《信息安全技术　工业控制系统安全控制应用指南》（GB/T 32919—2016）解读与实施

范科峰　姚相振　周睿康　李　琳　编著

科学出版社

《信息安全技术　工业控制系统安全控制应用指南》（GB/T 32919—2016）解读与实施

范科峰　姚相振
周睿康　李　琳　编著

科学出版社
北京

内 容 简 介

本书按照 GB/T 32919—2016 的章节顺序，对标准内容进行解读并给出实施建议，具体包括：一是标准编制背景、适用范围、规范性引用文件、术语、标准概述等基本信息解读；二是安全控制概述、安全控制基线设计、选择、补充等过程应用解读；三是工业控制系统在策略规程、网络硬件、网络结构、无线连接等方面存在的安全问题解读；四是工业控制系统安全控制措施及安全控制基线解读。

本书为工业控制系统信息安全相关从业人员依据 GB/T 32919—2016 开展工控安全保障相关工作提供了指导依据。

图书在版编目（CIP）数据

《信息安全技术　工业控制系统安全控制应用指南》（GB/T 32919—2016）解读与实施/范科峰等编著. —北京：科学出版社，2016

ISBN 978-7-03-050811-9

Ⅰ. ①信…　Ⅱ. ①范…　Ⅲ. ①工业控制系统-信息安全-安全规程-中国　Ⅳ. ①TP273-65

中国版本图书馆 CIP 数据核字（2016）第 280201 号

责任编辑：赵丽欣　张瑞涛 / 责任校对：刘玉靖
责任印制：吕春珉 / 封面设计：东方人华平面设计部

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

新科印刷有限公司 印刷

科学出版社发行　　各地新华书店经销

*

2016 年 11 月第　一　版　　开本：787×1092　1/16
2016 年 11 月第一次印刷　　印张：14 3/4
字数：354 000

定价：59.00 元

（如有印装质量问题，我社负责调换〈新科〉）
销售部电话 010-62136230　编辑部电话 010-62134021

序

工业控制系统（ICS）包括监控和数据采集系统（SCADA）、分布式控制系统（DCS）、可编程逻辑控制器（PLC）等产品，在核设施、航空航天、装备制造、石油石化、油气管网、电力系统、交通运输、水利枢纽、城市设施等重要领域得到了广泛的应用。最初的工业控制系统遵循专用控制协议、使用专用软硬件而自成独立系统，信息安全问题较少。但是，随着两化深度融合，“中国制造 2025”“互联网+”等国家战略的不断推进，工业控制系统正在通过改变其专用解决方案而越来越多地引入 IT 技术来进行工业改造升级，这在极大地提高工业生产力和引发新的工业革命的同时，也引入了 IT 系统的信息安全（security）问题。这些信息安全问题如果不慎重处理，则有可能造成人身安全和财产损失，甚至危及国家安全。

在应对这些安全问题时，与传统 IT 系统的保密性优先，可靠性、可用性次之的安全目标不同，工业控制系统有着完全不同的安全目标，同时，工业信息系统的运行环境、应用、维护、管理也与原有的 IT 系统大不相同，原适用于 IT 系统的信息安全标准不能照搬至工业控制系统，工业控制系统信息安全保障工作急需一套能应用于实践指导的安全控制指南。

为应对工控系统面临的信息安全威胁，国家信息技术安全研究中心和中国电子技术标准化研究院承担了国家标准《信息安全技术 工业控制系统安全控制应用指南》（以下简称为《指南》）制定项目（项目计划号：20100384-T-469），成立标准工作组，吸纳优秀的企业及院所加入标准研制工作。经过大家共同努力，2016 年 8 月 29 日，《指南》正式发布，国家标准编号为 GB/T 32919—2016，实施日期为 2017 年 3 月 1 日。

该标准的研制工作遵循两个原则：一是充分吸收已有国内外工控信息安全相关标准。本标准在编制过程中充分参考、吸收了国际标准化组织提出的工控安全先进标准，包括 IEC 62443、NIST SP 800—53、NIST SP 800—82、ISA 99 等系列标准，以及国内法律法规、政策、文件和相关标准等资料，确保该标准符合国家有关主管部门开展工控系统信息安全管理以及工控用户企业开展工控信息安全保障能力建设的工作需要。二是标准编制具备通用性、可操作性、实用性等原则。本标准立足于当前工业信息化技术水平，参考国外先进标准，对国内外工控系统分类方法进行总结、归纳、简化，同时针对工控系统特点和需求构建了典型安全控制措施集，具备较强的通用性以及良好的可操作性和实用性，为工控系统信息安全管理、检查及工控信息安全保障能力建设工作提供了坚实基础。

