中国人民公安大学外国警学译丛

ELSEVIER
爱思唯尔

Vulnerability Assessment of Physical Protection Systems

安全防范系统脆弱性评估

[美]玛丽·琳·加西亚（Mary Lynn Garcia） 著
赵兴涛 张翔 陈志华 金华 梁震 译

CPPSUP 中国人民公安大学出版社

中国人民公安大学外国警学译丛

安全防范系统脆弱性评估

Vulnerability Assessment of Physical Protection Systems

[美] 玛丽·琳·加西亚（Mary Lynn Garcia） 著
赵兴涛 张 翔 陈志华 金 华 梁 震 译

中国人民公安大学出版社
·北 京·

图书在版编目（CIP）数据

安全防范系统脆弱性评估/（美）加西亚著；赵兴涛等译. —北京：中国人民公安大学出版社，2015.10

（中国人民公安大学外国警学译丛）

书名原文：Vulnerability Assessment of Physical Protection Systems

ISBN 978-7-5653-2347-8

Ⅰ.①加… Ⅱ.①赵… Ⅲ.①安全系统—安全评价 Ⅳ.①X913

中国版本图书馆 CIP 数据核字（2015）第 214818 号

本书版权登记号：图字：01 - 2015 - 5029

安全防范系统脆弱性评估

［美］玛丽·琳·加西亚（Mary Lynn Garcia） 著
赵兴涛 张 翔 陈志华 金 华 梁 震 译

出版发行：中国人民公安大学出版社
地　　址：北京市西城区木樨地南里
邮政编码：100038
经　　销：新华书店
印　　刷：北京通天印刷有限责任公司

版　　次：2015 年 10 月第 1 版
印　　次：2015 年 10 月第 1 次
印　　张：26
开　　本：787 毫米×1092 毫米　1/16
字　　数：472 千字

书　　号：ISBN 978-7-5653-2347-8
定　　价：98.00 元

网　　址：www.cppsup.com.cn　www.porclub.com.cn
电子邮箱：zbs@cppsup.com　zbs@cppsu.edu.cn

营销中心电话：010-83903254
读者服务部电话（门市）：010-83903257
警官读者俱乐部电话（网购、邮购）：010-83903253
法律分社电话：010-83905745

致所有负责保护我们国家资产的人士

通过法律或其他途径求索一成不变的安全是一种误导。

事实是，只能通过永恒的变化来实现安全，使那些已经失去作用的陈旧理念适应当前的事实。

美国最高法院威廉·道格拉斯（William O. Douglas）

前 言

本书是2001年4月出版的《安全防范系统设计与评估》一书的延伸。《安全防范系统设计与评估》一书介绍了安全防范系统的构建过程和基本原则，而本书则阐述了该过程和原则在脆弱性评估中的应用。与前书相同，本书的一个基本前提是以安全防范系统的整体系统效能为目标，而非仅仅罗列设备、人员和规章制度。尽管现存许多探讨脆弱性评估的实践和书刊，但是仍然需要本书这样一本教材。上述实践和书刊中的多数都是基于合规为本的安全方法，甚至对关键资产也是如此。由于需要向高管阐明安全对于业务的合理性，从而限制了评估的目的性。安全防范系统的根本目标是保护资产。虽然大家都认为应该在安全防范上进行投资，但是也必须表明防范系统的效能达到了这一投资的期望。因为人员、规章制度或设备的简单存在不一定能提供防护。企业是可以做到在拥有有效安全的同时又能遵守规范和政策的。

脆弱性评估意味着识别安全防范系统的漏洞，怀有恶意的人为威胁可能会利用这些漏洞。采用检查表核实现有安全防范措施（以合规为本）的评估，与展现系统效能（以性能为本）的评估之间的区别非常显著。选择哪种方法取决于资产损失的后果。每个单位，无论规模大小，都会有关键资产。必须保护关键资产免遭侵害，并且必须采用以性能为基础的评估方法来确保有效的防护。低价值的资产不要求太多防护，以合规为本的方法在这些情况下更加合适。自“9·11”恐怖袭击事件后，我们在提高关键资产和其他重要资产的安全防范方面已取得了一些进步，但是还有很多工作要做。

