电磁脉冲袭击对国家重要基础设施的影响

——电磁脉冲袭击对美威胁评估委员会报告

美国电磁脉冲袭击对美威胁评估委员会/编
郑 毅　梁 睿　曹保锋/译

Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack

Critical National Infrastructures

科学出版社

电磁脉冲袭击对国家重要基础设施的影响

——电磁脉冲袭击对美威胁评估委员会报告

Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack

Critical National Infrastructures

美国电磁脉冲袭击对美威胁评估委员会 编

郑 毅 梁 睿 曹保锋 译

科学出版社

北京

内 容 简 介

本报告是电磁脉冲袭击对美威胁评估委员会出版的报告之一，介绍了委员会所做的关于高空电磁脉冲（EMP）对美国关键基础设施的袭击效果评估的结果，并提出了如何减少危害的建议。本报告对高空核爆炸电磁脉冲对于电力、通信、金融、能源、交通、食品、水利、应急服务、空间系统、政府部门等国家基础设施产生的影响以及应对措施给出了较为详细的介绍。报告的结论基于理论分析和实验研究得出，得到了美国国家核安全委员会实验室（劳伦斯利弗莫尔国家实验室、洛斯阿拉莫斯国家实验室、桑迪亚国家实验室）的支持。

本报告的读者不仅包括各高校电机系、电子系的学生、教师、科研工作者，还包括国家重要基础设施的设计者、建造者、维护者，电磁兼容领域的科技人员，以及对核武器效应防护感兴趣的社会各界人士。

图书在版编目(CIP)数据

电磁脉冲袭击对国家重要基础设施的影响：电磁脉冲袭击对美威胁评估委员会报告/美国电磁脉冲袭击对美威胁评估委员会编；郑毅，梁睿，曹保锋译. —北京：科学出版社，2019.2

书名原文：Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack: Critical National Infrastructures

ISBN 978-7-03-059930-8

Ⅰ.①电… Ⅱ.①美… ②郑… ③梁… ④曹… Ⅲ.①电磁脉冲-影响-基础设施-研究 Ⅳ.①TL91 ②F294.9

中国版本图书馆 CIP 数据核字（2018）第 274427 号

责任编辑：周 涵 田轶静/责任校对：邹慧卿

责任印制：吴兆东/封面设计：无极书装

科学出版社 出版

北京东黄城根北街 16 号

邮政编码：100717

http://www.sciencep.com

北京中石油彩色印刷有限责任公司印刷

科学出版社发行 各地新华书店经销

*

2019 年 2 月第 一 版 开本：720×1000 B5

2019 年 2 月第一次印刷 印张：13 3/4 插页：2

字数：275 000

定价：98.00 元

（如有印装质量问题，我社负责调换）

电磁脉冲袭击对美威胁评估委员会成员

John S. Foster，Jr. 博士
Earl Gjelde 先生
William R. Graham 博士（主席）
Robert J. Hermann 博士
Henry（Hank）M. Kluepfel 先生
Richard L. Lawson 美国空军将军（退役）
Gordon K. Soper 博士
Lowell L. Wood，Jr. 博士
Joan B. Woodard 博士

前　言

美国的社会架构和实体结构由一个个小系统组成的一个大系统支撑着。这是一个环环相扣、相互依存的复杂的动态基础设施（国家重要基础设施）网络，其和谐运转保证了各种活动、事务和信息流的正常运行，从底层支撑了这个社会的有序运转。“9·11”事件和最近的卡特里娜飓风、丽塔飓风事件，使得这些基础设施在各种威胁（故意的、偶然的、自然的）面前的脆弱性越来越成为当今社会高度关注的焦点。

本报告介绍了电磁脉冲袭击对美威胁评估委员会（以下简称委员会）关于高空电磁脉冲对国家重要基础设施袭击效果的评估结果，并提出了减轻危害的建议。评估报告中的结论基于理论分析和实验研究得出，具体内容将在后面章节详细讨论。在较早的一份执行报告《电磁脉冲（EMP）对美国威胁评估委员会报告》第1卷：执行报告（2004年）中，对这个主题进行了概述。