本书编写的目的是帮助读者学习和深入理解 GB/T 32919—2016，不仅要理解标准文本，更需要理解标准中各个控制项的来源、前提、目的、功能和适用范围，以便企业根据自身工业控制系统的现实情况适当选择、裁剪、调整、适配各项控制措施，有效控制工控信息安全风险，抵御信息安全威胁，防范信息安全危害，保障工控系统的信息安全。

本书是学习理解 GB/T 32919—2016 的基础教材，尽量采用平实的语言解读标准中的复杂概念和控制措施。本书在编写过程中得到工控安全主管部门、网络安全和工控安全产业界同行的关注和指导，在此表示感谢！同时也对 GB/T 32919—2016 标准制定的主要承担单位国家信息技术安全研究中心、中国电子技术标准化研究院的各位领导和同事的支持表示感谢！

本书的篇幅较大，介绍力求翔实细致，但由于工控安全问题本身的深度和广度，同时在编写过程中加入了作者实践中的部分个人观点，因此书中难免有不足之处，敬请读者批评指正。

前　言

《信息安全技术　工业控制系统安全控制应用指南》（GB/T 32919—2016）（Information security technology - Application guide to industrial control system security control）是构建我国工业控制系统安全防护的基础性标准，适用于工业控制系统信息安全管理部门和企业，可以为工业控制系统信息安全建设工作提供指导，同时也为工业控制系统信息安全的运行维护以及安全检查工作提供参考。

GB/T 32919—2016 关注各工业行业广泛使用的工业控制系统，规定了工控系统安全控制应用的基本方法，规范了工业控制系统的安全控制选择过程，指导工业企业形成安全控制基线，实现对工控系统进行有效风险管控，为工业企业开展工控安全防护工作提供指导，是重要的信息安全技术标准之一。为了帮助读者学习和理解 GB/T 32919—2016 标准文本，推进其贯彻与实施，特编写了本书。

本书按照 GB/T 32919—2016 的章节顺序进行解读并给出实施建议。本书组成结构如下：

- 第一章　概述，包括编制背景、适用范围、规范性引用文件、术语和缩略语，共四节，分别对 GB/T 32919—2016 的引言和第 1～4 章进行解读。
- 第二章　安全控制应用，包括安全控制概述、安全控制基线及其设计、安全控制选择、基线安全控制补充、建立安全控制决策文档和安全控制选择过程应用，分别对 GB/T 32919—2016 的第 5～8 章进行解读，用于帮助标准使用者全面、正确理解安全控制的应用过程。
- 第三章　工业控制系统面临的安全风险，包括工业控制系统策略规程、网络硬件、网络结构、无线连接和设备配置等方面的脆弱性分析，主要对 GB/T 32919—2016 的附录 A 进行解读。
- 第四章　工业控制系统安全控制列表，主要对 GB/T 32919—2016 的附录 B 进行解读。
- 第五章　工业控制系统安全控制基线，主要对 GB/T 32919—2016 的附录 C 进行解读。

我们在撰写本书时，得到了工业和信息化部工控安全评估专项（工信软函[2015]366 号、工信软函[2016]1181）、国家智能制造专项（京财经一指[2015]1170 号）、国家科技支撑计划课题（No.2012BAI23B07）的资助，并得到了工业和信息化部信息化和软件服务业司有关领导、中央网信办网络安全协调局有关领导、中国电子技术标准化研究院有关领导的支持和指导，相关科研人员也积极贡献他们的智慧和力量，在此一并表示感谢。

受时间及水平所限，本书难免有错漏之处，希望读者朋友批评指正。若有任何意见或建议，请发送邮件至 fankf@126.com。

目　录

第一章 概 述

第一节 编制背景

标准条款 GB/T 32919—2016

引 言

工业控制系统（ICS）（包括监控和数据采集系统（SCADA）、分布式控制系统（DCS）、可编程逻辑控制器（PLC）等产品）在核设施、航空航天、先进制造、石油石化、油气管网、电力系统、交通运输、水利枢纽、城市设施等重要领域得到了广泛的应用。

