素文译.—北京：中国建筑工业出版社，2012.5
ISBN 978-7-112-13902-6

Ⅰ.①安… Ⅱ.①比…②马…③奥…④李…⑤刘…⑥陈… Ⅲ.①建筑物-安全评价②建筑物-安全管理③基础设施-安全评价④基础设施-安全管理 Ⅳ.①TU714

中国版本图书馆CIP数据核字（2011）第277575号

责任编辑：赵梦梅 董苏华
责任设计：赵明霞
责任校对：姜小莲 赵 颖

安全风险评估和管理
——建筑物及基础设施防护指南

[美] 贝蒂·E·比林格
鲁道夫·V·马塔卢奇 著
沙伦·L·奥康纳
李国强 刘春霖 陈素文 译

*
中国建筑工业出版社出版、发行（北京西郊百万庄）
各地新华书店、建筑书店经销
北京嘉泰利德公司制版
北京建筑工业印刷厂印刷
*
开本：787×1092毫米 1/16 印张：14 字数：350千字
2012年7月第一版 2012年7月第一次印刷
定价：46.00元
ISBN 978-7-112-13902-6
（21891）

谨以此书献给早在“9·11”事件（2001年9月）之前就已承诺保障和防护国家关键基础设施安全并为之献计献策的基础设施防护论坛的志愿者！

前　言

我们的目的是向工程师、建筑师、安全专业人员、执法和应急管理人员以及对建筑物和基础设施的住户和业主的安全环境负有责任的管理人员提供一本最好的专业指导书。为了防止建筑物及住户受恶意行为的破坏，建立一个安全风险评估管理流程是必要的，因为它可以：(1) 识别一个区域性的、可能且可信的具体场所受到的可能威胁，以及基本威胁的连锁发展；(2) 评估后果，包括生命财产损失、经济影响、其他具有意义的损失以及公众信心的丧失；(3) 评估实体安全和网络安全系统在威胁下的失效，并且识别和确定安全系统中的所有薄弱环节。

我们旨在提供一套系统的且可靠的安全风险管理方法，以帮助业主和管理人员完成一项完整的风险评估，并作出接受评估的风险或把风险减少到可接受的水平的决定。通过基于性能的可多选择的提升安全或减轻后果的措施，提出可行的减少风险的策略流程。

随着民众对防止恐怖主义造成生命和财产损失采取适当措施的需求的增长，各种可选择的且证明有效的安全措施，反映出现行条文式的建筑物规范的局限性。目前，建筑物基本安全标准的清晰定义很少，尤其是在民用和商业设施方面，受恐怖威胁的建筑物基本安全标准的清晰定义甚至还没有，防护通常基于一定假设的威胁和针对假定的防护系统的弱点。

2001 年“9 · 11”事件以来，运用一种有效的方法去判定建筑物新的安全需求的必要性更加显著，施行一项严格的安全风险管理方法符合国家利益。这种安全风险管理方法已经应用于一些联邦政府设施，并且可以有效地判断某种防护程度需求的合理性。这种方法也可以用于证明安全升级或减小后果措施的效果，确保投资的有效回报。

一个可行的风险管理流程如果使用得当，还能剔除任何形式的伪安全，这些伪安全来自不适宜的安全措施构思和不恰当的安全措施升级或降低计划的判断。

本指导书采纳较可靠的安全措施和技术，这些措施和技术由美国国家能源安全实验室开发，已在美国应用。本书介绍的风险管理方法和系统流程已从原来广泛应用的基于规范条文式规定的安全防护流程向基于性能的系统评估发展。我们不再认为，按条文式的标准安全规范所完成的项目是足够安全的。我们希望将来在任何意识到的或建议的防护行为实施前，采用基于风险管理的方法进行安全评估和分析。这本“最佳实践”指导书希望能给专业人员提供必要的指导，并且进一步能够帮助他们进行安全风险管理，逐步达到降低风险和确保足够安全的目标。

若要获取更多的资料，请浏览网址：www.wiley.com/go/securityrisk。

致　谢

感谢技术评审（特别是 Ivan Waddoups 和 Greg Wyss）大量有益的意见和建议，使本书内容和叙述过程得到极大的改进。十分感谢 Elizabeth Affeldt 和 P. Rebecca Baca 为本书所作的高效而细致的文本编辑工作，特别是 Ktech 公司技术部的 Jackie Ripple，她花费了大量时间，为本书的文字和图形编辑作出了贡献。感谢桑迪亚（Sandia）国家实验室的 Tommy Woodall 和 Carla Ulibarri 为本书提供的管理支持。