一些读者可能会发现本书的某些部分，尤其是分析部分，例子中所使用的情节和假设过于简单。这一点是正确的，但是由于脆弱性评估是一个非常容易受到外界影响的过程，所以宁缺毋滥。我们的目标是全面而非过于详细的描述安全防范系统的一般脆弱性。如果有读者感到失望，我们将非常遗憾，因为，可公开使用的信息类型存在合理的限定（那些对安全防范系统负有责任和义务的管理者或许比其他读者更容易理解这一点）。

对第一本书不熟悉的读者会发现，在阅读本书之前回顾一下评估过程非常

有帮助。尽管有些读者可能仍不熟悉一些术语，但该书的第一章、第十四章和第十五章应该足以提供大部分的背景知识。本书的第一章概述了风险管理、脆弱性评估过程和系统工程在脆弱性评估中的应用。第二章阐述了安全防范系统的原理，重复了“设计”一书第五章的内容，并特别增加了脆弱性评估一节。第三章包括项目管理、团队组建和项目启动，用于帮助那些我们遇到过的很多人，他们需要这些安全防范项目方面的帮助，以及辅助制定脆弱性评估规划。对于不熟悉评估过程输入的人们，第四章回顾了防护目标，但是第一本书描述得更全面。第五章到第十章是脆弱性评估的核心内容，阐述了评估安全防范系统各组成部分（包括人员、规章制度和设备）的效能，以及采集各子系统的数据。第十一章对所有的数据进行分析，第十二章讨论了撰写评估报告的技术和脆弱性评估结果的使用。

与第一本书一样，有很多人对本书的问世做出了贡献。我衷心感谢桑迪亚国家实验室工作的麦克·本森（Mike Benson）、贝蒂·比林格（Betty Biringer）、吉姆·布兰肯希普（Jim Blankenship）、弗兰克·鲍彻（Frank Bouchier）、艾伦·坎普（Allen Camp）、李·康宁汉姆（Lee Cunningham）、伊万杰琳·德尔加多（Evangeline Delgado）、黛比·伊格林（Debi Eaglin）、罗恩·格莱泽（Ron Glaser）、史蒂夫·汉兰德（Steve Highland）、约翰·亨特（John Hunter）、利兹·贾拉米洛（Liz Jaramillo）、史蒂夫·乔丹（Steve Jordan）、弗恩·库恩斯（Vern Koonce）、丹·凯勒（Dan Keller）、卡罗尔·洛耶克（Carole Lojek）、丹尼斯·三吉（Dennis Miyoshi）、迈克·莫尔顿（Mike Moulton）、戴尔·默里（Dale Murray）、莎伦·奥康纳（Sharon O’Connor）、兰迪·彼得森（Randy Peterson）、查尔斯·林格勒（Charles Ringler）、戴安娜·罗斯（Diane Ross）、JR·拉塞尔（JR Russell）、乔·桑多瓦尔（Joe Sandoval）、史蒂夫·斯科特（Steve Scott）、鲍里斯·斯塔尔（Boris Starr）、巴兹尔·斯蒂尔（Basil Steele）、戴夫·斯沃兰（Dave Swahlan）、约翰·沃顿（John Wharton）、罗恩·威廉姆斯（Ron Williams）、约翰·沃斯宾斯基（John Wirsbinski）、汤米·伍德奥（Tommy Woodall）和格雷格·慧智（Greg Wyse）等同事。除桑迪亚之外，也得到了乔·卡隆（Joe Carlon）、丹尼斯·吉尔沃（Dennis Giever）、欧尼·昆（Ernie Kun）、布拉德·罗格斯（Brad Rogers）和乔·皮埃尔（Joe St Pierre）等人的大力协助。本书阐述的专业内容归功于他们，若有任何错误肯定是我的原因。我也非常感谢史密斯检测（Smiths Detection）公司的辛迪·斯切法诺（Cindy Schifano）和康泰科（Kontek）公司的唐·乌兹（Don Utz）允许我使用第七章和第九章中的图片。

感谢艾斯维尔公司的帕姆·切斯特（Pam Chester）、希瑟·法柔（Heather

Furrow）、马克·李斯特夫尼克（Mark Listevnik）、克瑞斯·诺林（Chris Nolin）和詹·苏西（Jenn Soucy）耐心和专业的指导，使得本书得以及时出版。最后，为了与“设计”一书的风格保持一致，特别感谢道格（Doug）先生、富齐（Fuzzy）先生和凯茜（Kasey）女士。

