ICS 43.020

CCS T 40

团　　体　　标　　准

T/GHDQ 101-2022

车辆生产运营阶段信息安全技术要求

Technical requirements for Information Security in vehicle production and operation stage

2022-11-02 发布　　2022-11-03 实施

吉林省汽车电子协会　发 布

目　　次

前　言

本文件按照GB/T 1.1-2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国第一汽车集团有限公司智能网联开发院、启明信息技术股份有限公司联合提出。

本文件由吉林省汽车电子协会归口。

本文件由吉林省汽车电子协会组织实施。

本文件主要起草单位：启明信息技术股份有限公司、中国第一汽车集团有限公司集工程与生产物流部、中国第一汽车集团有限公司智能网联开发院。

本文件主要起草人：李丹、董玮、李岩、刘宇航、赵沛时、辛明、魏利、陈有志、郭宏伟、吉岩、渠谨黛、谷淼、陈后立、边泽宇。

本文件参与起草单位：吉林大学汽车仿真与控制国家重点实验室、沙龙机甲科技有限公司、一汽奔腾轿车有限公司、中国汽车技术研究中心有限公司、联通智网科技股份有限公司、长春吉大正元信息技术股份有限公司、一汽-大众汽车有限公司、中电信数智科技有限公司长春分公司、中电福富信息科技有限公司。

本文件参与起草人：李杰、王思涵、雷凯、李宝田、刘书勇、苏日、王博、孙冰楠、于鑫淼、陈雄华。

本文件审查人：杨彦鼎（东风汽车集团有限公司技术中心）、夏国强（中国汽车工程研究院股份有限公司）、马文峰（一汽奔腾轿车有限公司）、马喜来（一汽解放汽车有限公司）、占锐（东风汽车集团有限公司技术中心）、孔晓霜（中国第一汽车集团有限公司创新技术研究院）。

本文件为首次发布。

引　言

近年来，随着网络技术的飞速发展，各类信息安全事故频繁发生，对经济、人员、环境、业务连续性、国家安全产生重大影响，信息安全威胁伴随着车辆的研发、生产、使用等各阶段车辆的全生命周期。

本文件规定了生产及运营阶段实施的信息安全活动与要求，主要目的是确保开发的信息安全规范在生产运营中得到实施，防止生产运营过程中引入额外的信息安全漏洞，避免或降低信息安全攻击产生的影响。

车辆生产运营阶段信息安全技术要求

1 范围

本文件规定了一个组织在汽车生产阶段和运营阶段为保证信息安全而实施的管理策略与活动的要求。车辆信息安全技术、解决方案或补救措施的内容不在本文件的范围内。

本文件适用于汽车制造企业及相关零部件、设备生产商与系统集成服务供应商。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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。