高空核爆炸产生的电磁脉冲是给我们社会带来灾难性后果的为数不多的威胁之一。日益增多的各种形式的电子设备是最易受到电磁脉冲袭击的对象。电子器件几乎用于美国民用系统的各个方面，如控制、通信、计算、存储、管理和执行等。当发生高空核爆炸时，它产生的电磁脉冲信号将在可视范围内覆盖广阔的地域。[①] 当这种宽频带、高强度的电磁脉冲耦合到敏感电子设备时，极有可能对维持美国社会运转的关键基础设施带来大范围持久的干扰和破坏。

美国社会对电力系统的依赖程度非常高，而电力系统对电磁脉冲袭击非常敏感，对电磁脉冲有特殊的耦合损伤机制，因此电力系统受到电磁脉冲袭击造成的灾难性后果可能是长期的。考虑到核武器及其运载工具扩散程度逐年增加，若有人利用电力系统的这一敏感性进行电磁脉冲袭击，那将是一个严重的威胁。单个电磁脉冲袭击将会瞬间使暴露在电磁脉冲辐射区域内的大部分电网严重破坏或断电。当电力影响从一个区域传到另一个区域时，即使电磁脉冲辐射不到的区域，其电网也有崩溃的可能。

服务完全恢复所需的时间取决于电力设施和其他国家基础设施被干扰和破坏的程度。受灾地区越大，电磁脉冲场强越强，恢复时间越长。一些关键的电

① 例如，高度100千米的核爆炸，将在爆点下方地球表面400万平方千米（约150万平方英里）的地域上产生不同强度的电磁脉冲。

力基础设施组件已不在美国制造，通常情况下，它们的采购周期最长会有一年的时间。损坏或缺少这些组件有可能使电力基础设施的关键部分在几个月到一年甚至更长的时间内无法工作。当可供调动、协调、分配的备用工作系统（包括应急电源、电池、燃料供应、通信以及人力资源等）出现短缺或耗竭时，关键基础设施故障时间将持续更久。

电力是其他关键基础设施运行的基础，包括水、食品、燃料的供应分配、通信、交通、金融交易、紧急服务、政府服务以及其他保障国民经济和福利的基础设施等。委员会认为，假如电力基础设施的关键部分长时间失效，其后果很可能是灾难性的，在人口密集的城区和郊外社区，可能有很多人最终会因缺乏基本的生存要素而死亡。事实上，委员会担忧的是，如果不采取实际行动为电力系统的关键部分（尤其是必不可少的服务设施）提供防护，快速恢复供电电力，这种灾难性的后果很有可能在电磁脉冲袭击的情况下发生。目前，单个基础设施的恢复计划都基于这样的假设，对该基础设施恢复至关重要的其他基础设施受到的损坏是有限的。在从电磁脉冲袭击中恢复时，这些计划几乎没有价值，因为电磁脉冲袭击对所有依赖电力电子的设施都有长时间的影响。

从袭击中恢复的能力是备受关注的研究领域。很多公司和机构使用自动化控制系统，可以利用少量人力高效运行。因此，虽然手动控制某些系统是可能的，但是懂得手动操作的技术人员数量有限，能够修复物理损伤的人手也不足。大部分维修人员只负责对高可靠性的设备进行日常维护。当维护超过常规水平时，通常从受影响区域以外抽调人员。然而，由于电磁脉冲同时作用的范围很大，预期的增援可能正忙于自己区域的问题。因此，通常情况下只需几周的维修时间，在遭受电磁脉冲袭击时维修周期会大大延长。

我们应该在能力范围内尽量采取措施预防电磁脉冲袭击带来的影响。对衰落国家或跨国集团这样的潜在对手，确保互相毁灭的冷战式的威慑并不是有效的威胁。做好应对电磁脉冲袭击的准备，包括对发生事件的了解、保持对态势的感知、有适当的恢复计划、演练并改进这些计划，以及降低易损性等，对于减轻袭击可能造成的危害才是最关键的。国家层面的应对方法应该兼顾预防、保护和恢复几个方面。

