山西省汽车行业协会文件

晋汽协〔2023〕2号

山西省汽车行业协会关于《汽车制造工业控制系统信息安全技术规范》团体标准征求意见的通知

各相关单位：

团体标准《汽车制造工业控制系统信息安全技术规范》征求意见稿已完成，为保证该团体标准的科学性、实用性及可操作性，按照《团体标准管理规定》及《山西省汽车行业协会团体管理办法》相关规定，现面向社会公开征求意见。

请各有关单位及专家将修改意见和建议填写在《征求意见表》中，并于2023年4月15日前回复至起草工作组。

感谢您对山西省汽车行业协会标准化工作的支持。

附件1:《汽车制造工业控制系统信息安全技术规范》编制说明；

附件2:《汽车制造工业控制系统信息安全技术规范》(征

求意见稿）

附件3：《征求意见表》

联系人：王晓　　邮箱：sxqcxh2021@126.com

电话：0351-4183204　13209822516

山西省汽车行业协会

2023年3月15日

主题词： 标准 征求意见 通知

山西省汽车行业协会　　2023年3月15日印发

《汽车制造工业控制系统信息安全技术规范》

编制说明

《汽车制造工业控制系统信息安全技术规范》

标准编制组

2023 年 3 月

目　　录

1. 研究背景

近年，全球工业控制系统信息安全风险加剧，我国工业控制系统更是受灾区。卡巴斯基实验室报告显示，2016 年 7 月至 2017 年 6 月期间我国工控系统受损占比 57.1%，排在全球第五位。为加快我国工业控制系统信息安全保障体系建设，提升工业企业工业控制系统信息安全防护能力，促进工业信息安全产业发展,2017 年 12 月 12 日工业和信息化部印发《工业控制系统信息安全行动计划（2018-2020 年）》（工信部信软[2017]316 号），提出“建立健全标准体系”。

近年全球工控信息安全形式越发严峻，以色列、乌克兰等一些国家关键信息基础设施遭受严重的网络攻击。2016 年 1 月，以色列电力供应系统遭受有史以来最大的网络攻击。2016 年 2 月,乌克兰矿业和铁路系统遭受 BlackEnergy 攻击，对国家造成严重破坏。2017 年 10 月，瑞典交通署信息系统遭黑客攻击，导致列车延误，并伴随道路和桥梁在内的瑞典关键基础设施数据的泄露。从这些攻击事件中可以看出，网络攻击从虚拟世界转向现实世界，关键性基础设施已成为安全威胁的指向目标，常掺杂着政治色彩，严重影响国家和社会的安全。

随着工控信息安全风险的升级，工控信息安全事件的后果严重。2009 年，国际上发生的震网事件，美国和以色列通过震网(Stuxnet)病毒秘密攻击伊朗布什尔核电站,Stuxnet 渗透至伊朗核电站的计算机系统并破坏了伊朗铀浓缩离心机，造成五分之一的离心机报废。2017 年 12 月，某国家支持的黑客入侵沙特阿拉伯能源工厂安全系统，造成工厂停止运行。由此可见，工控系统一旦遭受攻击，受破坏程度巨大，

可导致工控系统瘫痪、设备报废、工厂停工。

工控信息安全事件波及范围广，涉及世界多个国家的多个领域。近年发生的工控信息安全事件影响范围不仅仅是某个国家或地区，也不仅仅是某个领域，它已波及全球，影响多领域多行业，工控信息安全威胁愈演愈烈。

工信部针对国内大型工业企业的核心管控系统开展检查，发现企业工业应用系统普遍存在安全漏洞，缺乏有效的安全配置策略，外网边界容易被突破。内网边界防护薄弱，工控设备普遍开启远程访问进行维护，工控主机安全防护措施较弱，控制权极易被远程获取；对工业控制系统的信息安全管理相对薄弱，严重滞后于工业互联网的发展。

汽车制造企业近年发生多次工控安全事件，导致生产业务中断，工控安全检查过程中发现工控的防病毒、补丁、备份等基本的管理要求均未全面覆盖，且在事件上报、应急响应等方面均无法及时有效开展，需统一去考虑整体的解决方案，形成覆盖全行业的制度标准。