GB/T 20720.1-2019 企业控制系统集成 第1部分：模型和术语

ISO 21434 道路车辆 网络安全工程（Road vehicles — cybersecurity engineering）

3 术语和定义

GB/T 20720.1和ISO 21434界定的以及下列术语和定义适用于本文件。

3.1

弱点 weakness

一个或多个威胁可以利用的项目或控件的弱点。

3.2

漏洞 vulnerability

系统设计、实现或操作和管理中存在的缺陷或弱点，可被利用来危害系统的完整性或安保策略。

3.3

更新 updates

对部署在现场的信息安全相关项目的硬件或软件所做的更改。

更新跟据其功能分为功能性更新和补救性更新。

3.4

信息安全事态 cybersecurity event

系统、服务或网络的一种可识别的状态的发生，它可能是对信息安全策略的违反或防护措施的失效，或是和安全关联的一个先前位置的状态。

已确认可能与组织或其产品相关并已升级到漏洞处理和事件响应过程的信息安全信息。

3.5

信息安全事件 cybersecurity incident

一个信息安全事件由单个的或一系列的有害或意外信息安全事态组成，它们具有损害业务运作和威胁信息安全的极大的可能性。

经评估需要启动事件响应流程的信息安全事件。

3.6

离线环境 offline environment

指的是与生产环境物理隔离的环境。

4 缩略语

下列缩略语适用于本文件：

DMZ：demilitarized zone 隔离区；

FTP：FileTransferProtocol 文件传输协议；

HTTP：Hyper Text Transfer Protocol 超文本传输协议；

ID 卡：Identification Card 身份识别卡；

Telnet：远程终端协议；

VPN：Virtual Private Network 虚拟专用网络。

5 组织管理

5.1 总则

组织应通过建立生产运营阶段信息安全管理机制、成立信息安全协调小组等方式，明确信息安全管理责任人，落实信息安全责任制，部署信息安全防护措施，对整个过程进行管理、实施和评估，培育和建立信息安全文化。

5.2 安全组织要求

建立一个安全的组织架构并建立责任制。

该组织对生产及运营阶段的整个信息安全进行管理、实施和评估。

组织应获得高级管理层的支持，对安全项目的承诺从组织高层开始，高层领导建立组织、结构或人员网络为信息安全管理提供监督和方向指导，并提供必要的人员制定、执行和评估信息安全策略、规程和活动。

5.3 安全策略和规程要求

5.3.1 范围

组织应基于现有风险特征及承受水平定义安全策略，建立信息安全规程来识别角色和职责。

组织应制定生产运营阶段相关的政策和程序，包括但不限于：

a） 生产阶段信息安全责任的政策和程序；

b） 信息安全监控的政策和程序；

c） 处理信息安全事件漏洞的政策和程序；

d） 事件响应的政策和程序；

e） 支持结束和退役程序；

f） 人员安全策略；
g） 信息共享策略和程序；
h） 汽车数据安全管理制度。

5.3.2 改进

在关键流程变更、重特大信息安全事件发生后，及时更新完善信息安全管理规范、安全机制等。

5.4 人员管理要求

5.4.1 制定人员安全策略

应制定人员安全策略，清晰阐明相关人员的安全职责。相关人员包括雇员、潜在雇员、第三方雇员等。

安全职责应于任用前在岗位描述、任用条款和条件中明确指出。

5.4.2 人员筛查

所有要雇用承包方人员和第三方人员的候选者应充分的审查。应签署相关安全角色职责的协议，确保人员在整个雇用期间维护网络的安全。

筛查对象和方式包括：
a） 对初始人员进行筛查；
b） 持续的人员筛查；
c） 对新进人员和在职人员的考察筛选。

5.4.3 人员安全培训

应使所有相关人员得到足够的与硬件、软件和社会工程相关的已知威胁和漏洞的技术培训。

培训的内容包括但不限于：
a） 组织机构的安全方针策略；
b） 安全意识；
c） 应当遵守的安全规程；
d） 发生信息安全事件的报告职责和报告方法；
e） 满足岗位职责需要具备的安全知识与技能。