委员会已从美国多家联邦机构和国家实验室获取了大量信息，包括北美电力可靠性公司（NERC）、总统国家安全电信咨询委员会、美国国家通信系统（后来被美国国土安全部合并）、美联储和美国国土安全部等。在本次评估之前，很明显只有少数现代电子系统和部件完成了电磁脉冲敏感性测试。为了弥补这个不足，委员会资助了对目前系统和基础设施组件的说明性测试。委员会的观点是，目前联邦政府没有足够的能力开展可靠的电磁脉冲后果评估与管理。

美国长期面临这样的挑战，即保持在了解和控制核武器效应（包括电磁脉冲效应）领域的技术竞争力。美国能源部和国家核安全局在过去十年间制订并实施了大规模的核武库管理计划。然而，核武器效应对现代系统的影响研究并未跟上。委员会对目前美国在电磁脉冲效应方面的理解和应对能力得出的结论是，在政府、国家实验室和工业部门需要进行电磁脉冲防护的领域，美国正在迅速失去相关的技术优势。

电磁脉冲对国家民用基础设施的袭击是一个严重的问题，但也是一个可以通过政府与企业合作、集中努力能够应对的问题。委员会认为，利用现有的时间和资源，处理电磁脉冲造成的不利影响是可行的。在国家层面郑重提出电磁脉冲袭击威胁，展现了一种国家姿态，这将有利于显著降低电磁脉冲袭击带来的影响，并让美国一旦面临电磁脉冲袭击便能够及时恢复正常。

致　　谢

委员会对在专业和技术方面为本报告做出贡献的以下工作人员表示感谢：

George Baker 博士

Yvonne Bartoli 博士

Fred Celec 先生

Edward Conrad 博士

Michael Frankel 博士

Ira Kohlberg 博士

Rob Mahoney 博士

Mitch Nikolich 博士

Peter Vincent Pry 博士

James Scouras 博士

James Silk 博士

Shelley Smith 女士

Edward Toton 博士

委员会对在科学和技术方面做出贡献的以下人员表示感谢：William Radasky 博士、Jerry Lubell 博士、Walter Scott 先生、Paul F. Spraggs 先生、Al Costantine 博士、Gerry Gurtman 博士、Vic Van Lint 博士、John Kappenman 博士、Phil Morrison 博士、John Bombardt 先生、Bron Cikotas 先生、David Ambrose 先生、Bill White 博士、Yacov Haimes 博士、Rebecca Edinger 博士、Rachel Balsam 女士和 Chris Baker 先生。委员会还对以下机构和人员的协助表示感谢：Linda Berg 女士、负责核化生事务的前国防部长助理 Dale Klein 博士、国防威胁降低局及其联络员 Joan Pierre 女士、国防威胁降低局高级科学家 Don Linger 博士、达尔格伦海军水面作战中心的 David Stoudt 博士、洛斯阿拉莫斯国家实验室的 Michael Bernardin 博士、劳伦斯利弗莫尔国家实验室的 Tom Thompson 和 Todd Hoover 博士。

感谢情报界（IC）的协助。

委员会还得到了以下合作机构的大力支持：美国国家核安全管理局下属实验室（劳伦斯利弗莫尔国家实验室、洛斯阿拉莫斯国家实验室、桑迪亚国家实

验室），阿贡国家实验室，爱达荷国家实验室，达尔格伦海军水面作战中心，美国国防分析研究所，Jaycor/Titan，Metatech 公司，美国科学应用国际公司，Telcordia 科技，Mission Research Corporation 和弗吉尼亚大学系统风险管理中心。

目　录

第 1 章　基础设施的共同点

美国的社会架构和实体结构由一个个小系统组成的一个大系统支撑着。这是一个环环相扣、相互依存的复杂的动态基础设施（国家重要基础设施）网络，其和谐运转保证了各种活动、事务和信息流的正常运行，从底层支撑了这个社会的有序运转。“9·11”事件和最近的卡特里娜飓风、丽塔飓风事件，使得这些基础设施在各种威胁（故意的、偶然的、自然的）面前的脆弱性越来越成为当今社会高度关注的焦点。