2. 国内外工控安全发展情况

近年来，工业控制系统信息安全的标准制定一直受到国内外专家的高度重视。国际上针对工业控制系统信息安全标准进行研究的组织很多，其中包括许多国际标准化组织，如美国国家标准技术研究院（NIST）、国际电工委员会（IEC），国际自动化协会（ISA）和电气与电子工程师协会(IEEE)等等。

国际电工委员会（IEC）、电气与电子工程师协会(IEEE)和国际自动化协会（ISA）致力于工控信息安全国际标准建设。工控信息安全国际标准主要集中在电力系统信息安全领

域：IEC 于 2002 年发布了《电力系统控制和相关通信：数据和通信安全（IEC62210）》，并于 2005 年发布《电力系统管理及信息交换：数据和通信安全性（IEC62351）》；IEEE 于 2007 年发布《变电站 IED 网路安全功能标准（IEEE1686-2007）》，并于 2011 年发布《变电站串行链路网络安全的机密协议试行标准（IEEE P1711）》。

美国国家标准技术研究院(NIST)、美国国土安全部(DHS)等机构致力于美国工控信息安全标准的建设。美国标准主要在三个领域：一是美国工控信息安全标准集中在石油天然气领域；二是美国针对电力、核电领域工控系统信息安全出台相应的标准；三是美国发布了一系列通用工控信息安全标准。

欧盟各国注重发展通用性的工控信息安全标准。此外，欧盟国家根据各自国情关注特定领域的工控信息安全标准建设，例如德国关注制造业的信息安全问题。

欧美国家在研究工控信息安全标准时注重借鉴和融合，例如，国际标准化组织 IEC 和 ISA 联合发布的 IEC 62443 标准，在研制过程中充分借鉴了荷兰 WIB 指定的《过程控制域（PCD）--供应商安全需求》，而美国 NIST 在研制《改善监管基础设施网络安全框架》时融合了国际标准化组织发布的 IEC 62443 标准中一些的技术要求。

我国工控信息安全标准起步较晚，工控信息安全标准体系尚未形成。建立健全我国工控信息安全标准体系，研制技术、产品、系统、设施等新标准，完善和修订已有标准，学习欧美借鉴、融合他国工控信息安全标准的经验，必要时实现部分工控信息安全标准的本土化。

我国已形成了一些通用的工控信息安全标准，并在一些

重要领域建立了工控信息安全标准，其中我国电力领域起步较早。目前，我国工控信息安全标准已覆盖电力、轨道交通、石油化工、机械、烟草等领域。然而，随着我国工控系统信息安全形势日益严峻，亟需在国家关键信息基础设施领域制定强制性工控信息安全国家标准，视情在行业特殊需求的领域制定推荐性工控信息安全行业标准，使得重点领域的工控信息安全工作做到有章可循。

总的来说，目前在信息安全领域人们所关注的焦点主要有以下几方面：

1）密码理论与技术；

2）安全协议理论与技术；

3）安全体系结构理论与技术；

4）信息对抗理论与技术；

5）网络安全与安全产品。

3. 已有标准检索情况

目前没有工业控制系统汽车制造过程安全技术规范的国家标准、行业标准和地方标准，与《汽车制造工业控制系统信息安全技术规范》相关的已经发布的国家标准有4项，分别是《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》。

4. 标准主要编制过程

随着工业信息化的迅猛发展，德国的“工业 4.0”、美国

的“再工业化”风潮、“中国制造2025”等国家战略的推出，以及云计算、大数据、人工智能、物联网等新一代信息技术与制造技术的加速融合，工业控制系统由从原始的封闭独立走向开放、由单机走向互联、由自动化走向智能化。但在工业企业获得巨大发展动能的环境背景下，也滋生了大量安全隐患，工控安全正面临严峻的挑战。