培训应持续进行，并对培训效果进行验证，必要时考虑新的和变化的威胁和漏洞及时修订培训计划，以确保相关人员正在接受适当的培训。

5.4.4 纪律处理

对于安全违规的人员，应有一个正式的纪律处理过程。

处理过程应规定一个分级的响应，要考虑诸如违规的性质、重要性及影响等因素，相关法律、业务合同和其他因素也是需要考虑的。

5.4.5 终止任用

雇员、承包方人员和第三方人员从组织退出，终止任用、合同或协议时，应归还所有组织资产，包括发放的软件、公司文件、访问卡和设备等。

雇员、承包方人员和第三方人员从组织退出，终止任用、合同或协议时，应删除他们的所有访问权。

注：访问权包括物理和逻辑访问、密钥、ID 卡、信息处理设施、签名等，并要从标识其作为组织的现有成员的文件中删除。

如果一个已离开的雇员、承包方人员或第三方人员知道仍保持活动状态的账户的密码，则应修改密码。

任用的变化应体现在不适用于新岗位的访问权的删除上。

当人员的职责调整时，应对职责对应的访问权限进行调整。

6 生产阶段的信息安全要求

6.1 信息安全要求导入

在进入车辆生产阶段后应立即导入开发阶段制定的对生产运营阶段的信息安全要求。

比如：在生产阶段导入开发阶段制定的对于密钥烧写过程的要求。

6.2 生产控制计划

应制定一份汽车生产控制计划，用于防止生产过程中未经授权的变更，并在整个生产过程中执行生产控制计划。

生产控制计划应包括：

a） 生产的步骤顺序；

b） 生产工具和设备；

c） 软件版本；

d） 硬件版本；

e） 信息安全控制措施，防止生产过程中未经授权的变更；

例如：阻止对包含软件的生产服务器进行物理访问的物理控制；应用加密技术和/或访问控制的逻辑控制。

f） 确认满足信息安全要求的方法。

6.3 供应商管理

6.3.1 能力评估

在选择管理控制系统规划、设计、建设、运维或评估等供应商时，优先考虑具备安全防护经验的企事业单位，以合同等方式明确供应商应承担的信息安全责任和义务。

以保密协议的方式要求供应商做好保密工作，防范敏感信息外泄。

6.3.2 供应商关系中的信息安全

应建立分布接口协议，明确信息安全活动的职责分配，定义客户和供应商之间分布式信息安全活动的相互作用、依赖关系和责任。

6.3.3 供应商服务交付管理

应明确供方产品和服务的信息安全评价标准、验证规范等，确定与供方的安全协议，协同管控供应链信息安全风险。

6.4 物流与运输过程

组织应建立控制措施，以确保供应链包含足够的控制措施和过程，以保护软件和硬件在物流和运输过程中的完整性。

6.5 更新

应分析所有车辆电控单元的软件的升级更新对信息安全的影响。

应建立控制措施，以保护所有更新的完整性。

更新应包含更新发布者的身份，可以通过使用数字手段（如密码技术）或其他非数字手段（如安全传送方法）来实现。