感谢所有为风险评估方法提出长远建议和支持的人员。基础设施安全风险评估方法学的原型由桑迪亚国家实验室为基础设施防护论坛组织 Interagency Forum for Infrastructure Protection（IFIP）所开发。IFIP 的创始成员包括美国陆军工程兵部队、废物回收局、田纳西河谷管理局、联邦调查局、邦纳维尔（Bonneville）电力管理局、西部地区电力管理部门和桑迪亚国家实验室，如果没有这些成员在经费和技术上的支持，本书将无法成功出版。

我们必须记住桑迪亚国家实验室前工作人员 William K. Paulus 对整个风险评估方法学流程的发展在技术上所作的贡献，他在故障树的应用、风险评估与计算、风险表格化和威胁评估流程方面的贡献是难以估量的。

十分感谢桑迪亚国家实验室董事 Dennis Miyoshi 的长期支持、关心和资助，使得本书的编写既获得了技术上的肯定，也得以顺利完成。没有他的指导和鼓励，本书是不可能完成的。

本书手稿的提交根据合同 DE-AC04-94AL85000，授权于美国政府的一个订约机构。因此，美国政府对本书持有非独家、无版税的许可，可依据需要，再版或授权其他出版商出版。

目 录

第一部分

第 1 章　安全风险评估与管理流程

1.1　概述

自 2001 年“9 · 11”事件发生以来，因恐怖威胁的潜在性，即恐怖袭击的可能性、动机和能力都急剧地增大，使得安全风险管理人员更难做出决定。对于原本就财政紧张的政府和企业来说，新增安全功能的要求无疑是雪上加霜。一些公司不得不考虑他们是否能够在维持正常的商业运作的同时，还能够提供必需的安全，以充分保护建筑物等基础设施和员工的生命安全。安全风险管理者迫切需要一种机制帮助他们分析所搜集的信息，采取最合理的商业决策来防护设施不受潜在的恶意行为的破坏。

首先，管理者必须明确这些设施的基本任务：导致设施失效的突发安全事件有哪些，事件产生哪些相关后果，以及防止这类安全事故发生的防护目标和应承担的责任是什么。在确定这些任务是什么的同时，同样重要的还要识别需应对或防止什么，即弄清威胁（事件）谱，了解谁企图制造突发事件。威胁谱包括国际或国内的恐怖事件，政治或宗教的极端事件，犯罪行为，精神失常或内部人员的威胁等。其次，管理者必须完成系统效能分析或弱点分析，确定目前的设施安全系统应对威胁谱的能力。一旦安全系统的效能已知，管理者就可以评估安全风险，同时评定风险等级能否被接受。如果风险级别过高，那么管理者必须综合考虑，通过改进安全系统或者降低后果来减小风险以及对运行和成本的影响。平衡风险结果和降低风险的成本是一个挑战，但却至关重要（图 1.1）。

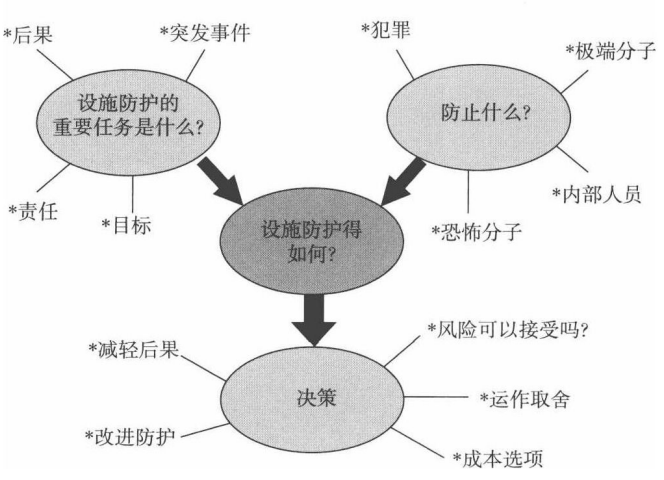

图 1.1　安全风险管理者决策

本章将简述一个有效的风险评估和管理流程，以帮助管理者确定企业或工业设施是否足够安全。后面每章将论述安全风险评估与管理流程的一个或多个步骤。这个流程已在各种应用中被采纳，包括国家重要基础设施的许多部件。