本报告的重点是阐述美国关键国家基础设施面临电磁脉冲（EMP）袭击时存在的漏洞，为此，本报告用单独的章节描述了电磁脉冲对各种关键基础设施的威胁。然而，想要洞察电磁脉冲效应同一时间对全部基础设施的影响，重要的一点是，必须认识到所有高度联动的关键基础设施这样一个整体的脆弱性，要大于其组成部分的脆弱性的简单相加。整体是一个十分复杂的系统集成，技术发展使得整体处于动态的高度协调状态，当有一个基础设施发生故障时，故障可能不是孤立的，而是会引起其他基础设施连锁故障。

同样重要的是，要明白技术进步不仅使基础设施之间产生了相互依存性和新的敏感性，同时也在不断使这种相互依存性增加。特别是，电磁脉冲袭击对美威胁评估委员会（以下简称委员会）认为有必要单独讨论一种目前在基础设施中常用的技术——现代社会中无所不在的，被称为数据采集与监控系统（SCADA）。

因此，开篇的重点是详细地论述现代基础设施与控制系统及其相互作用这两个方面，这些内容适用于所有基础设施，委员会同时认为这为洞察所有国家基础设施电磁脉冲袭击敏感性来源提供了脉络。

SCADA

引言

悄然进行的工业革命在计算机时代加速发展，SCADA 成为其中越来越关键的因素。广泛使用的 SCADA 及其相关电子产品、数字控制系统（DCS）和可编程逻辑控制器（PLC）也注定成为国家关键基础设施各个方面的关键要素。在 21 世纪这个不断发展的数字时代，我们的基础设施对这些无所不在的控制系统

的日益依赖，带来了经济效益和极大的操作灵活性，也带来了新的脆弱性，如网络安全问题。这些问题在今天仍是受到高度关注和重视的。高空电磁脉冲将我们的注意力转向这些系统的另一个潜在的脆弱性，这个脆弱性问题可能会产生更加广泛的影响。

什么是 SCADA?

SCADA 是在较大地理区域范围内对基础设施系统进行数据采集和控制的电子控制系统。它们广泛应用于电力传输和分配、水资源管理、石油和天然气管道等关键基础设施。SCADA 技术已经发展了几十年，它起源于铁路和航空工业的遥测系统。

> 1999 年 11 月，圣地亚哥水务局和圣地亚哥天然气及电力公司的 SCADA 无线网络遭受了严重的电磁干扰。这两家公司发现自己无法通过 SCADA 电子系统的远程控制驱动关键阀门的开关。远程操作失效使得他们必须派遣技术员到现场，手动操作水阀和气阀，才得以避免一场水道系统的“灾难性故障”，这是事后圣地亚哥水务局给联邦通信委员会投诉信里所说的。这次水流量为 8.25 亿加仑[①]/天的故障，造成的后果是“水管破裂产生的每分钟数千加仑的泄漏，可能造成服务中断、大洪水以及个人和公共财产的相关损失”。事后确定引起 SCADA 故障的原因是圣地亚哥海岸 25 英里（1 英里＝1.609 千米）以外的船上雷达的操作。

SCADA 的物理形式在各行各业可能会有不同的应用形式，但它们通常都具有某些通用的性质。SCADA 物理结构与个人计算机的内部结构很相似。通常情况下，它可能包含常见的电路板、不同种类的芯片，以及连接外部设备的电缆连接器。连接到相应电缆连接器上的各种传感器系统可作为 SCADA 的眼睛和耳朵，连接的电子控制装置可用于发出系统性能调整的命令，这些设备或许会距离很远。图 1-1 是一个典型的 SCADA 控制器。

SCADA 的主要功能之一是对物理系统的运行状态进行远程监控。通过系统提供的在线监测参数进行监控，这些参数表征了系统的工作状态，如发电厂内的电压或电流、天然气管道中的流量、区域电气系统产出或消耗的电网净功率，或者监测环境参数，如监测核电站内的温度，当这些参数超出预设的状态时发出警报。