每次更新应具有唯一可识别性。

应将其补救性更新分类为严重或非严重，并且该分类将包含在更新中。更新的接收者应该优先评估标记为严重的更新。

6.6 变更管理

组织应对生产阶段的变更进行评估，以确保这些变更不会影响信息安全规范在生产项目中的实施。

生产阶段的变更包括：生产顺序的变更、生产系统的变更、生产地点的变更以及其他变更。

7 运营阶段的信息安全要求

7.1 总则

车辆运营阶段的主要活动包括信息安全监控、信息安全事态评估、脆弱性分析、漏洞管理和信息安全事件响应等过程，过程关系的具体表示见图 1。

应记录数据以支持网络攻击的检测，并提供数据取证能力，以便对未遂或成功的网络攻击行为进行分析。

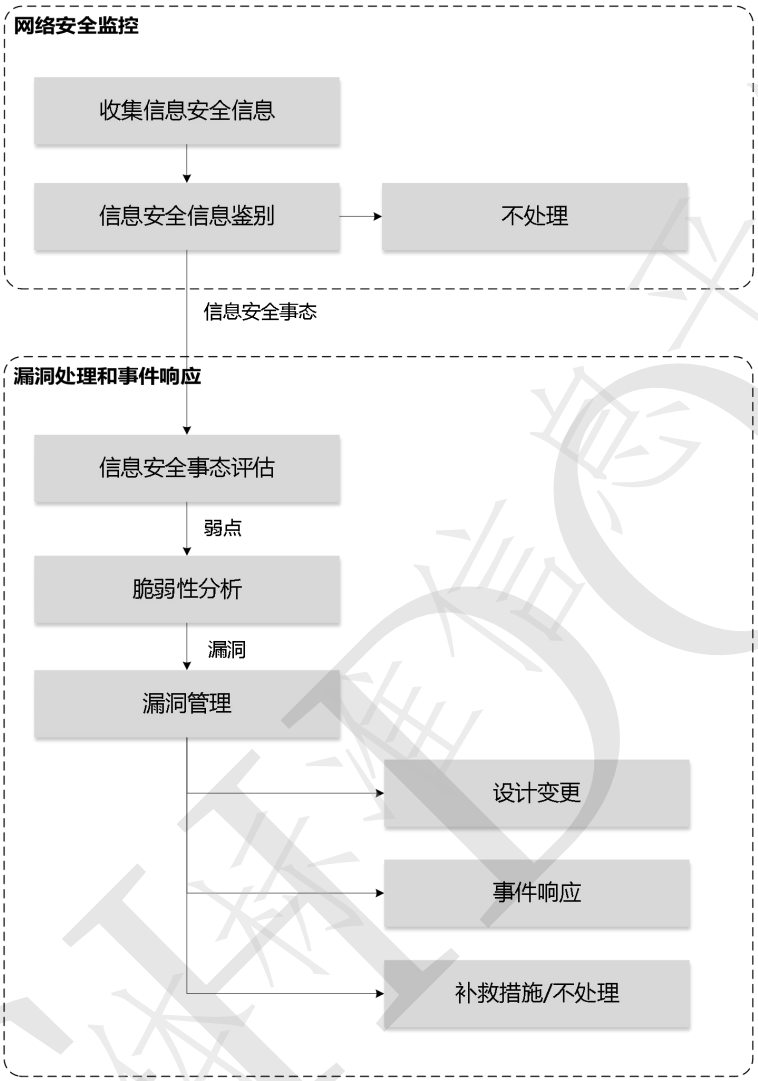

图 1　运营阶段活动流程

7.2　信息安全监控

7.2.1　监控过程总则

信息安全监控提供有关信息安全威胁和漏洞的信息，从概念阶段开始，并持续到项目的整个现场运行，以避免已知问题和应对新的威胁。

组织应制定信息安全监控的政策和程序，这些政策和程序应包括但不限于：

a）　确定信息源可信性的可靠性准则；

b）　组织内部信息共享程序：

1）　确定内部各方；

2）　制定通知程序。

c）　分析信息安全信息的过程。

7.2.2　收集信息安全信息

信息安全信息的收集可选择内部和/或外部来源。

a） 内部来源可包括：

1） 项目定义；

2） 信息安全规范；

3） 威胁场景；

4） 过去的脆弱性分析；

5） 从现场收到的信息。

b） 外部来源可包括：

1） 研究人员；

2） 商业或非商业来源；

3） 组织的供应链；

4） 组织的顾客；

5） 政府消息来源。

确定信息源可信性的可靠性准则，组织内部信息共享程序。

7.2.3 信息安全信息鉴别

应定义和维护信息安全信息鉴别规则，以便对信息安全信息进行分类与分析，确定该信息是否升级为信息安全事态。

7.3 信息安全事态评估

应对信息安全事态进行评估，以确定项目和/或组件中的弱点。

如果存在弱点，并且有可用的补救措施（例如，供应商为组件中的漏洞提供的修补程序），则组织可以实施补救措施，而无需任何其他活动。

7.4 脆弱性分析

应对弱点进行攻击路径分析及攻击可行性评级，以识别弱点是否会导致系统出现漏洞。应为未确定为漏洞的弱点提供判断依据。

若攻击路径分析显示不存在任何攻击路径，则该弱点不被视为漏洞。

若对弱点实施攻击的可行性评级非常低，则该弱点不被视为漏洞。（例如：使用基于通用漏洞评分系统，得出的评估值低于 1.05）。

7.5 漏洞管理

应根据之前信息安全事态的评估结果和脆弱性分析结果，进行漏洞管理，保证相应的风险被处置。

