库七七 www.kqqw.com 提供下载

ICS 65.060.01;35.240.99
B 90

中华人民共和国国家标准

GB/T 38874.4—2020/ISO 25119-4:2018

农林拖拉机和机械 控制系统安全相关部件 第4部分:生产、运行、修改与支持规程

Tractors and machinery for agriculture and forestry—Safety-related parts of control systems—Part 4:Production, operation, modification and supporting processes

(ISO 25119-4:2018,IDT)

2020-06-02 发布　　2020-12-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

库七七 www.kqqw.com 提供下载

前　言

GB/T 38874《农林拖拉机和机械　控制系统安全相关部件》分为以下4个部分：

——第1部分：设计与开发通则；

——第2部分：概念阶段；

——第3部分：软硬件系列开发；

——第4部分：生产、运行、修改与支持规程。

本部分为GB/T 38874的第4部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分使用翻译法等同采用ISO 25119-4:2018《农林拖拉机和机械　控制系统安全相关部件　第4部分：生产、运行、修改与支持规程》。

本部分由中国机械工业联合会提出。

本部分由全国农业机械标准化技术委员会(SAC/TC 201)归口。

本部分起草单位：中联重机股份有限公司、安徽泗州拖拉机制造有限公司、上海联适导航技术有限公司、中国农业机械化科学研究院、广州市智慧农林科技有限公司、河南科技大学、洛阳西苑车辆与动力检验所有限公司。

本部分主要起草人：苑严伟、王丽丽、高一平、王丹、张俊宁、朱如龙、李由、李玉光、吕程序、赵庆亮、董云雷、冀保峰、高宏峰、陈嵩。

库七七 www.kqqw.com 提供下载

农林拖拉机和机械 控制系统安全相关部件 第4部分:生产、运行、修改与支持规程

1 范围

GB/T 38874的本部分规定了控制系统安全相关部件(SRP/CS)设计与开发通则。本部分适用于农林拖拉机、农用自走式机械、农用全挂及半挂机械、农用牵引机械,也适用于市政机械(例如:道路清扫机)。

本部分不适用于:

——农用飞机和农用飞行器;

——草坪和园艺设备。

本部分规定了SRP/CS执行安全相关功能所要求的特性及类别,本部分未规定用于特定场合的性能等级。

注1:机械特定C类标准可为其范围内的机械安全相关功能指定农业性能等级(AgPL)。否则,AgPL的规范由制造商负责。

本部分适用于与机电系统有关的电气/电子/可编程电子系统(E/E/PES)的安全部件。本部分涵盖了E/E/PES安全相关系统(包括这些系统间的交互)的故障行为可能造成的危险。本部分不涉及触电、火灾、烟雾、高温、辐射、毒性、易燃、化学反应性、腐蚀、能量释放等相关危险,除非直接由E/E/PES安全系统故障引起。本部分还涵盖了在非E/E/PES危险下E/E/PES安全相关系统的故障行为,涉及防护措施、保障措施或安全相关功能。

本部分包含以下范围内的示例:

——SRP/CS限制电动混合动力系统中的电流,以防止绝缘失效/电击危险;

——SRP/CS的电磁干扰;

——SRP/CS的防火设计。

本部分不包含以下范围内的示例:

——摩擦导致电击危险产生的绝缘失效;

——影响附近机器控制系统的电磁辐射;

——腐蚀导致的电缆过热。

本部分不适用于非电气/电子/可编程电子系统(E/E/PES)(例如:液压、机械或气动)。

注2:参见ISO 12100中机械安全的设计通则。

本部分不适用于实施日期之前制造的控制系统安全相关部件。

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。

GB/T 38874.1—2020 农林拖拉机和机械 控制系统安全相关部件 第1部分:设计与开发通则(ISO 25119-1:2018,IDT)

GB/T 38874.2—2020 农林拖拉机和机械 控制系统安全相关部件 第2部分:概念阶段(ISO 25119-2:2018,IDT)

库七七 www.kqqw.com 提供下载

GB/T 38874.3—2020 农林拖拉机和机械 控制系统安全相关部件 第3部分:软硬件系列开发(ISO 25119-3:2018,IDT)