随着信息技术的发展，特别是信息化与工业化深度融合以及物联网的快速发展，工业控制系统产品越来越多地采用通用协议、通用硬件和通用软件，以各种方式与互联网等公共网络连接，传统信息系统所面临的病毒、木马等威胁正在向工业控制系统领域不断扩散，工业控制系统的信息安全问题日益突出。

工业控制系统安全控制应用指南是针对各行业使用的工业控制系统给出的安全控制应用基本方法，指导选择、裁剪、补偿和补充工业控制系统安全控制，形成适合组织需要的安全控制基线，以满足组织对工业控制系统安全需求，实现对工业控制系统进行适度、有效的风险控制管理。

本标准适用于工业控制系统拥有者、使用者、设计实现者以及信息安全管理部门，为工业控制系统信息安全设计、实现、整改工作提供指导，也为工业控制系统信息安全运行、风险评估和安全检查工作提供参考。

条款解读 1.1

一、目的和意图

作为 GB/T 32919—2016 的编制背景，简要阐述工业控制系统的重要性以及面临的安全形势，体现工业控制系统安全防护工作的必要性和工作内容。

二、解释和示例

工业控制系统信息安全是国家网络和信息安全的重要组成部分，是推动智能制造、“互联网+制造业”发展的基础保障。随着工控系统从单机走向互联、从封闭走向开放、

从自动化走向智能化，工控安全形势日益复杂、严峻和紧迫。然而，当前我国工业控制系统普遍存在着工业控制系统网络安全基础能力薄弱，信息安全防护措施不足，人员安全意识淡薄，重要工业控制系统核心技术产品和关键环节严重依赖国外等问题，一旦其遭受攻击，将直接影响人民生命财产安全和国家政权稳定。为提高我国重要工业领域工业控制系统信息安全防护能力，在参考借鉴了美国 NIST 800—53、NIST 800—82 等国际先进经验的基础上，结合我国工业行业实际发展现状，编制了本标准。

本标准针对各行业使用的工业控制系统给出的安全控制应用基本方法，通过选择、裁剪、补偿和补充工业控制系统安全控制，形成适合组织需要的安全控制措施，帮助组织对工业控制系统开展适度、有效的风险控制管理。此外，本标准可与在研标准《信息安全技术 工业控制系统信息安全分级规范》和《信息安全技术 工业控制系统安全管理基本要求》配套使用，《信息安全技术 工业控制系统信息安全分级规范》将工业控制系统作为定级对象，综合考虑工业控制系统资产重要性、受侵害后的潜在影响和需抵御的信息安全威胁等因素，评判工业控制系统需达到的安全级别，根据该安全级别，可以确定本标准适用的基线，继而得到相应的安全控制措施建议，用以指导具体的工业控制系统信息安全实践工作；《信息安全技术 工业控制系统安全管理基本要求》针对工业企业等组织的工业控制系统，提出安全管理基本框架和安全要求，并根据工业控制系统需达到的安全等级，提供通用的参考性安全管理详细需求；本标准通过提供的选择、裁剪、补偿和补充等活动，提供了构建适合组织实际需求的安全控制基线，为工业企业等组织建立安全防护体系提供指导。

本标准适用于工业控制系统信息安全管理部门和企业，为工业控制系统信息安全建设工作提供指导，工业控制系统信息安全的运维以及安全检查工作均可参考使用。标准中安全控制措施一般分为控制和增强控制，工业企业可根据自身生产活动和实际情况，依据风险评估等活动的结果灵活选择。