自“9·11”恐怖袭击事件之后，世界各方面都发生了巨大的变化。我希望本书能帮助学生理解脆弱性评估的基本原理，能帮助安全防范专业人士在有限的资源内实现更大的目标。

玛丽·琳·加西亚（Mary Lynn Garcia）
2005 年 5 月

译者序

随着经济的发展和安全需求的提升，各地投资建设了大量的安全防范系统。在系统的建设、应用、升级和监管中，安全防范风险和系统效能评估受到越来越广泛的关注。其中最重要的一环就是脆弱性评估，即通过识别资产防护中可能被预设威胁利用的薄弱环节，采用定量或定性的技术来预测安全防范系统组成部分的性能和整体系统的效能，并在此基础上确定安全防范系统的设计或完善需求。

为学习借鉴国外先进的安全防范系统理论和评估技术，推进国内安全防范系统建设，提升安全防范评估水平，译者精选了《安全防范系统脆弱性评估》一书以飨读者。原书作者加西亚女士是桑迪亚国家实验室的资深技术专家，从事安全防范行业的相关工作超过 30 年，在安全防范技术的科学研究、工程开发、行业应用、教学和项目管理等相关领域拥有丰富的经验，自 1997 年起，即获得美国注册安保专家（CPP）认证。

《安全防范系统脆弱性评估》一书完整地阐述了脆弱性评估的全部过程，包括评估规划、评估结果分析和评估报告出具。该书大量引用了该作者《安全防范系统设计与评估》一书中的原理，并引导读者运用这些原理，根据系统目标，并在现有预算和人力资源的条件下开展脆弱性评估。该书致力于解决脆弱性评估过程中的所有问题，包括与客户协商评估任务、项目管理和脆弱性评估规划、团队组建、执行脆弱性评估的详细步骤、数据采集和分析，以及如何利用脆弱性评估提出设计改进和多种备选设计方案。该书最后讨论了如何向高层管理人员扼要汇报评估结果，并展示安全投入获得的回报，以便为提升安全防范系统赢得管理层的支持。

该书的七个附录极具特色，巨细无遗地为读者提供了真实评估项目中采用的公式、图表、表格和检查表，便于读者更好地理解书中内容、开展实际评估工作。该书被许多专家看作安全防范评估人员的标准参考手册，甚至认为不参考该书就无法开展实地评估工作，该书也是学生深入理解脆弱性评估过程的极其重要的参考文献。

陈志华教授从诸多外版教材中选定翻译该书，并负责组织实施整体的翻译工作，最后还对全书进行了审校。赵兴涛、张翔、陈志华、金华和梁震负责具体的翻译（目录、前言、第5、6、7章由赵兴涛负责翻译，第1、2、3、4章、术语、附录由张翔负责翻译，第8、9章由金华负责翻译，第10、11、12章由梁震、陈志华负责翻译），何军政、姚刚洋、郭诚开等也参与了部分翻译和辅助工作，最后由赵兴涛对各部分进行统稿。另外，本书在编写过程中得到了中国人民公安大学出版社多位老师的大力支持和帮助，在此一并表示诚挚的谢意。

由于译者水平有限，书中难免存在一些缺点和纰漏，敬请读者和专家不吝赐教。

目 录

第 1 章 脆弱性评估绪论

这本书是之前出版的《安全防范系统设计与评估》（加西亚，2001 年）一书的续作。该书（下面简称为“设计”一书）概述了建设安全防范系统（PPS）时必须考虑的原则和概念；本书则阐述了如何运用这些原则和概念去识别一个已建成的安全防范系统的薄弱环节，并在必要时提出有效升级的建议。桑迪亚国家实验室在过去 30 年间为大量客户实施了脆弱性评估项目，这些客户包括美国能源部（DOE）、美国国防部（DoD）、北大西洋公约组织（NATO）、美国国务院（DOS）、联邦事务管理局（GSA）、堤坝和水利系统、监狱、学校、社区及化工企业，本书则以所有这些实践为基础。

脆弱性评估（VA）是一种系统性的评估，在评估过程中，通过识别资产防护中能被预设威胁利用的弱点，采用定量或定性的技术来预测安全防范系统组成部分的性能和整体系统的效能。在脆弱性评估识别出弱点之后，以此为基础确定安全防范系统升级设计的需求。另外，脆弱性评估也被用于辅助有关安全防范系统升级的管理决策。风险评估与脆弱性评估之间关系密切，许多安全专业人士互换使用这两个术语就可说明这一点。在实践中，这可能不会有特别大的问题，但它的确妨碍了安全服务提供商与客户之间及其内部的交流。