风险评估管理流程是20世纪90年代由桑迪亚国家实验室为美国联邦机构(IFIP)开发。IFIP是由一些关心安全问题的有关政府机构，应前总统比尔·克林顿（Bill Clinton）签署的第63号总统令，为处理安全防护问题以应对恐怖威胁而联合成立的。桑迪亚国家实验室经过30多年的实验和研究，将证明有效的具体防护措施和概念整合形成了一个评估基础设施和生命安全威胁风险的系统方法。这个流程最初用于防护美国大坝、高压电力传输系统以及其他重要的国家基础设施。该方法完整的流程经过测试，在“9·11”事件前一个月发表，自此已经在数百个政府和商业设施应对恐怖威胁中应用，用于评估相对安全风险级别、防护效果、设计安全性和减轻威胁后果等。

然而，安全风险很难量化。我们可以从使用传统的风险方程开始。传统上，安全风险是包含敌方袭击的可能性、敌对袭击成功的可能性和袭击造成的后果三个参数的函数。这里所描述的相对风险评估流程在属性上是定性的，允许决策者调整事件相对顺序，使之能做出风险管理决策。图1.2描述了评估安全风险所用到的三个参数。

由于风险评估过程所用的信息和评估结论包含公司的敏感信息，因此必须予以保护。信息防护程度和防护手段必须在分析开始之前就确定、计划并实施。安全风险方程中的三个参数所包含的信息如果泄漏，就可能给敌方提供重要的信息。

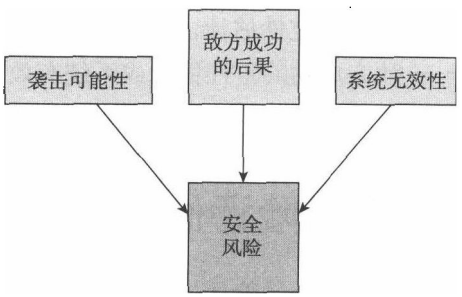

图 1.2　评估安全风险的参数

1.2　安全风险方程

安全风险由以下传统风险方程评估：

$$R=P_A\times(1-P_E)\times C$$

其中：

R= 与敌对袭击相关的风险；

P_A= 袭击可能性；

P_E= 安全系统有效抵抗袭击的概率；

$(1-P_E)$ = 系统无效性；

C= 袭击造成损失的后果。

因不能满足数学概率的基本假设，即变量既不独立也非随机，所以所有安全风险很难量化。猜测敌方袭击某个特定设施的可能性是相当困难的，因为从数学意义上来讲预测人类行为也不是随机事件，人类总是在不断地策划、实施、学习并改变其行为。因此，这种分析往往是针对安全应用评估的条件风险即假定初步事件发生（对于安全应用，这意味着敌方确实决定针对具体的设施进行袭击）。

上述假设是将风险评估集中于敌方成功的可能性和袭击造成的相关后果，但有时建筑物业主和经营者在风险评估中需要更具体的解答。他们可能有几座建筑物容易遭到威胁，且破坏所造成的经济损失很大，但是他们有可靠证据表明其中一栋建筑物会比其他的建筑物更容易受到袭击，尤其是在资金有限的情况下，必须优化安全开支。

现在已开发出多种风险评估和风险管理方法。虽然每种方法都有自己特定的名字、关注的重点和方法论，但所有的方法都试图回答下面的三个基本问题：

1. 我们的设施会发生什么糟糕的情况？

2. 这些糟糕的事情有多大可能性发生？

3. 这些糟糕的事情对我们设施的任务、住户、周边和更大的环境会造成怎样的影响？

本书将提供一个基于三个风险参数的量化估计的流程，来评估相对的安全风险。

- **袭击可能性** ——定性估计敌方袭击的可能性P_A。注意，在本书中，袭击的威胁潜在性、袭击可能性和P_A的意思是相同的。
- **敌方成功袭击的后果**——后果的定性估计，C。
- **系统无效性（$1-P_E$）**——敌方成功的定性估计或系统有效性（P_E）的补集。

