ICS 35.040
CCS L80

T/SXQCTB

团　　体　　标　　准

T/SXQCTB 001—2023

汽车制造工业控制系统信息安全技术规范

Technical specifications for information security of automobile manufacturing industrial control systems

2023－04－18 发布　　2023－05－19 实施

山西省汽车行业协会　　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。

本文件由山西省汽车行业协会提出、归口并宣贯。

本文件起草单位：山西吉利汽车部件有限公司、吉利汽车集团有限公司

本文件主要起草人：乔慧、武善君、刘玉东、汤耀文、胡庆邦、付建林、高震

汽车制造工业控制系统信息安全技术规范

1 范围

本文件规定了汽车制造业装备建设实施过程中涉及的工业控制系统信息安全防护技术要求和在装备安装调试验收阶段需要满足的信息安全验收要求。

本文件适用于汽车制造企业工业控制系统的新建及已建项目。

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。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。

GB/T 30976.1 信息安全技术 工业控制系统信息安全 第1部分：评估规范

GB/T 32919 信息安全技术 工业控制系统安全控制应用指南

GB/T 36324 信息安全技术 工业控制系统信息安全分级规范

GB/T 40813 信息安全技术 工业控制系统安全防护技术要求和测试评价方法

3 术语和定义、缩略语

下列术语和定义适用于本文件。

3.1 术语和定义

GB/T 32919、GB/T 40813 和 GB/T 30976.1 界定的以及下列术语和定义适用于本文件。

3.1.1

工业控制系统 Industrial Control System；ICS

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。

3.1.2

信息安全 security

a) 保护系统所采取的措施；

b) 由建立和维护保护系统的措施而产生的系统状态；

c) 能够免于非授权访问和非授权或意外的变更、破坏或者损失的系统资源的状态；

d) 基于计算机系统的能力，能够提供充分的把握使非授权人员和系统既无法修改软件及其数据，也无法访问系统功能，却保证授权人员和系统不被阻止；

e) 防止对工业自动化和控制系统的非法或有害的入侵，或者干扰其正确和计划的操作。

注：措施可以是与物理信息安全（控制物理访问计算机的资产）或者逻辑信息安全（登录给定系统和应用的能力）相关的控制手段。

3.1.3

控制设备 Control Equipment

工业生产过程中用于控制执行器以及采集传感器数据的装置。

注：包括 DCS 现场控制单元、PLC 以及 RTU 等进行生产过程控制的单元设备。

3.1.4

工业主机 Industrial Host

工业生产控制各业务环节涉及组态、工作流程和工艺管理、状态监控、运行数据采集以及重要信息存储等工作的设备。

注：包括工程师站、操作员站、服务器等。

3.1.5

工业控制资产 Industrial Control Asset

工业生产过程中具有价值的软硬件资源和数据。

注：包括控制设备、工业主机、网络设备、应用程序、工业数据等。

3.2 缩略语

ICS：工业控制系统（Industrial Control System）

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

SCADA：监控和数据采集系统（Supervisory Control and Data Acquisition）

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

RTU：远程终端单元（Remote Terminal Unit）

HTTP：超文本传输协议（Hypertext Transfer Protocol）

FTP：文本传输协议（File Transfer Protocol）

VLAN：虚拟局域网（Virtual Local Area Network）

VPN：虚拟专用网络（Virtual Private Network）

4 工业控制系统

4.1 基本构成

按照 GB/T 36324 中根据工业控制系统（ICS）的功能特点和部署形式，企业的与工业控制系统（ICS）相关系统纵向划分为 5 个层级，如：第 1 层物理过程、生产装置，第 2 层安全和保护系统、基本控制系统，第 3 层监控系统，第 4 层运营管理系统，第 5 层业务规划和物流系统。其中第 1 层～第 3 层的相关系统、设备，可作为构成工业控制系统的范围。