第二节 适 用 范 围

标准条款 GB/T 32919—2016

1. 范围

本标准提供了可用于工业控制系统的安全控制列表，规约了工业控制系统的安全控制选择过程，以便构造工业控制系统的安全程序——一种概念层面上的安全解决方案。

本标准适用于：

1）方便规约工业控制系统的安全功能需求，为安全设计（包括安全体系结构设计）和安全实现奠定有力的基础。

2）指导工业控制系统安全整改中安全能力的调整和提高，以便能使工业控制系统保持持续安全性。

本标准的适用对象是负责工业控制系统建设的组织者、负责信息安全工作的实施者和其他从事信息安全工作的相关人员。

条款解读 1.2

一、目的和意图

界定 GB/T 32919—2016 的适用范围。

二、解释和示例

本标准提供了一种针对工业控制系统安全控制选择过程的方法，可以帮助工业企业根据自身需求、实际现状和安全评估结果，构建一种概念层面上的安全解决方案。本标准既可独自使用，也可与其他分级、要求、评估等标准配套使用。

第三节 规范性引用文件

标准条款 GB/T 32919—2016

2. 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

《信息安全技术 术语》（GB/T 25069—2010）

《信息安全技术 信息系统安全等级保护定级指南》（GB/T 22240—2008）

条款解读 1.3

一、目的和意图

提供 GB/T 32919—2016 正文中所引用的相关标准或规范性文件的信息。

二、解释和示例

GB/T 32919—2016 列出了 2 项引用的国家标准：

- 《信息安全技术 术语》（GB/T 25069—2010）。该标准界定了与信息安全技术领域相关的概念的技术和定义，并明确了这些条目之间的关系。该标准适用于信息安全技术概念的理解，有利于其他信息安全技术标准的制定以及信息安全技术的国内外交流。
- 《信息安全技术 信息系统安全等级保护定级指南》（GB/T 22240—2008）该标准依据等级保护相关管理文件，从信息系统所承载的业务在国家安全、经济建设、

社会生活中的重要作用和业务对信息系统的依赖程度这两方面，提出确定信息系统安全保护等级的方法，适用于为信息系统安全等级保护的定级工作提供指导。

第四节 术语和缩略语

标准条款 GB/T 32919—2016

3. 术语和定义

GB/T 25069—2010 界定的以及下列术语和定义适用于本标准。

3.1 工业控制系统（ICS，industrial control system）

工业控制系统（ICS）是一个通用术语，它包括多种工业生产中使用的控制系统，包括监控和数据采集系统（SCADA）、分布式控制系统（DCS）和其他较小的控制系统，如可编程逻辑控制器（PLC），现已广泛应用在工业部门和关键基础设施中。

3.2 监控和数据采集系统（SCADA，supervisory control and data acquisition system）

在工业生产控制过程中，对大规模远距离地理分布的资产和设备在广域网环境下进行集中式数据采集与监控管理的控制系统。它以计算机为基础、对远程分布运行设备进行监控调度，其主要功能包括数据采集、参数测量和调节、信号报警等。SCADA 系统一般由设在控制中心的主终端控制单元（MTU）、通信线路和设备、远程终端单元（RTU）等组成。

3.3 分布式控制系统（DCS，distribution control system）

以计算机为基础，在系统内部（组织内部）对生产过程进行分布控制、集中管理的系统。DCS 系统一般包括现场控制级和控制管理级两个层次。现场控制级主要是对单个子过程进行控制，控制管理级主要是对多个分散的子过程进行调度管理、数据采集和集中显示。

3.4 可编程逻辑控制器（PLC，programmable logic controller）

采用可编程存储器，通过数字运算操作对工业生产装备进行控制的电子设备。PLC 主要执行各类运算、顺序控制、定时执行等指令，用于控制工业生产装备的动作，是工业控制系统的主要基础单元。

3.5 安全控制（security control）

应用于工业控制系统的管理、运行和技术上的防护措施和对策，以保护工业控制系统及其信息的保密性、完整性和可用性等。

3.6 安全程序（security program）

在工业控制系统的安全建设中，为满足组织安全需求和安全目的，适当采选的一组有序的安全控制集。

3.7 安全控制族（security control family）

本标准将相关主题的安全控制作为一个安全控制族，所有的安全控制分成 18 个

安全控制族，即：规划（PL）、安全评估与授权（CA）、风险评估（RA）、系统与服务获取（SA）、程序管理（PM）、人员安全（PS）、物理与环境安全（PE）、应急计划（CP）、配置管理（CM）、维护（MA）、系统与信息完整性（SI）、介质保护（MP）、事件响应（IR）、教育培训（AT）、标识与鉴别（IA）、访问控制（AC）、审计与问责（AU）、系统与通信保护（SC）。