SCADA 的监控功能反映了通过调节设备输出主动控制系统运行的能力。例

① 1 加仑＝3.785 升。

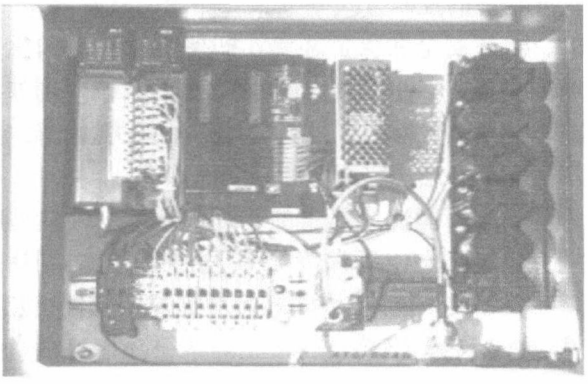

图 1-1　典型的 SCADA 架构（后附彩图）

如，当发电厂由于关键硬件组件失效而发生故障或发生其他工业事故时，实时监测的 SCADA 将检测到故障向有关当局发出警报，并向其控制下的其他发电厂发出增加功率输出的命令以匹配负载。所有的这些操作都在数秒时间内自动完成，没有任何人为操作参与到这个快速的控制回路中。

电力行业典型的 SCADA 架构包括一台中央计算机——主控终端（MTU），通过许多远程终端设备（RTU）子系统进行通信，如图 1-2 所示。RTU 用于执行远距离无人看管位置的数据采集和控制任务。典型的 RTU 数据采集包括获取热电偶传感器、电压传感器、功率计等传感器的信号，以及开关和断路器等设备的工作状态等。典型的控制操作包括开关电机、控制阀门和断路器等。

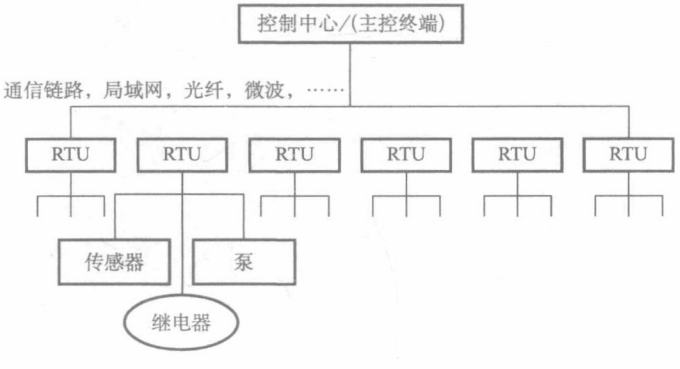

图 1-2　常见的 SCADA 架构

DCS 与 SCADA 由许多相似的功能和硬件组成。DCS 通常被用于单个场所的自动化控制过程，如炼油厂或化工厂。相比之下，SCADA 通常用于设施分散布置的环境下，在这种条件下，从远程实时感知事态是集中控制的关键。大多数 DCS 装置用于控制复杂的动态系统，这些系统如果仅采用手动控制的方式，

几乎难以找到安全或经济的控制方式。

为了提高效率、保证安全和保护环境，即使相对简单的生产过程，如使用传统蒸汽循环发电的发电厂，也要拥有非常复杂的系统。例如，蒸汽发生装置的控制系统参数就包括发电机转速、发电机润滑油压力、励磁电流及电压输出、给水压力及锅炉汽包水位、燃烧室压力和燃烧速率等。

这些控制点的混乱有可能造成严重的物理损害。一个典型的例子是锅炉的燃烧端点和循环端点控制问题。通常情况下，控制系统先到达燃烧端点（提供锅炉空气进入和燃油添加的限值），可以避免对锅炉产生任何热损伤。如果控制系统被打乱，它就会在到达燃烧端点前，先到达循环端点（产生蒸汽的最大速率）或结余端点（水不被排出锅炉时的最大速率）。这种情况将会导致锅炉管道的热损伤，或造成汽轮机叶片的物理损伤。

另一种与 SCADA 在物理结构上相似的硬件是 PLC，主要用于控制执行器或传感器，在大型的 SCADA 或 DCS 中非常常见。SCADA、DCS、PLC 在电子特性方面是相同的，因此其固有的电子敏感性也一样。由于 SCADA 倾向于大面积的布设并直接暴露，所以我们随后重点讨论 SCADA。若 PLC 和 DCS 存在裸露或未受保护的电缆连接问题，后面的讨论也同样适用于它们。典型的 PLC 结构见图 1-3。