4.2 安全防护的对象

本文件涉及的防护对象为系统层级中第 1 层（物理过程、生产装置）、第 2 层（安全和保护系统、

基本控制系统）和第 3 层（监控系统）的工业控制资产。

4.3 安全防护措施的约束条件

按照 GB/T 40813 的安全防护技术要求，不应对 ICS 的功能安全产生不利影响；不能锁定用于基本功能的账户；不应因实施安全措施而显著增加延迟并影响系统的响应时间；不能因安全措施失效导致系统的基本功能中断等。

在符合本文件提出的技术要求时，经评估对可用性有较大影响而无法实施的，可调整要求并研究制定相应的补偿防护措施，但采取补偿防护措施后不应降低原有要求的整体安全防护强度。

5 安全防护的技术要求

按照 GB/T 32919与工业和信息化部印发的《工业控制系统信息安全防护指南》，做好工业控制系统（ICS）信息安全防护工作。

5.1 安全软件选择与管理

a）应在工业主机上安装防病毒软件或应用程序白名单软件，确保有效防护病毒、木马等恶意软件及未授权应用程序和服务的运行。

b）在安装防病毒软件或应用程序白名单等安全软件之前，应在非生产环境中进行充分验证测试或已有验证案例。误杀的应用程序或文件可列入白名单配置，白名单配置清单需记录和上报给使用方，确保防病毒软件不会对 ICS 的正常运行造成影响。

5.2 配置和补丁管理

a）ICS 具备时钟配置能力的网络设备、工业主机和控制设备需配置好时钟同步功能，与 IT 时钟服务器保持同步。

b）具有安全配置的工业主机、服务器、交换机和防火墙等设备需做好配置备份，建立配置清单，清单需与实际配置一致。

c）发生重大配置变更时，需制定配置变更计划，进行影响分析，确保该重大配置变更不会引入重大安全风险。

d）同设备类型网络设备，工业主机和控制设备的固件版本或操作系统版本需保持一致。

e）可提前对操作系统进行补丁修复和杀毒软件安装加固后，再进行工业软件安装调试，避免后期安装补丁和杀毒软件带来兼容性问题。

5.3 边界安全防护

a）禁止没有防护的工业控制网络与互联网连接，以确保互联网的安全风险不被引入工业控制网络。

b）禁止调试笔记本与工业控制网络同时连接互联网，以确保互联网的安全风险不被引入工业控制网络。

c）ICS 之间需做子网隔离、物理隔离或 VLAN 逻辑隔离。ICS 的子网划分和 VLAN 逻辑隔离需符合

GB/T 36324 安全等级划分要求。

5.4 物理和环境安全防护

a）重要工程师站、数据库、服务器等核心工业控制硬件所在区域采取物理安全防护措施。

b）应拆除或封闭工业主机上不必要的 USB、光驱等接口，以防止病毒、木马、蠕虫等恶意代码入侵，并避免数据泄露。

c）在确需使用工业主机外设接口时，企业应建立主机外设接口管理制度，并通过主机外设安全管理技术手段实施访问控制，以避免未授权的外设终端接入。

5.5 身份验证

a）在工业主机登录、应用服务资源访问、工业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，如口令密码、 USB-key、智能卡、生物指纹、虹膜等。

b）合理分类设置账户权限，以满足工作要求的最小特权原则来进行系统账户权限分配。

c）强化工业控制设备、SCADA 软件、工业通信设备等的登录账户及密码，避免使用默认口令或弱口令，定期更新口令。

5.6 远程访问安全

a）严格禁止 ICS 面向互联网开通 HTTP、FTP、Telnet 等高风险通用网络服务。

b）确需远程访问的，应在 ICS 与其他信息系统之间设置访问控制规则，部署访问控制设备，默认情况下受控接口仅允许交换符合安全策略的指定格式的数据。

c）确需远程维护的，应采用 VPN 等远程接入方式进行。

d）严禁在工业主机上安装无线热点连接互联网进行远程访问。

5.7 安全监测和应急演练

a）在工业控制网络部署网络安全检测设备，及时发现、报告并处理网络攻击或异常行为。

b）制定工控安全事件应急响应预案，内容至少应包括：目的、范围、角色、责任、管理层承诺、相关部门的协调、合规性。

c）适用时，当 ICS 因信息安全威胁出现异常或故障时，应按应急响应预案做好应急响应工作，采取紧急防护措施，防止事态扩大，并逐级报送直至属地省级工业和信息化主管部门，同时注意保护现场，以便进行调查取证。