3.8 安全控制基线（security control baseline）

安全控制基线是安全控制选择过程的起始点，是为帮助组织选择满足安全需求的、最具成本效益的、适当的安全控制集而制定的最低安全基准线。

4 缩略语

下列缩略语适用于本文件。

ICS 工业控制系统（Industrial Control System）

SCADA 监控与数据采集系统（Supervisory Control And Data Acquisition）

DCS 分布式控制系统（Distributed Control System）

PCS 过程控制系统（Process Control System）

PLC 可编程逻辑控制器（Programmable Logic Controller）

RTU 远程终端单元（Remote Terminal Unit）

IED 智能电子设备（Intelligent Electronic Device）

DRP 灾难恢复计划（Disaster Recovery Planning）

ACL 访问控制列表（Access Control List）

DNS 域名系统（Domain Name System）

DHCP 动态主机配置协议（Dynamic Host Configuration Protocol）

DNP 分布式网络协议(Distributed Network Protocol）

RPC 远程过程调用协议（Remote Procedure Call Protocol）

DCOM 分布式组件对象模式（Microsoft Distributed Component Object Model）

OPC 用于过程控制的对象连接与嵌入(Object Linking and Embedding for Process Control)

PAD 个人数字助手，又称掌上电脑（Personal Digital Assistant）

DoS 拒绝服务(Denial of Service)

CVE 通用漏洞列表(Common Vulnerabilities and Exposures)

OVAL 脆弱性评估语言（Open Vulnerability Assessment Language）

EAL 评估保证级（Evaluation Assurance Level）

PKI 公钥基础设施(Public Key Infrastructure)

AC 访问控制（Access Control）

AT 教育培训（Awareness and Training）

AU 审计与问责（Audit and Accountability）

CA 安全评估与授权（Security Assessment and Authorization）

CM 配置管理（Configuration Management）
MA 维护（Maintenance）
CP 应急计划（Contingency Planning）
IA 标识与鉴别（Identification and Authentication）
IR 事件响应（Incident Response）
MP 介质保护（Media Protection）
PE 物理与环境安全（Physical and Environmental Protection）
PL 规划（Planning）
PM 程序管理（program management)
PS 人员安全（Personnel Security）
RA 风险评估（Risk Assessment）
SA 系统与服务获取（System and Services Acquisition）
SC 系统与通信保护（System and Communications Protection）
SI 系统与信息完整性（System and Information Integrity）

条款解读 1.4

一、目的和意图

定义了工业控制系统信息安全领域的相关术语，术语引用了《信息安全技术—术语》（GB/T 25069—2010）中的术语定义，并在工业控制系统领域内为其作了更为清晰的界定，能够为本标准使用者提供严谨、清晰的概念定义。

二、解释和示例

3.1 工业控制系统（ICS）

工业控制系统（ICS，Industrial Control System）（也称工业自动化与控制系统）是由计算机设备与工业过程控制部件组成的自动控制系统，工业控制系统被广泛地应用于电力、水处理、石油与天然气、楼宇自动化、化工、交通运输、制造业等行业。在震网病毒爆发后，国家关键基础设施的控制系统也纳入了工业控制系统定义之内，并作为其重要组成部分，逐渐成为国家空间安全和信息安全的关注热点。国际自动化协会（ISA）与 IEC/TC65/WG 整合后发布的《工业过程测量、控制和自动化网络与系统信息安全》（IEC 62443）也曾对工业控制系统给出了定义，即："工业控制系统包括了制造和加工厂站和设施、建筑环境控制系统、地理位置上具有分散操作性质的公共事业设施（如电力、天然气）、石油生产以及管线等进行自动化或远程控制的系统"。该定义与本标准中工业控制系统中的定义基本相符。

通常情况下，工业控制系统的子系统或功能组件包括但不限于：

1）数据采集与监控系统（SCADA）、分布式过程控制系统（DCS）、可编程逻辑控制器（PLC）、远程测控单元（RTU）、网络电子传感/监视/控制/诊断系统等。

2）相关信息系统，如图形化界面、过程历史库、制造执行系统（MES）以及厂站信息管理系统。

3.2 监控和数据采集系统（SCADA）

SCADA（Supervisory Control And Data Acquisition）系统，即数据采集与监视控制系统，涉及组态软件、数据传输链路（如数传电台、GPRS 等）工业隔离安全网关，其中安全隔离网关是保证工业信息网络安全的，大多数工业信息网络都要用到这种安全防护性的网关，防止病毒，以保证工业数据、信息的安全。