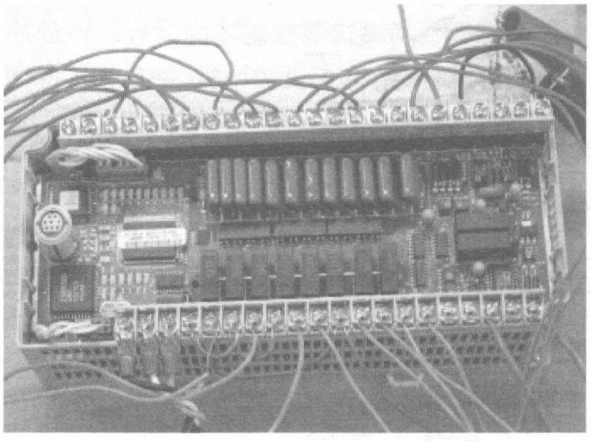

图 1-3　PLC 开关执行器（后附彩图）

电磁脉冲与 SCADA 相互作用

SCADA 部件通常安装在远距离没有人为干预的位置。虽然它们的关键电子元件通常放置于某些金属盒内，但是其外壳作为保护性法拉第笼的作用是微弱的。这些金属容器主要是为设备提供物理防护和避免化学腐蚀，它们在设计时

通常没有考虑高能电磁脉冲的影响，电磁脉冲可能通过空间或天线（电缆连接）耦合，进入电子设备，破坏电子设备的电磁完整性。SCADA 对电磁脉冲的敏感性问题主要集中于电磁脉冲信号的早期部分 E1。这是因为，电磁脉冲后期信号 E3 一般不会与 SCADA 中的长电缆直接耦合，即使是电力行业中的长电缆也不会。

无处不在的 SCADA 控制系统若受到威胁，则可能成为国家关键基础设施的敏感源，为了理解这一点，我们必须首先了解底层硬件组件本身的敏感性。为此，委员会利用国有的电磁脉冲模拟器，资助了一系列 SCADA 常用组件的电磁脉冲敏感性试验（图 1-4）。模拟试验提供了观察设备在工作状态下与电磁能量相互作用的环境。模拟器没有复制威胁级电磁脉冲环境的所有特征，通过模拟试验和真实案例之间的对比分析，可以对真实场景中系统响应进行分析评估。

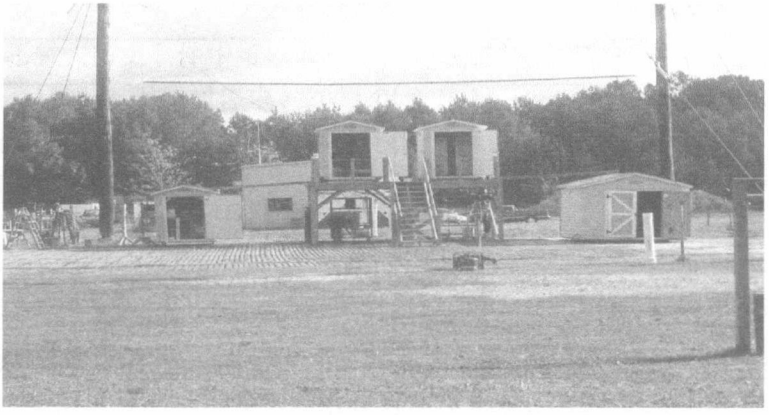

图 1-4　电磁脉冲模拟器结构和内部电器

委员会通过征求北美电力可靠性协会等相关工业部门专家的意见，以及现场和市场调查，确定了进行测试的典型控制系统，提出的测试矩阵代表了应用于发电、配送电、管网分布、制造工厂的电子控制技术。试验所用的部分被测件如图 1-5 所示。

电磁脉冲模拟测试

本节给出一个照明电子控制系统测试结果的简要总结。详细的模拟测试结果记录在委员会的分报告中。在第 2 章我们将描述完整的试验方法，并讨论如何开展评估电网电磁脉冲敏感性试验。

很多控制系统都是通过以太网电缆连接的。当威胁来临时，瞬变电场与电缆的电磁脉冲耦合将是重要的敏感源。因为系统需要人工修复，所以系统的完