d）定期对 ICS 的应急响应预案进行演练，必要时对应急响应预案进行修订。

5.8 资产安全

a）建立 ICS 资产清单，明确资产责任人，以及资产使用及处置规则。

b）对关键主机设备、网络设备、控制组件等进行冗余配置。

5.9 数据安全

a）应对静态存储和动态传输过程中的重要工业数据进行保护，根据风险评价结果对数据信息进行

分级分类管理。

b）应建立关键业务数据清单，如订单数据，历史数据，质量数据，操作日志和故障日志等。对关键业务数据进行定期备份并定期进行数据恢复测试，确保备份数据的可用性。

c）应对测试数据进行保护。

5.10 供应链安全

a）选择 ICS 规划、设计、建设、运维或评价等服务商，宜优先考虑具备工控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。

b）与访问、处理、存储、传递组织信息或为组织信息提供 ICS 基础设施组件的供应商，建立所有相关的信息安全要求，并达成一致。

c）供应商协议应包括信息与通信技术服务以及产品供应链相关的信息安全风险处理要求。

5.11 责任落实

a）应建立工控安全管理机制、成立信息安全协调小组等，明确工控安全管理责任人，落实工控安全责任制，部署工控安全防护措施。

b）组织所有员工和相关的合同方，应按其工作职能，接受教育和培训，明确组织策略及规程的定期更新的信息。

c）应有正式的、且已被传达的违规过程以对信息安全违规的员工采取措施。

6. 安全防护的验收

6.1 安全软件选择与管理验收

a）查阅工业主机上安装防病毒软件或应用程序白名单软件的证明材料，采购合同、服务协议等，评估其来源是否安全正规。

b）核查其工业主机防病毒软件或应用程序白名单软件是否已安装运行、病毒库或白名单规则是否及时升级，原则上 3 个月内。若未及时升级，查阅不适合升级病毒库的分析报告。

c）查阅防病毒软件或应用程序白名单软件已在离线或测试环境中充分测试验证的技术报告，评估其是否影响 ICS 正常运行。

6.2 配置和补丁管理验收

a）ICS内的网络设备，交换机、防火墙等；工业主机，工程师站、操作员站、工控机、服务器、存储设备等；控制设备，PLC、机器人等已配置好时间同步功能。

b）核查企业工业控制网络安全配置，网络分区、端口禁用等；工业主机安全配置，远程控制管理、默认账户管理等；工业控制设备安全配置，口令策略合规性等是否落实，评估其安全配置是否存在安全风险隐患。

c）查阅ICS安全配置清单。

d）核查企业工控安全漏洞补丁升级记录，评估企业ICS是否已安装最新版补丁程序。

6.3 边界安全防护验收

a）人工核查或工具检测的方式，检查企业为ICS开发、测试和生产环境是否分离，网络是否相连、生产环境是否存在测试账户/数据等。

b）人工核查或工具检测的方式，检查工业控制网络是否在无防护状态下直接连接互联网。

c）查阅企业工业控制网络安全防护设备部署实施相关证明材料，网络拓扑结构图、网络安全防护设备采购合同、安全防护设备配置策略等，评估其是否依据工业控制网络安全区域实施逻辑隔离安全防护以满足企业网络边界防护需求。