可将脆弱性评估过程划分为三个明确的阶段——评估规划、评估实施、评估报告撰写与采纳。脆弱性评估过程本身是更大规模风险评估过程的一部分。本书后续章节会详细阐述每一个阶段。本章节中讨论的要点包括：

- 风险管理与脆弱性评估。
- 风险评估与脆弱性评估流程。
- 脆弱性评估流程概述。
- 系统工程与脆弱性评估。

本书面向安全防范系统的脆弱性评估，但这些概念也适用于网络防护、人员防护以及某一场所或者单位的整体安全防护。为了简明起见，全书中的单位包括组织、企业、机构、政府，或者任何其他需要管理安全风险的实体。资产包括人员、财产、信息，或者单位认为有价值的任何其他所有物。

在讨论脆弱性评估时，区分“security”和“safety”非常重要。“safety”是指用来预防或探测危及人员、财产或单位的异常情况的措施（人员、规章制度或设备）。这些情况包括由于人为疏忽、不专心或缺乏培训造成的事故，以及其他非故意事件。“security”，从另一方面说，包括用来保护人员、财产或单位免受人为恶意威胁的措施。这些威胁包括民间骚乱、破坏、偷窃、窃取关键资产或信息、工作场所暴力行为、敲诈勒索或其他对资产的人为蓄意攻击。优秀的安全（security）脆弱性评估应该考虑安全（safety）方面的控制措施，因为一些安全（safety）措施将有助于对安全（security）事件进行探测和反应（喷水器能灭火而不考虑起因）；然而一些攻击行为却需要更多的探测和反应能力。例如，一名心怀不满的员工会破坏关键的制造设备并造成大规模减产。若没有安全（security）控制措施，很难迅速确定这是不是蓄意破坏行为并避免收益上的巨大损失。

1　风险管理与脆弱性评估

风险管理是单位采取的处置已识别风险的一系列行动，包括规避、降低、分散、转移、消除和接受等各种选项（Grose，1987）。高水准的风险管理项目可能会组合使用上述选项。风险规避可通过消除风险源来实现。例如，某公司可能会从其他公司采购关键部件，而非自己生产。这就消除了生产线作为破坏目标的风险。风险降低是通过采取一些行动以减少损失的严重程度来降低单位的风险。这是许多安全防范项目的目标，即通过实施至少几项安全措施来降低风险。风险也可被分散在多个场所，也许可以在单位的多处设施实现相似的生产能力。这样，在一个场所损失的生产能力可能通过提高其他场所的生产量来得到弥补。另一个关于风险分散的例子是将资产分布在大型工业生产设施的各处。通过分散资产，任意一次入侵攻击中将有较少的资产处于风险之中。风险转移是利用保险来弥补因损失而导致的设备更换或其他费用。这是许多安全防范系统采用的一种重要工具。风险接受是认识到总会有一些剩余风险存在。关键是主动确定可接受的风险水平而不是被动承担。在安全风险管理中，这些决定取决于资产损失的后果、已知威胁及单位对风险的承受能力。应当进行权衡分析，以确保在安全防范上的投资能提供一个高性价比的安全解决方案。如果其他风险管理选项能以更低的成本提供相同或更好的效果，采用安全防范系统可能就不太合理。

安全只是风险的一个方面，因此，安全风险必须在覆盖单位整体风险管理的背景下，与诸如市场、信用、运营、战略、流动性以及灾害等其他类别风险一并考虑。风险管理、风险评估及脆弱性评估的关系如图 1-1 所示。