应根据攻击可行性等级和影响等级，进行风险处置决策，风险处置决策包括：缓解、消除、接受。

对于漏洞采取的不同措施有：设计变更、信息安全事件响应、补救措施（如打补丁）。

应对漏洞措施的实施进行跟踪。

7.6 信息安全事件响应

对于每个信息安全事件，应制定并实施信息安全事件响应计划，信息安全事件响应计划包括：

a） 沟通计划：

1） 沟通计划的制定可能涉及内部相关方（例如营销或公共关系、产品开发团队、法律、客户关系、质量管理、采购）；

2） 沟通计划可包括确定内部和外部沟通伙伴（例如开发、研究人员、公众、当局）以及为这

些受众开发特定信息。

b） 分配补救行动的责任，负责人需要具有：

1）受影响的项目或组件的专业知识，包括遗留项目和组件；

2）组织知识（例如业务流程、沟通、采购、法律）；

3）决策权。

c） 补救行动；

d） 记录与信息安全事件相关的信息安全信息的程序，如：

1） 受影响的组件；

2） 相关事件和漏洞；

3） 取证数据（例如数据日志、碰撞传感器数据）或最终用户投诉。

e） 确定进度的方法，衡量进展的例子有：

1） 已补救的受影响项目或组件的百分比；

2） 或者受补救措施影响的项目或组件的百分比。

f） 关闭信息安全事件响应的标准和关闭的行动。

8 管理控制系统要求

8.1 功能要求

8.1.1 功能总则

生产运营管理控制系统应具备一定的信息安全保障能力，系统具备的功能可包含资产发现、入侵检测、响应取证等。

8.1.2 资产发现

定期通过主动扫描、被动发现、手工录入和人工排查等多种方法收集当前网络中所有软硬件资产，包括全网所有的端点资产和在用的软件名称、版本，确保整个网络中没有安全盲点。

8.1.3 入侵检测

应建立防病毒和恶意软件入侵管理机制，对管理控制系统及临时接入的设备采取病毒查杀等安全预防措施。

8.1.4 响应取证

针对全网的安全威胁进行可视化展示，能够针对安全威胁自动化地进行隔离、修复和补救，自动完成安全威胁的调查、分析和取证工作。

8.2 信息安全要求

8.2.1 网络划分与边界安全防护

网络划分与边界安全防护应满足如下条件：

a） 对生产运营管理控制系统的开发、测试和生产环境进行分离；

b） 通过网络边界防护设备对管理控制系统网络与企业网或互联网之间的边界进行安全防护，禁止没有防护的管理控制系统网络与互联网连接；

c） 建立 DMZ 和工厂防火墙，部署工厂防火墙管理在企业和制造区之间的信息流。不同区域之间的 DMZ 中的数据和服务能够安全地共享；

d） 从一个区域企图访问另一个区域的资源时，强制执行用户鉴定；

e） 采取内部网络分段机制，对不同的工作单元进行风险评估，根据不同的评估结果划分不同的防护等级，各工作单元间进行边界安全防护，防止风险由一个工作单元扩散到其他工作单元。

