国家电网公司
STATE GRID
CORPORATION OF CHINA

信息系统安全开发手册

国家电网公司 编

中国电力出版社
CHINA ELECTRIC POWER PRESS

国家电网公司
STATE GRID
CORPORATION OF CHINA

信息系统安全开发手册

国家电网公司　编

中国电力出版社
CHINA ELECTRIC POWER PRESS

内容提要

本书针对信息系统安全开发过程中可能遇到的问题，结合具体实例，从隐患、风险、措施三个层次对身份认证、权限管理、数据安全、资源控制四大类安全功能设计，以及15种典型安全漏洞进行了详细描述。

本书可供国家电网公司信息系统开发人员及相关工作人员参考使用。

图书在版编目（CIP）数据

信息系统安全开发手册／国家电网公司编. —北京：中国电力出版社，2013.6

ISBN 978-7-5123-4494-5

Ⅰ.①信… Ⅱ.①国… Ⅲ.①信息系统－安全技术－技术手册 Ⅳ.①TP309-62

中国版本图书馆CIP数据核字（2013）第110092号

中国电力出版社出版、发行

（北京市东城区北京站西街19号 100005 http://www.cepp.sgcc.com.cn）

北京九天众诚印刷有限公司印刷

*

2013年6月第一版 2013年6月北京第一次印刷

889毫米×1194毫米 32开本 2.125印张 55千字

定价 10.00 元

前 言
PREFACE

随着坚强智能电网和“三集五大”建设的不断推进，信息系统业务集成度更高，数据交互性更强，国家电网公司业务高度依赖信息系统，信息安全对于公司生产经营的保障作用愈加明显，基础性、全员性、全局性作用更加增强。当前，任何单个系统都可能成为公司信息安全防护体系的“短板”，任何一个系统安全漏洞都可能带来严重后果，信息系统研发安全水平直接关系到公司信息化建设的整体质量。

为了提高公司信息系统研发人员的安全开发意识，提升全员安全开发专业技能水平，公司组织编写了《信息系统安全开发手册》，旨在为信息系统研发人员提供一个全面的安全开发参考范例。

本书结合具体实例，从隐患、风险、措施三个层次，对身份认证、权限管理、数据安全、资源控制四大类安全功能设计，以及15种典型安全漏洞，进行了详细描述。通过对本书的学习和应用，有助于公司信息系统研发人员加强对公司信息安全基本规范及要求的理解，提高安全编程能力，综合提升公司软件开发质量。

本书在编写过程中得到了系统内外多位专家、领导，以及信息安全管理和技术人员的大力支持，吸取了他们提出的大量宝贵意见和建议。公司信息安全实验室承担了本书大量的编写工作，在此一并表示衷心感谢！

国家电网公司信息通信部

二〇一三年四月

目 录
CONTENTS

E 安全漏洞

A

身份认证类

A

身份认证类

A-1 未提供专用的登录控制模块

! 隐患

未提供专用的登录控制模块对登录用户进行身份标识和鉴别。

⊗ 风险

系统未对用户提供健全的身份确认机制，无法验证登录用户身份的合法性，易造成系统被恶意用户入侵破坏。

登录模块

措施

提供专用的登录控制模块，实现对登录用户进行身份标识和鉴别。

A-2 未强制要求口令强度

隐患

未强制要求口令复杂度和口令定期更换，口令明文存储。

风险

口令抗暴力破解能力差，易被恶意用户冒用、盗用，导致信息泄露或违规操作。

措施

系统可检测初始口令或口令强度，要求口令必须具有一定的强度、长度和复杂度。提供定期更改口令机制和弱口令强制更改机制。

A-3 未对同一用户采用组合鉴别技术

隐患

未对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别。

风险

无法有效避免恶意用户针对系统账户进行身份冒用、盗用等操作，且无法有效控制系统关键账户共用。

措施

采用动态密码、数字证书等方式，结合“用户名+密码”的身份鉴别形式。

A-4 未提供登录失败处理机制

! 隐患

未提供登录失败锁定或退出等安全功能。

⊗ 风险

无法避免攻击者针对口令进行暴力破解，导致系统账户被猜解进而信息被窃取或系统被恶意操作。

措施

通过采取结束会话、限制非法登录次数和自动退出等登录失败处理措施，避免用户反复尝试口令。

B

权限管理类

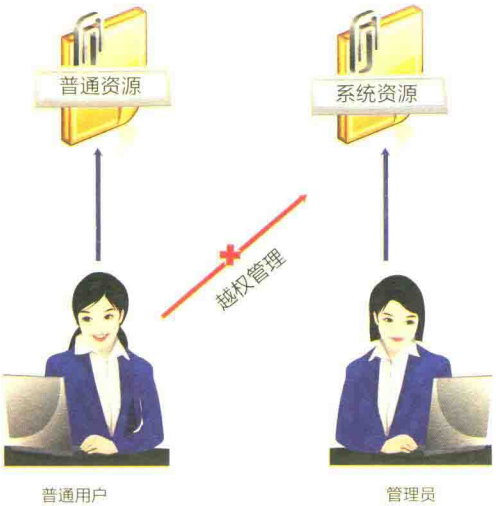
B-1 未严格限制账户权限

隐患

未严格限制账户的访问权限。

风险

存在越权操作的风险，即无访问权限的用户获得高级操作权限后对系统进行风险操作。



措施

为用户配置访问控制策略，严格限制账户的访问权限。

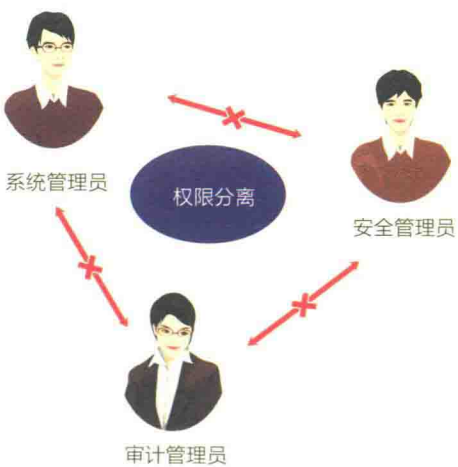
B-2 未进行特权账户权限分离

隐患

未对特权账户（如系统管理员账户、安全审计员账户、安全管理员账户等）的权限进行分离。

风险

未对特权账户进行制约，造成事件发生后无法准确查找原因，无法确定责任人。



措施

规范特权账户承担任务时所需的最低权限。

B-3 未提供安全审计模块

隐患

未提供安全审计模块，或审计内容不全面。

风险

对系统误操作、权限滥用或恶意操作等安全事件难以追溯及准确定位。

措施

提供覆盖每个用户的安全审计功能，对应用系统的用户登录、用户退出、增加用户、修改用户权限等重要安全事件及系统操作内容进行审计。

C

数据安全类

C-1 重要系统未采用加密数据传输

! 隐患

重要系统在通信过程中未采用SSL安全协议实现数据加密传输，对用户口令、会话密钥等敏感信息缺乏加密保护。

⊗ 风险

采用明文传输无法有效防止第三方窃听和篡改通信内容。恶意用户通过窃听通信内容，可直接获得系统用户名/密码，对系统进行攻击。

措施

重要业务系统可通过合理配置中间件实现SSL安全套接字，对通信过程中的用户口令、会话密钥等敏感信息进行加密传输。