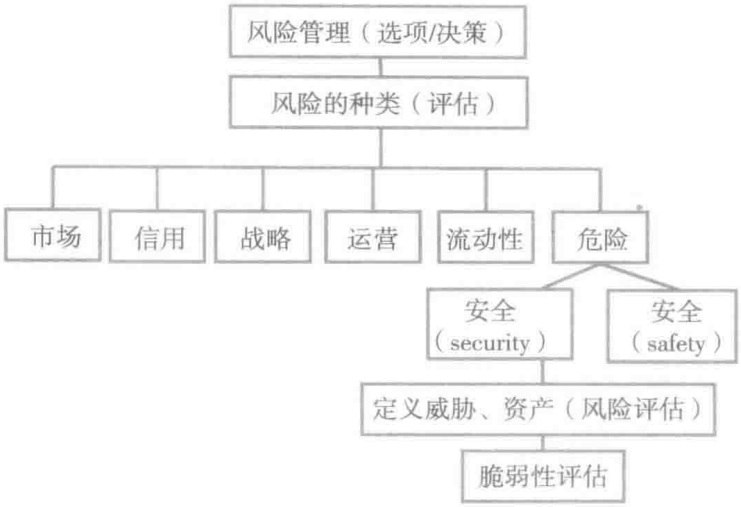

图 1-1 风险管理与脆弱性评估的关系

贯穿整个单位的风险应得到全面管理，且必须解决那些被确定为超出可承受水平之上的风险。脆弱性评估是安全风险评估的一部分，用于辅助风险管理决策。

为了构建风险评估与风险管理的关系，可以参考由卡普兰（Kaplan）和盖瑞克（Garrick，1981）提出的一些定义，他们认为在风险评估中，分析者试图回答三个问题：什么会出错？出错的可能性有多大？后果是什么？对这些问题的回答有助于鉴别、衡量、量化和评估风险。然后，通过回答第二组问题来将风险管理建立在风险评估的基础之上：能做到什么？存在哪些选项？从损失、收益和风险的角度，选项之间如何权衡？当前的管理决策对未来选择有哪些影响？最后一个问题的答案提供了最优解决方案。全面风险管理源自该过程，通过回答两组问题并定位系统失效的来源，将全面风险管理定义为一个建立在正规风险评估和管理基础之上的系统性的、基于统计的、整体性的过程。

安全风险评估是回答前三个问题的过程，采用威胁、攻击的可能性和损失的后果作为前三个问题的基准。

一个周密的安全风险评估应该考虑安全系统（计算机、行政、运输保护等）组成部分的风险，以利于做出整个单位的知情风险决策。正如用于安全防范系统中的脆弱性评估一样，风险评估是用一系列的分析方法评估安全防范系统，包括：

* 威胁分析。

* 后果分析。

＊事件和故障树分析。

＊脆弱性分析。

第四章回顾了前三种技术；脆弱性分析是本书第十一章的内容。

1.1 风险评估和脆弱性评估过程

大多数设施或单位会常规性地对其安全防范系统进行风险评估，以表明它们在持续保护单位资产，与此同时，识别出那些可能需要关注的额外区域。不同的单位对评估的定义不同，但通常而言，都会考虑一次负面事件的可能性，这里是指一次安全事件及其后果。“设计”一书的最后部分阐述了风险评估，并提出了一个风险计算公式，可使用定性或定量指标。这里会再次讨论该公式，并增加新的内容。

通过使用下述方程可以定性或定量地衡量安全风险：

$$R=P_A * (1-P_E) * C$$

式中，R 表示攻击者接近或窃取设施（或利益相关者）关键资产的风险。范围是 0 至 1.0，0 即无风险，1.0 为最大风险。风险按一个时间段进行计算，比如 1 年或 5 年。P_A表示一段时间内入侵攻击的可能性。这可能很难确定，但通常可以用历史数据来协助确定。可能性范围是 0（一次攻击的可能性也没有）至 1.0（肯定会有攻击）。有时在计算风险时，假设肯定会有攻击，并从数学上将 P_A设置为 1.0，这称为条件风险，该条件是对手发起攻击。这并不意味着绝对会有一次攻击，而是攻击的可能性未知，或者资产非常有价值一定要得到保护。这一方法可用于任意资产，但通常更适用于设施最核心的资产，在这里，即使 P_A值很低，但损失程度也会高到难以承受。对这些资产来说，安全防范系统通常是必需的。

$P_E=P_I * P_N$，P_I是被响应者拦截的可能性，P_N是在拦截的情况下，制止对手的可能性。制止行动包括从口头命令上升到致命武力等一系列的策略。恰当的响应取决于预设威胁和资产损失的后果。P_E代表安全防范系统防范预设威胁的效果。

C 是后果值。C 与所发生事件的严重程度有关，取值范围从 0 到 1，是一个归一化因子。可将条件风险值与所在设施的其他风险进行比较，制作一张全部事件的后果表，涵盖从最大到最小的损失范围。利用这张表，对所有可能事件的风险均进行归一化处理。这样，可以合理地分配有限的安全防范系统资源，确保后果最严重的资产得到保护，并达到可承受风险。

注意上述方程首次采用了一个新术语，即制止概率（P_N）。“设计”一书仅仅扼要讨论了这一术语，因为很多设施缺乏对安全事件的快速响应。由于响