ISO 3600 农林拖拉机和机械、草坪和园艺动力机械 使用说明书编写规则(Tractors, machinery for agriculture and forestry, powered lawn and garden equipment—Operator's manuals—Content and format)

3 术语和定义

GB/T 38874.1 界定的术语和定义适用于本文件。

ISO 和 IEC 标准术语数据库的地址为:

——ISO 在线浏览平台:https://www.iso.org/obp

——IEC 电子百科:http://www.electropedia.org/

4 缩略语

下列缩略语适用于本文件。

AgPL:农业性能等级(agricultural performance level)

$AgPL_r$:农业性能等级要求(required agricultural performance level)

CAD:计算机辅助设计(computer-aided design)

Cat:硬件类别(hardware category)

CCF:共因失效(common-cause failure)

DC:诊断覆盖率(diagnostic coverage)

DC_{avg}:平均诊断覆盖率(average diagnostic coverage)

ECU:电子控制单元(electronic control unit)

ETA:事件树分析(event tree analysis)

E/E/PES:电气/电子/可编程电子系统(electrical/electronic/programmable electronic systems)

EMC:电磁兼容(electromagnetic compatibility)

FMEA:失效模式及影响分析(failure mode and effects analysis)

FSM:功能安全管理(functional safety management)

FTA:故障树分析(fault tree analysis)

HARA:危险分析及风险评估(hazard analysis and risk assessment)

HIL:硬件在环(hardware in the loop)

MTTF:平均失效前时间(mean time to failure)

$MTTF_D$:平均危险失效前时间(mean time to dangerous failure)

PES:可编程电子系统(programmable electronic system)

QM:质量度量(quality measures)

RAM:随机存取存储器(random-access memory)

SOP:开始生产(start of production)

SRL:软件需求等级(software requirement level)

SRP/CS:控制系统安全相关部件(safety-related parts of control systems)

UoO:观察单元(unit of observation)