基于此背景之下，2019年10月，由浙江吉利汽车ME中心提出制定《工控安全技术要求》的企业标准，用于指导吉利汽车制造基地整车制造过程所有车间工业控制系统建设实施过程涉及的信息安全防护技术指标和具体要求，在装备安装调试验收阶段需要满足的信息安全验收要求。

吉利汽车ME中心联合吉利信息化中心、吉利整车制造基地、整车制造线提供商组建标准联合编制小组。标准编制小组迅速响应，查阅了国内外工业控制系统信息安全相关的标准材料，包括国内外有关工业控制系统信息安全方面的技术标准，现有相关法律法规和标准等，作为制定此次标准的依据，确保标准符合国家相关法律法规和管理规定的要求。此外，标准编制小组还系统收集了现有工厂工业控制系统的实际使用情况和安全方案，积累了大量的一手资料，力求技术完整全面便于实施。

在掌握了丰富翔实的资料后，标准编制小组着手编写标准的草案。草案经吉利内部进行了标准框架和技术内容的多次讨论，在充分消化吸收资料的基础上于2020年3月形成了本标准的初版文件。2020年4月之后在多个吉利汽车制造基地试点运行两年，过程中与制造基地、整车制造线提供商进行了多次讨论，针对实施过程中遇到的各项问题，各方提

供了意见和建议，各小组成员经过评估，完成修改，并在2022年3月形成了标准的修订版本。

2022年3月，浙江吉利汽车ME中心决定将《工控安全技术要求》的企业标准文件升级为团体标准文件。在保持原有标准编制小组成员结构的基础上，后续加入山西省汽车协会，行业制造企业等相关组员。2022年4月-6月，由浙江吉利汽车ME中心组织相关单位的标准修订小组成员和协会专家，以网络会议的形式对标准文件进行了多轮讨论，会议对标准文件进行了逐条讨论，并提出了初步修改意见。ME中心根据修改意见做了修订。

2022年6月，分别与山西省汽车协会，行业制造企业，制造基地等单位的相关专家在太原市召开会议深入讨论，相关专家对该标准提出了大量宝贵意见和建议，对标准的格式和内容进行了改进并进一步完善了标准框架、技术内容，形成了团体标准《工业控制系统汽车制造过程安全技术规范》。

2023年2月，与山西省汽车协会及邀请的5位行业专家在山西省晋中市召开会议讨论，在会上，各位专家对标准的结构及各项条款进一步进行了补充要求，并形成了报批文件《汽车制造工业控制系统信息安全技术规范》。

5. 标准的编制原则

在标准的编制过程中严格遵循国家有关方针、政策、法规和规章，标准的编写规则及表述遵循科学、合理、可行的原则，力求做到规范、统一。首先，在标准制定过程中，遵循政策和协调统一性原则。严格遵循国家有关方针、政策、法规和规章，严格执行强制性国家标准和行业标准，与同体系标准及相关的各种基础标准相衔接。其次，主要技术指标

的确定是以现有技术实施中基本原则与运行效果参数、运行维护等为目标，确保因地制宜、节约高效等技术目标。再次，广泛征求管理单位、建设单位、施工单位和设计单位专家意见，并与技术、设计和建设等方面的专家进行深入交流和研讨，进行适当的修改和规范，使标准既保持技术上的科学性和先进性，又具有实施上的适用性和可操作性。同时结合汽车行业的应用特点进行补充，形成与国标相辅相成并确实对汽车制造行业有落地指导作用的规范性文件。

1）技术标准内容收集资料

2016 年 10 月，《工业控制系统信息安全防护指南》指出要做好工控安全防护工作。

2017 年 6 月 1 日，《中华人民共和国网络安全法》正式实施，提出重点保护关键信息基础设施。

2019 年 5 月 13 日，等保 2.0《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》正式发布，将工业控制系统、云计算、物联网和大数据等安全纳入到等级保护中。对标合资整车厂在 2015 年开始已逐步将工控安全技术引用到工业控制系统中去。国有背景的整车厂在 2019 年已经开始在做等保 2.0 满足国家法律法规要求。