1.3 安全风险评估与管理流程

这里我们用一个分析流程来进行安全风险评估。图 1.3 描述了流程的基本步骤。

为便于公司优化设施，此流程开始于一个可选的筛选分析，然后是主体设施的表征，包括突发事件和各自的关键资产的识别。接下来是定义敌对威胁以及使用威胁定义去估计袭击威胁的潜在性或对特定设施的敌对袭击可能性，从而估计后果的相对价值，最后给出相对风险。其中，一个可选的步骤是允许业主优化某一特定设施的资产，该方法同样也用来评估抵抗敌方袭击的安全系统效能。在风险值被认为高于预先确定的临界值（太高）的事件中，该方法强调识别和评价风险降低策略以降低风险的流程。

1.3.1 设施表征

安全系统分析的初始步骤是设施特征化。设施表征要求全面透彻地了解建筑物的功能

和运作情况，并考虑安全因素。安全因素应当描绘突发事件，最好是防护系统能够避免的具体事件。突发事件的扩展描述是对最有可能被敌方破坏或获得的公司关键资产的识别。有时此类资产较容易确定，而对于复杂的运作，则可能需要借助逻辑分析的方法来确保所有的关键资产都被识别并加以防护。

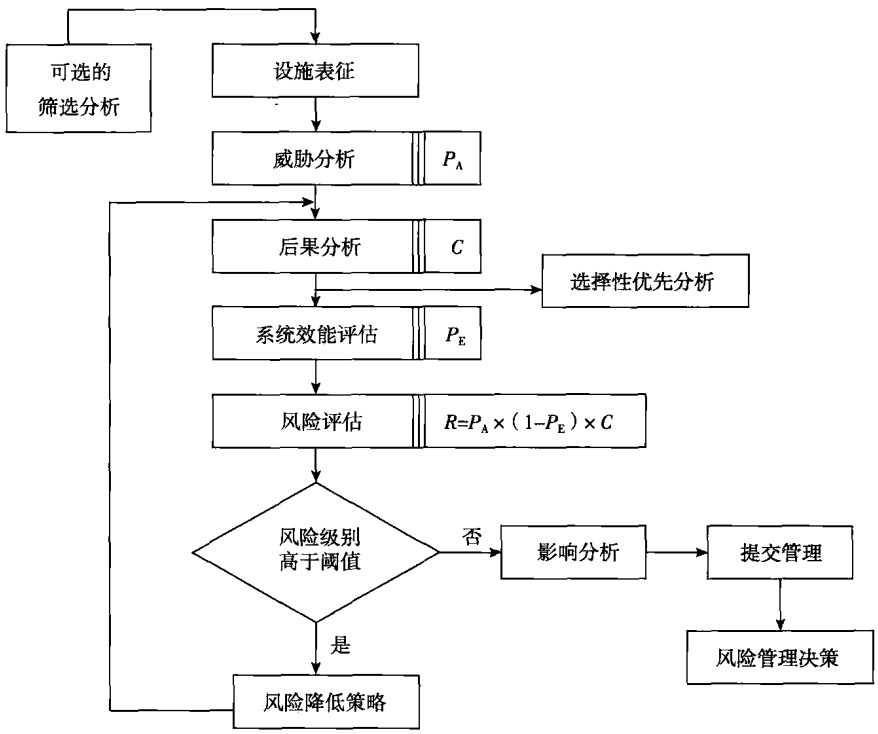

图 1.3　安全风险评估与管理流程

设施表征的完整实体描述不仅包括建筑物的实体布局，还包括建筑物细部、周边位置、建筑物的位置、平面图、接入点、政策和程序以及实体和网络防护功能及其位置，同时，必须注意防护系统已知的任何弱点。

设施表征可以概括为对设施防护目标的说明。通常，防护目标是突发事件的列表或一些突发事件的子集以及要防护的各个关键资产的列表。例如，一个建筑物的防护目标可能是确保住户的健康和安全或者防止个别关键资产被盗窃。

1.3.2　威胁分析

风险分析流程的第一个参数是威胁潜在性，尤其是敌方袭击的可能性。

威胁——在完成弱点分析和评估袭击的威胁潜在性或袭击可能性之前，要对威胁进行描述。描述内容包括可能敌方的类型、战术和能力（如在群体中的数量、武器、设备和运