库七七 www.kqqw.com 提供下载

5 质量管理体系

质量管理体系是功能安全的重要组成部分。本部分用户应通过以下方式证实符合第7章、第8章、第9章和第11章：

——以第7章、第8章、第9章和第11章作为指南，执行质量管理准则(例如：ISO 9001中的质量管理准则)。

——执行本部分中第7章、第8章、第9章和第11章中特定条款。

6 安全确认与验证

6.1 目的

第一个目的是证实每个功能安全需求已充分得到满足，并适合UoO的安全目标。

第二个目的是证实每个安全目标已按照最初设想和规定得到实现，并适合UoO的功能安全。

6.2 概述

验证和确认阶段(例如：审查、安全分析、组件集成测试)的目的是证实每个特定阶段的结果符合GB/T 38874.3中描述的设计与实现中的安全需求。

6.3 前提条件

本阶段的前提条件为：

——依据GB/T 38874.1—2020的6.4.6.3的安全计划，即截止日期、资源、设备、成熟度等。

——设备测试计划，为现有质量保证流程中的一部分。

——依据GB/T 38874.2—2020的第6章的HARA，即潜在危险的识别。

——依据GB/T 38874.2—2020的第7章的功能安全概念，即安全目标、安全状态及功能安全需求。

——依据GB/T 38874.3—2020的第5章的技术安全概念，即技术安全需求。

6.4 要求

6.4.1 SRP/CS设计的确认与验证

应对SRP/CS的设计进行确认与验证(见GB/T 38874.1—2020的图1)。

确认与验证时，应证实：

——每个SRP/CS满足指定AgPL的要求，包括：

a) 硬件类别、$MTTF_{DC}$、DC、CCF(见GB/T 38874.2—2020的附录A、附录B、附录C和附录D)；

b) SRL(见GB/T 38874.3—2020的第7章)。

——每个SRP/CS满足安全目标、安全状态及其他功能和技术的安全需求。

——每个SRP/CS实现了分配的安全相关功能。

6.4.2 安全确认与验证的范围

在安全寿命周期内，应按照以下方面进行安全需求的确认与验证：

——机器级的完整系统(例如：台架测试、硬件在环测试、测试设备)；

——硬件；

——软件。

库七七 www.kqqw.com 提供下载

6.4.3 活动

结构化安全确认与验证，应按照以下顺序：

——确认与验证计划；

——确认与验证规范；

——确认与验证的执行；

——确认与验证结果的记录。

6.4.4 确认与验证计划

应制定安全目标、安全状态、功能和技术安全需求等方面的确认与验证计划，且应包含下列条款：

——确认与验证及其可能的变化形式；

——系统成熟度；

——确认与验证目标；

——确认与验证技术；

——确认与验证负责人与开发人员之间的独立性声明；

——要求的设备和环境条件，包括工具校准规范；

——对总体安全计划的特定引用；

——通过/不通过的测试准则。

6.4.5 确认与验证的测试规范

应根据具体情况，指定下列测试方法：

——测试(例如：黑盒测试、HIL、机器测试、现场测试)；

——分析(例如：仿真)；

——相关文档复查(硬件/软件输入，例如：FMEA、电路图)。

6.5 工作产品

本阶段的工作产品为：

a) 详细的确认与验证计划；

b) 测试规范；

c) 确认与验证文档，应证实在下列方面已达到确认与验证目标：

1) 系统级和机器级的完整系统；

2) 硬件；

3) 软件。

7 配置管理

7.1 目的

第一个目的是对于给定的安全相关功能，确保 SRP/CS 与相关技术文档可随时被唯一标识和复制。

第二个目的是确保 SRP/CS 早期与当前版本的关系和差异可追溯、相关技术文档的可追溯。