8.2.2 系统部署

应在主机上采用经过离线环境中充分验证测试的防病毒软件或应用程序白名单软件。

只允许经过主机厂自身授权和安全评估的软件运行。

应建立系统配置清单，定期进行配置审计。

8.2.3 系统维护

应对重大配置变更制定变更计划并进行影响分析，配置变更实施前进行严格的安全测试。

应密切关注重大工控安全漏洞及其补丁发布，及时采取补丁升级措施。在补丁安装前，对补丁进行严格的安全评估和测试验证。

应删除不使用的应用程序、协议和服务等，禁用冗余和不需要的服务。

8.2.4 身份认证与访问控制

应在主机登陆、应用服务资源访问、云平台访问等过程中使用身份认证管理。

对于关键设备、系统和平台的访问采用多因素认证。

应合理分类配置账户权限，以最小特权原则分配账户权限。

应强化登陆账户及口令，避免使用默认账户、默认口令或弱口令，口令设置要提高复杂度并定期更新。

应加强对身份认证证书信息保护力度，禁止在不同系统和网络环境下共享。

为了制造产品并安装必要的硬件和软件，生产阶段应使用高度特权访问。一旦产品被生产和测试，生产访问就应被移除，或者可以设置控制来防止使用此访问。

8.2.5 远程访问安全

原则上禁止管理控制系统面向互联网开通 HTTP、FTP、Telnet 等高风险通用网络服务。

确需远程访问的，采用数据单向访问控制等策略进行安全加固，对访问时限进行控制，禁止访问方在远程访问期间实施非法操作。

确需远程维护的，应通过对远程接入通道进行认证、加密等方式保证其安全性，如采用虚拟专用网络（VPN）等方式，对接入账户实行专人专号，并定期审计接入账户操作记录。

应保留管理控制系统设备、应用等访问日志，并定期进行备份，通过审计人员账户、访问时间、操作内容等日志信息，追踪定位非授权访问行为。

8.2.6 冗余备份

应对关键业务数据，如工艺参数、配置文件、设备运行数据、生产数据、控制指令等进行定期备份。

9 资产管理

9.1 范围

对以下类型的资产进行资产管理：

a） 信息资产：数据库和数据文件、培训材料、操作和支持程序、业务连续性计划、审核跟踪记录等；

b） 软件资产：应用软件、系统软件、开发工具、实用程序等；

c） 物理资产：计算机设备、通信设备、可移动介质、生产工装设备等；
d） 服务：计算和通信服务、设施服务，如：供暖、照明、能源等；
e） 人员：人员的资格、技能、经验和健康等；
f） 无形资产：组织的声誉形象等。

9.2 总则

9.2.1 有关资产的责任

应为所有资产指定部门或人员承担管理责任，责任方的责任包括：
a） 确保资产进行了适当的分类和访问限制，并监督访问限制的执行情况；
b） 确定资产允许的使用规则，并形成文件加以实施。如：邮件与互联网使用规则，移动设备使用规则等。

9.2.2 识别安全资产

应建立资产清单，明确资产责任人，以及资产使用及处置规则，对关键主机设备、网络设备、控制组件等进行冗余配置。

9.2.3 制定资产的控制程序

应建立并应用控制措施，以保护从开发阶段收到的软件和硬件不受未经授权的访问、删除或更改。包括物理访问和逻辑访问。

可能的逻辑控制可以包括密码技术和/或访问控制。物理控制可能包括防止对持有软件的生产服务器进行物理访问。

组织应建立并实施控制措施，以保护生产设施中从供应商处收到的软件和硬件不被未经授权的访问、删除或更改。

9.3 环境、设备与工具管理要求

9.3.1 安全区域的访问控制

关键或敏感的信息处理设施应放置在安全区域内，并受到确定的安全边界（如墙、卡控制的入口或有人管理的接待台等）的保护，包括适当的安全屏障和入口控制，确保只有授权的人员才允许访问。