目前，SCADA 系统在电力系统中的应用最为广泛，技术发展也最为成熟。它作为能量管理系统（EMS 系统）的一个最主要的子系统，有着信息完整、可提高效率、可正确掌握系统运行状态、可加快决策、可帮助快速诊断出系统故障状态等优势，现已经成为电力调度不可缺少的工具。它在提高电网运行的可靠性、安全性与经济效益，减轻调度员工作负担，实现电力调度自动化与现代化，提高调度的效率和水平等方面有着不可替代的作用。

其次，铁道电气化远动系统也是 SCADA 应用的主要领域之一，该领域 SCADA 应用得较早，且在保证电气化铁路的安全可靠供电、提高铁路运输的调度管理水平上起到了很大的作用。在我国铁道电气化 SCADA 系统的发展过程中，随着计算机的发展，不同时期对应着不同的产品，其中包括从国外引进的大量的 SCADA 产品与设备。SCADA 在我国铁道电气化远动系统发展中占据着举足轻重的地位。

3.3 分布式控制系统（DCS）

DCS 是分布式控制系统（Distributed Control System）的简称，国内一般习惯称为集散控制系统。它通常是一个由过程控制级和过程监控级组成的以通信网络为纽带的多级计算机系统，综合了计算机（Computer）、通信（Communication）、显示（CRT）和控制（Control）等 4C 技术，其基本思想是分散控制、集中操作、分级管理、配置灵活、组态方便。

随着现代计算机和通信网络技术的高速发展，DCS 正向着多元化、网络化、开放化、集成管理方向发展，使得不同型号的 DCS 可以互连，进行数据交换，并可通过以太网将 DCS 系统和工厂管理网相连，实现实时数据上网。使用以太网技术的 DCS 已成为过程工业自动控制的主流。

DCS 应用的一个主要行业是火电厂，近几年来，各火电厂为提高生产效率，实现工厂管理信息系统与各种分散控制系统（DCS）之间的数据交换，实现整个电厂范围内信息共享，实现厂级生产过程的实时信息监控和调度，广泛采用 IT 技术来改造 DCS。以采用 IT 技术 DCS 为基础的厂级监控信息系统渐渐流行。

3.4 可编程逻辑控制器（PLC）

可编程逻辑控制器实质是一种专用于工业控制的计算机，其硬件结构基本上与微型计算机相同，基本构成为：电源、中央处理单元（CPU）、存储器、输入输出接口电路、功能模块、通信模块。当可编程逻辑控制器投入运行后，其工作过程一般分为三个阶段，即输入采样、用户程序执行和输出刷新。完成上述三个阶段称作一个扫描周期。在整个运行期间，可编程逻辑控制器的 CPU 以一定的扫描速度重复执行上述三个阶段。

PLC 控制系统实例：十字路口红绿灯控制、洗手间自动冲水控制、地下停车场出入红绿号标志控制、喷水池控制、自动门控制等。

第二章　安全控制应用

内容要点

从本章开始解读标准的主体内容。本章主要内容包括：工业控制系统信息安全相关方应根据自身实际需求和风险评估等结果，建立安全保障体系，提高安全防护水平。为此，本章给出了安全控制相关内容的介绍，主要包括安全控制的概述，讲述了针对每个安全控制的描述格式，如控制、补充指导、增强控制等，给出了安全控制基线的基本概念、前期假设等内容，提供了安全控制的选择、裁剪、补充的具体实施方法，指导企业在安全控制程序构建过程中建立安全控制决策文档，从而帮助企业建立工业控制系统信息安全防护体系。