7.2 前提条件

见安全寿命周期每个阶段的工作产品。

库七七 www.kqqw.com 提供下载

7.3 要求

应包含对软件工具和软件开发环境的配置管理。

应包含对 SRP/CS 规范和相关技术文档的配置管理。

应依照公司文档保留规定维护配置管理数据。

应明确标注包含 SRP/CS 的 E/E/PES 系统的所有变体或版本，标注可采用序列号或日期代码的形式。

7.4 工作产品

本部分的工作产品为：

SRP/CS 的列表，并参考给定配置的相关技术文档。

8 产品发布

8.1 目的

本阶段的目的是规定 E/E/PES 系统开发完成后的产品发布条件。产品发布证实了设备的功能安全需求已得到满足。

8.2 概述

图 1 给出了 E/E/PES 系统开发的批准程序以及产品发布的程序。

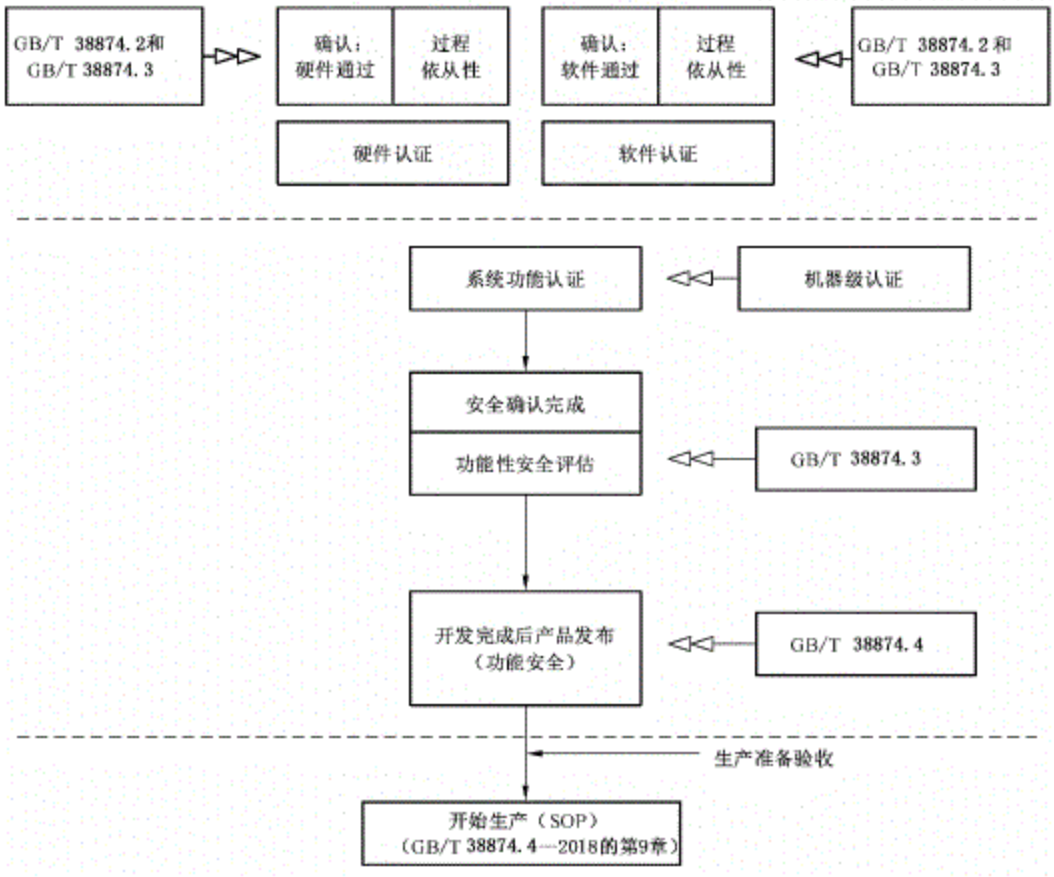

图 1 批准流程

库七七 www.kqqw.com 提供下载

8.3 前提条件

本阶段的前提条件为：

——硬件认证文档；

——软件认证文档；

——系统级或机器级的认证文档；

——功能安全评估文档。

8.4 要求

8.4.1 产品发布条件

仅在寿命周期(参见附录 A)前期阶段的下列结果有效时，才可批准产品发布：

——通过评估；

——硬件认证；

——软件认证；

——E/E/PES 系统级或机器级的系统认证(包括数据参数化设置)。

8.4.2 产品发布文档

产品发布内容应形成文档，并应包含下列内容：

——已发布的 E/E/PES 系统版本；

——已发布的 E/E/PES 系统配置；

——相关文档的引用；

——发布日期。

注：功能安全的发布文档可为 E/E/PES 系统产品发布文档的一部分或者为独立文档。

8.5 工作产品

产品发布文档。

9 生产计划、生产和产品测试

9.1 目的

本阶段的目的是制定 SRP/CS 生产与装配计划，并确保在生产过程中保持所要求的功能安全。由相关产品制造商或者负责人或者机构(机器制造商、供应商、分供应商等)负责该过程。

9.2 概述

本阶段定义了确保生产过程中保持功能安全所需的步骤，安全相关特性包含在生产计划和检验过程中。

9.3 前提条件

生产和生产测试的前提条件为：

——装配说明(与装配有关的部件或者功能的文档)；

——测试说明；

库七七 www.kqqw.com 提供下载

——产品发布文档；
——测试准则(待测试的安全相关特性)；
——产品监控：对安全相关特性的要求，并确保组件的安全相关特性符合在机器制造商生产过程中的规范。

9.4 要求

9.4.1 生产计划

生产计划包含装配说明，应包括：
——安全相关特性的标识；
——生产步骤的顺序和方法；
——装配设备/工具。

9.4.2 产品测试计划

测试计划应包括：
——安全相关特性的标识；
——测试步骤的顺序和方法；
——测试设备/工具、测试准则；
——生产测试频率。

9.4.3 人员

应由经过培训的人员按照生产和测试计划完成生产和测试。

9.4.4 工序能力

应按照行业通用要求确保工序能力。

9.4.5 文档

测试计划的实施情况应文档化。测试文档应最少包含测试日期、测试人员、部件唯一标识和测试结果。

9.4.6 不依从性

应建立不依从 SRP/CS 测试准则的规程。仅在验证过程可控的情况下，才允许重新开工。

9.4.7 储存和运输条件

当储存和运输产品时，应遵循 SPR/CS 特殊处理和包装要求。

9.5 工作产品

本阶段的工作产品为：
a) 符合测试计划的测试文档；
b) 不依从规程；
c) 储存和运输条件。

库七七 www.kqqw.com 提供下载

10 运行计划和维护(运行、维护、维修和报废说明)