6.4 物理和环境安全防护验收

a）人工核查等方式，现场核查企业是否针对重要资产区域采用适当物理安全防护措施。

b）人工核查企业是否拆除或封闭工业主机上不必要的 USB、光驱、无线等接口。

c）查阅企业主机外设接口管理制度，在适用时，人工核查或工具检测等方式验证企业主机外设安全管理技术手段实施情况，以技术手段评估企业是否落实管理技术手段。

6.5 身份验证验收

a）人工核查等方式，在关键设备、系统和平台，审核是否采用多因素认证方式，评估身份认证方式是否满足安全强度要求。

b）查阅企业系统账户权限分配规则，评估其是否按照最小特权原则进行权限分配。

c）人工核验、工具检测等方式，核查企业的工业控制设备、SCADA软件、工业通信设备等登录账户及密码设定情况，账户密码管理制度，评估其强度及管理制度是否满足需求。

6.6 远程访问安全验收

a）人工核查或工具检测等方式，检查企业是否采用数据单向访问控制等策略对远程访问进行安全加固，评估其安全加固措施是否满足企业安全和业务需要。

b）人工核查或工具检测等方式，验证ICS是否面向互联网开通 HTTP、FTP、Telnet等高风险通用网络服务。

c）人工核查或工具检测等方式，检查工业主机上是否已禁止使用无线热点进行联网服务。

6.7 安全监测和应急演练预案验收

a）人员核查、文档查阅等方式，核查企业是否在工业控制网络部署了网络安全监测设备。 评估该监测设备是否可及时发现、报告网络攻击或异常行为。

b）人员访谈、查阅企业工控安全事件应急响应预案相关文件，评估其科学性、合理性。

c）查阅企业是否明确具有保护现场和调查取证相关流程和要求，ICS信息安全威胁事件报送机制相关流程及要求，适用时，查阅相关执行记录。

d）人员访谈、查阅企业应急响应预案演练相关记录文档，评估是否定期组织相关人员开展应急响应预案演练及演练是否覆盖应急预案的全部内容。

6.8 资产安全验收

a）查阅企业ICS资产清单相关文档材料，评估资产信息是否完整和准确，资产责任人是否明确，处置规则是否得到有效执行。

b）人工核验等方式，核查企业是否针对关键主机设备、网络设备、控制组件等实行了冗余配置。

6.9 数据安全验收

a）人工核查或工具检测等方式，核查企业是否针对静态存储重要工业数据进行加密存储、访问控制等防护，评估其能否满足企业静态存储数据的安全防护要求。

b）查阅企业数据管理相关文档材料，评估其是否建立并严格实施数据分级分类管理制度。

c）查阅企业是否建立关键业务数据清单，订单数据、历史数据、质量数据、操作日志和故障日志等。检查企业关键业务备份数据、数据备份日志文件、恢复测试记录文档，核查备份方式、备份周期、恢复测试等策略是否满足企业数据备份的需求。

d）人工核查或工具检测等方式，对企业测试过程中产生的数据保护进行审核，评估测试数据是否存在被未授权获取及使用的风险。

6.10 供应链安全验收

a）查阅企业与ICS服务商签署的合同等资料，评估其是否以明文条款的方式约定服务商在服务过程中应当承担的信息安全责任和义务。

b）查阅ICS服务商已向企业提供的相关证明材料，工控安全合同、工控安全防护案例、验收报告等，评估服务商是否具有工控安全防护经验且专业可靠。

c）查阅企业与服务商签订的保密证明材料，保密协议等。审核协议中是否约定保密内容、保密时限、违约责任等内容，评估是否存在ICS敏感信息外泄的风险。

6.11 责任落实验收

a）查阅企业ICS安全管理机制等文档，检查人员工控安全培训制度、应急响应与演练制度、风险评估制度等，评估其指导ICS安全管理工作的有效性。

b）查阅信息安全协调小组成立相关文档材料，评估小组成员构成的合理性。同时通过人员访谈，评估小组成员对自身职责的熟悉程度。

c）访谈工控安全管理责任人，评估工控安全责任制和安全防护措施的落实情况。

附录 A.