应记录访问者进入和离开的日期和时间。

敏感区域的访问要受到控制，所有访问者在进入敏感区域内要佩戴可视标识，如遇无人护送的访问者或未佩戴可视标识的任何人应立即通知保安人员。

对重要工程师站、数据库、服务器等核心软硬件所在区域采取访问控制、视频监控、专人值守等物理安全防护措施。

对安全区域的访问权应定期予以评审和更新，并在需要时废除。

9.3.2 介质处理

拆除或封闭主机上不必要的 USB、光驱、无线等接口。若确需使用，通过主机外设安全管理技术手段实施严格访问控制。

9.3.3 设备与工具管理

应管理可能影响项目或组件信息安全的工具，包括软件工具。管理方式包括但不限于：
a） 使用带有勘误表的用户手册；

b） 防止意外使用或行动；
c） 工具用户的访问控制；
d） 工具的身份验证。

9.4 信息和文档管理

9.4.1 信息分类维护

应对信息进行分类分级，指明保护的需求、优先级和期望程度。

信息分类应按照其对组织的价值、法律要求、敏感性和关键性。

保密级别可通过分析信息的保密性、完整性、可用性及其他要求进行评估。

分类等级如：机密级/限制级/公开级，以用于信息的获取和控制，在需要的保护等级内存储、共享、复制、传输、删除和销毁等。

应按照分类机制建立和实施一组合适的信息标记和处理程序，对分类信息进行标记和处理。

标记信息的程序应涵盖物理标记、电子标记或其他标记方式。待考虑的项目包括打印报告、屏幕显示、记录介质。

对每种信息分类级别，要定义包括安全处理、储存、传输、删除、销毁的处理程序，还要包括安全相关事件的监督和记录程序。

9.4.2 记录与存储

应对重要信息进行加密存储，设置访问控制功能。

9.4.3 备份与恢复

应采取适当的措施来保证长期记录能够恢复（如将数据转换为新格式或保留可读取原数据的旧设备）。

9.5 数据安全

9.5.1 范围

应对重要数据进行安全管理，考虑的范围包括但不限于：

生产数据：工艺参数、配置文件、设备运行数据、生产数据、控制指令等；

测试数据：包括安全评估数据、现场组态开发数据、系统联调数据、现场变更测试数据、应急演练数据等；

用户数据：用户个人信息、行为信息、位置信息等。

9.5.2 措施

应对静态存储的重要工业数据进行加密存储，设置访问控制功能，对动态传输的重要工业数据进行加密传输，使用 VPN 等方式进行隔离保护，并根据风险评估结果，建立和完善数据信息的分级分类管理制度。

应对关键数据进行保护，如签订保密协议、回收测试数据等。应对关键业务数据进行定期备份。

应建立数据资产管理台账，实施数据分类分级管理，加强个人信息与重要数据保护。

应建设数据安全保护技术措施，确保数据持续处于有效保护和合法利用的状态，依法依规落实数据安全风险评估、数据安全事件报告等要求。

在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当按照有关法律法规规定在境内存储。需要向境外提供数据的，应当通过数据出境安全评估。

10 审计与评估

10.1 信息安全过程审计

应定期对信息安全管理和技术措施运行、信息安全风险管理和人员安全能力等开展内部审计。

应定期审查信息和文件管理政策的符合性。

应定期对资产进行安全巡检，审计资产使用记录，并检查资产运行状态，及时发现风险。

涉及对运行系统核查的审计活动，应谨慎的加以规划并取得批准，以便最小化造成业务过程中断的风险。

对于审计工具的访问应加以保护，以防止任何可能的滥用或损害。

10.2 系统能力评估

评估过程要确保对管理控制系统的评估不干扰到系统设备的管控功能，在实施评估前，可能需要使系统离线。

可基于以下几个方面对系统能力进行评估：

a） 标识和认证：所有用户（人、软件进程和设备）在被允许访问系统之前，对他们进行标识和认证；

b） 使用控制：为已认证用户（人、软件进程和设备）分配特权以执行所请求的操作，并对这些特权的使用进行监视；

c） 系统完整性：确保系统的完整性，以防止未经授权的操作与篡改；

d） 数据保密性：确保通信信道和数据仓库的信息的保密性，防止未授权的泄露；

e） 限制的数据流：利用区域和管道对控制系统分区，来限制不必要的数据流；

f） 对事件的及时响应：当事故发生时，对安全事件进行响应，通知适当的权威、报告所需证据、采取及时的纠正行动；

g） 资源可用性：确保控制系统的可用性，防止拒绝基本服务。

能力等级可由低到高定义为：

a） 1 级：提供机制保护系统防范偶然的、轻度的攻击；

b） 2 级：提供机制保护系统防范有意的、利用较少资源和一般技术的简单手段可能达到较小破坏后果的攻击；

c） 3 级：提供机制保护系统防范恶意的、利用中等资源、特殊技术的复杂手段的可能达到较大破坏后果的攻击；

d） 4 级：提供机制保护系统防范恶意的、使用扩展资源、特殊技术的复杂手段与工具可能达到重大破坏后果的攻击。

参 考 文 献

[1] 《工业控制系统信息安全防护指南》

[2] GB/T 30976.1-2014 《工业控制系统信息安全 第一部分 评估规范》

[3] IEC62443-2-1:2010/GBT33007-2016建立工业自动化和控制系统安全程序