第一节　安全控制概述

标准条款 GB/T 32919—2016

5. 安全控制概述

从概念上来说，工业控制系统的安全与其他领域的安全是一样的，如图 2.1 所示。

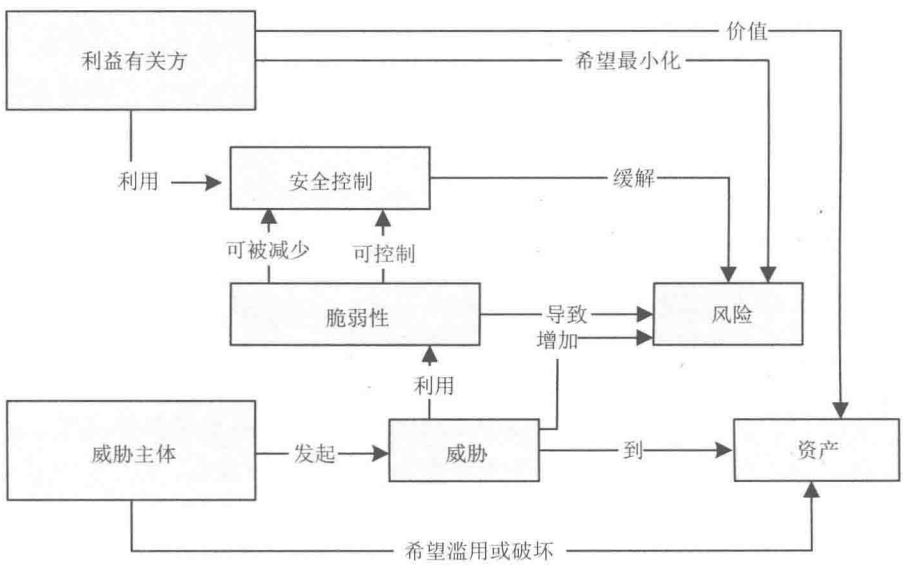

图 2.1　安全（security）及其相关概念

图 2.1 表明了安全及其相关概念间的关系。其中的控制是指：应用于工业控制系统中管理、运行和技术上的保护措施和对策，以保护工业控制系统及其信息的保密性、完整性和可用性等。应用这些控制的目的是减少脆弱性或影响，抵御工业控制系统所面临的安全威胁，从而缓解工业控制系统的安全风险，以满足利益相关者的安全需要。

本标准附录 B 中给出了可用于工业控制系统的安全控制列表。

为了有效地表达工业控制系统中管理、运行和技术上的措施和对策，应给出该措施对应的动作、输入/输出及其对应的前置条件和后置条件，特别是给出该控制的效果。例如，关于审计处理失效响应的控制如下。

控制：

工业控制系统：

a）对于审计处理失效的事件，向【赋值：组织定义的人员】报警；

b）采取【选择：组织定义的动作，例如：停止系统的运行，重写原有的审计记录，停止生成新的审计记录等】。

其中的“报警”和“采取组织定义的动作”，就是该控制对应的动作；而“审计处理失效的事件”就是该控制的一个输入；“向组织定义的人员（报警）”就是该控制的一个后置条件。并且通过补充指导，强调了该措施和对策的其他要素，例如：

补充指导：

a）审计处理失效包括软硬件错误、审计获取机制失败、审计存储空间达到或超出极限等；

b）组织可针对不同审计处理失效（例如，由于类型、位置、严重程度或这些因素的组合），选择定义附加的措施；

c）该控制应用于每个审计数据存储库（即存储审计记录的 ICS 部件），应用于组织的整个审计存储能力（即组合了所有审计数据存储库）；

d）在 ICS 不支持审计的情况下，包括对审计失效的响应，组织应按裁剪指导，使用合适的补偿控制（例如，在隔离的信息系统上提供审计能力）；

e）相关安全控制：AU-4、SI-12。

如果有必要强调一个控制在深度上的能力，以支持更可靠的保护，可通过控制增强来表达，例如，就上述的控制而言，其控制增强可表达为：

控制增强：

a）对审计处理失效/审计存储能力的响应。在【赋值：组织定义的时间段】内，当分配给审计记录的存储量达到【赋值：组织定义的最大审计记录存储容量】的某一百分比时，ICS 向【赋值：组织定义的人员、角色或岗位】提供一个警示；

b）对审计处理失效|实时报警的响应。当【赋值：组织定义的、要求实时报警的审计失效事件】发生时，ICS 在【赋值：组织定义的实时报警时间段】内，向【赋值：组织定义的人员、角色和岗位】发出报警；