（资料性附录）

工控信息安全验收检查表

验收项目	实施细则	是	否	无关
安全软件选择与管理	1.工业主机（工程师站、操作员站、工控机、服务器、存储设备等）已安装了防病毒软件，并登记在《工业控制系统资产清单》			
	2.防病毒软件来源是指定或厂家设备自带并得到认可的			
	3.同一工业主机上不存在同时安装两种以上同类型防病毒软件			
	4.工业主机安装的防病毒软件的白名单策略已登记在《工业控制系统资产清单》			
	5.工业主机安装的防病毒软件的病毒库为最新版本			
配置和补丁管理	1.工业控制系统内的网络设备（交换机，防火墙等），工业主机（工程师站、操作员站、工控机、服务器、存储设备等）和控制设备（PLC，机器人等）已配置好时间同步功能			
	2.具有安全配置的网络设备、工业主机和控制设备等已提交配置备份文件			
	3.网络设备（交换机，防火墙等），工业主机（工程师站、操作员站、工控机、服务器、存储设备等）和控制设备（PLC，机器人等）等设备的安全策略清单已提交			
	4.同类型的网络设备、工业主机和控制设备的固件版本或操作系统版本已保持一致			
	5.Windows 系统工业主机，指定的系统安全补丁已进行修复，例如：防勒索病毒补丁和远程协议漏洞补丁等			
边界安全防护	1.无防护的工业控制网络已禁止与互联网连接。			
	2.工业控制系统已按照要求完成子网隔离、物理隔离或 VLAN 逻辑隔			
物理和环境安全防护	1.重要的工程师站，服务器和网络设备已做好物理防护			
	2.工业主机上不必要的 USB、光驱已拆除或封闭			
	3.确需使用的外设接口已进行外设（USB 和光驱等）访问控制			
身份验证	1.工业主机、工业软件、网络设备和控制设备的登录密码已设置			
	2.账户权限已以满足工作要求的最小特权原则进行系统账户权限合理分配			
	3.工业主机的账户口令已进行强化，口令字长应不少于 8 个字符并由字母数字混合组成			
远程访问安全	1.工业控制系统已关闭了面向互联网的 http、FTP、Telnet 等高风险通用网络服务			
	2.工业主机上已禁止使用无线热点进行联网服务			
	3.供方申请开通的 VPN 远程账户已关闭			
	4.设备安装调试验收后，继续使用的 VPN 远程账号已经过业务部门允许			
安全监测和应急演练	1.供方提供的安全监测软件已完成使用培训			
	2.供方提供的冗余方案已完成现场演练			
资产安全	1.《工业控制系统资产清单》已提交，包含工业主机，网络设备和控制设备等。			
	2.采购范围内的工业软件为正版软件			
	3.工控系统的网络拓扑图已提供			
	4.工业控制系统的 IP 地址分配清单已提供			
数据安全	1.工控资产（包括控制设备、工业主机、网络设备、工业数据、应用程序等）的数据备份已提交			
	2.工控资产已做好数据还原验证（抽检）			
	3.重要的工业数据清单已按照模板提供			
	4.数据备份文件已存放在指定路径			

供应链安全	1.按照相关管理办法，供方已签订保密协议			
	2.按照相关管理办法，供方已经过需求方的工控信息安全培训			
	3.按照相关管理办法，供方已提交《供应商出入场信息安全检查表》，保证入场人员经过工控信息安全培训，携带的调试电脑、U盘和移动硬盘等调试相关设备安全可用			
责任落实	1.供方已提供工控信息安全的运维培训			
特例情况说明	对于因特殊原因而无法实现的验收条款，已向需求方相关部门进行过特例报备，并得到确认。对于所涉及的特例设备，已将相关信息登记到《工控信息安全特例记录表》			