2）与现行有效文件的协调性情况（包括但不限于国家标准、行业标准、企业标准、企业质量体系文件）

从汽车制造工控建设前期规划的角度和后期改造提升项目，提炼出针对汽车制造工业控制系统需要遵守的总体技术要求。力求从汽车制造过程中的工业装备建设实施过程涉及的信息安全防护技术指标和具体要求，在装备安装调试验收阶段需要满足的信息安全验收要求。

本标准依据GB/T 1.1-2020《标准化工作导则 第1部分：标准的结构和编写规则》规定的要求进行编写。

6. 与现行国家标准的关系

本文件是在执行国家标准的基础上，针对行业特点，规范了汽车制造工业装备建设实施过程中涉及的信息安全技术规范，对各项内容进行细化及推荐性指导，作为国家标准的补充规定。

7. 工控安全的定义

工控，指的是工业自动化控制，主要利用电子电气、机械、软件组合实现。即是工业控制系统，或者是工厂自动化控制。工控安全指的是工业控制系统的数据、网络和系统安全。工业信息安全是工业互联网健康有序发展的重要基石和防护中心，是工业安全和互联网安全的深度结合。广义的工业互联网安全涉及设备、控制、网络、平台、工业APP、数据等多方面网络安全问题，其核心任务就是要通过监测预警、应急响应、检测评估、功能测试等手段确保工业互联网健康有序发展。

工业控制系统安全是工业互联网安全的核心，一方面工业控制系统广泛适用于在工业生产过程的控制，是工业生产的核心大脑；另一方面，目前80%以上的国家关键基础设施以及智慧城市业务系统都是依赖于工业控制系统进行控制。

8. 标准的主要内容

本标准针对汽车行业制造业的工业控制系统防护特点，从11个方面对工业控制系统信息安全的基本管理提出了规范性指导措施，以满足汽车行业对其工业控制系统的安全管理需求，为实现汽车行业制造的工业控制系统适度、有效的

安全管理控制提供参考。

标准主要从以下几个方面阐述：

1）本标准范围规定了汽车制造过程中的工业装备建设实施过程涉及的信息安全防护技术指标和具体要求，在装备安装调试验收阶段需要满足的信息安全验收要求。

2）引用现行国家标准文件5项，保证了国家和行业标准的一致性。

3）对标准中需要用到的且容易产生歧义或意义不明确的短语，结合引用标准中已有的相近的定义，参考国内外相关文献，按照本标准需要给出了“工业控制系统”、“控制设备”、“信息安全”、“控制设备”、“工业主机”等术语的定义。

4）规定了汽车制造过程工业控制系统安全防护技术要求和汽车制造过程工业控制系统安全防护验收要求，为工业控制系统汽车制造过程的安全提供规范的指导。

9. 与有关的现行法律、法规和强制性国家标准的关系

本标准制定过程中，标准起草单位收集了国内相关技术资料、标准和法律法规，严格贯彻国家有关方针、政策、法规和规章，严格执行国家和行业标准，各项技术内容不违背我国目前颁布的相关法律、法规和标准，政策性和协调性较强。本标准是以现有汽车制造工业控制系统信息安全需求为目标导向，基于生产过程中大量积累的数据和经验编制，具有较强的科学性、适用性。与我国国情相适应，与国际要求基本接轨，本标准的制定严格按照 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，技术内容编写。

10. 贯彻标准的要求和措施建议

建议在本标准发布后，在山西省汽车行业进行宣贯，鼓励企业使用本标准。本标准适用汽车制造企业工业控制系统的新建及已建项目。

11. 标准属性

《汽车制造工业控制系统信息安全技术规范》属于推荐性标准。

《汽车制造工业控制系统信息安全技术规范》

标准编制组

2023 年 3 月

ICS 35.040
CCS L80

T/SXQCTB

团　　体　　标　　准

T/SXQCTB XXXX—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

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

2023－XX－XX 发布　　2023－XX－XX 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》			

《汽车制造工业控制系统信息安全技术规范》
团体标准征求意见表

提出意见单位/专家：　　联系人：　　电话：

序号	章、条编号	原稿内容	修改意见	修改理由