10.1 目的

本阶段的目的是定义 SRP/CS 的维护范围、客户信息和维修说明,以便在运行、现场观察、维护、维修和报废期间保持要求的功能安全。

10.2 概述

本条描述了安全相关特性的各方面,涉及维修说明和用户信息编制以及维护工作的计划、执行和监控。

10.3 前提条件

运行计划和维护的前提条件为:

——产品发布:发布功能安全相关文档;

——质量管理体系(常规的质量管理体系,例如:ISO 9001);

——维护记录:受维护(维护任务)影响的安全相关方面以及现场分析经验;

——配置管理计划:配置管理的文档化过程。

10.4 要求

10.4.1 概述

维护和维修活动期间的功能安全需求可能与运行期间有所不同,应予以考虑。

10.4.2 维护计划表

维护计划表的编制应与系统设计并行开展,应包括:

——标识需预约维护的 SRP/CS 组件,并考虑已发布的子系统或系统的相关配置;

——顺序、方法(若必要可采用工具)以及维护时间间隔与维护范围。

10.4.3 维修说明

维修说明应包括:

——SRP/CS 维修组件的标识;

——工作步骤和工作流程、方法及工具(例如:适用的编程设备和诊断设备);

——已发布的系统或子系统的相关配置;

——可以停用子系统或系统并对整机进行必要的附加调整;

——标识备件,并在适当时批准更换备件。

10.4.4 维护人员说明

维修和维护工作应:

——由被授权且经培训的专业人员承担;

——依照维护计划或维修说明进行,并记录维护过程。

库七七 www.kqqw.com 提供下载

10.4.5 用户使用信息

应编制用户使用信息(例如:操作说明)。操作说明应包含在符合 ISO 3600 要求的用户手册中,且应包括:

——潜在危险的警告,包括与第三方产品所产生的危险;

——对子系统或系统的描述、状态信息(显示概念)以及用户反应情况;

——对维护组件的描述;

——禁止修改 SRP/CS(适用于 AgPL=a～AgPL=e)的警告。

10.4.6 现场观察

应制定现场观察的过程。基于现场分析结果,启动相应的应对措施。

10.4.7 储存和运输信息

对于产品的储存和运输条件定义,应考虑与正常驾驶有偏差的驾驶模式的安全相关特性(例如:被牵引、简化驾驶操作)。

10.4.8 报废和拆卸

由制造商提供关于机器报废和拆卸的要求。

10.5 工作产品

本阶段的工作产品为:

a) 维修说明;

b) 用户使用说明;

c) 储存和运输说明;

d) 报废和拆卸说明。

11 修改(变更管理)

11.1 目的

在修改与改造阶段期间或之后阶段,应确保功能性安全系统是适当的。

11.2 概述

当因生产、运行、现场观察、维护、维修或者子功能报废而对产品进行修改时,应通过影响分析来确定安全寿命周期需要重复的阶段。

变更管理有助于确保变更的系统规划、控制、监控、实施和归档,同时保持工作产品的一致性。在变更之前,要求对功能安全的潜在影响进行评估。因此,应引入并建立变更决策程序,划分各部门间的责任。

注:此处"变更"可理解为修改(修正、移除、添加和增强等)。

11.3 前提条件

变更管理的前提条件为:

库七七 www.kqqw.com 提供下载

——安全计划；

——配置管理计划。

11.4 要求

11.4.1 产品修改和改进规程

应制定产品修改或者改进的活动规程(标准操作规程)。图 2 给出了修改规程模型的示例,运行与维护管理模型的示例见图 3。

对 AgPL 等于“a”或以上的 SRP/CS 的修改只能由系统制造商授权的负责人或服务商执行。

只有按照功能安全管理规程发出授权请求后,才能启动修改产品和改进产品阶段(见 GB/T 38874.1—2020 的第 6 章)。

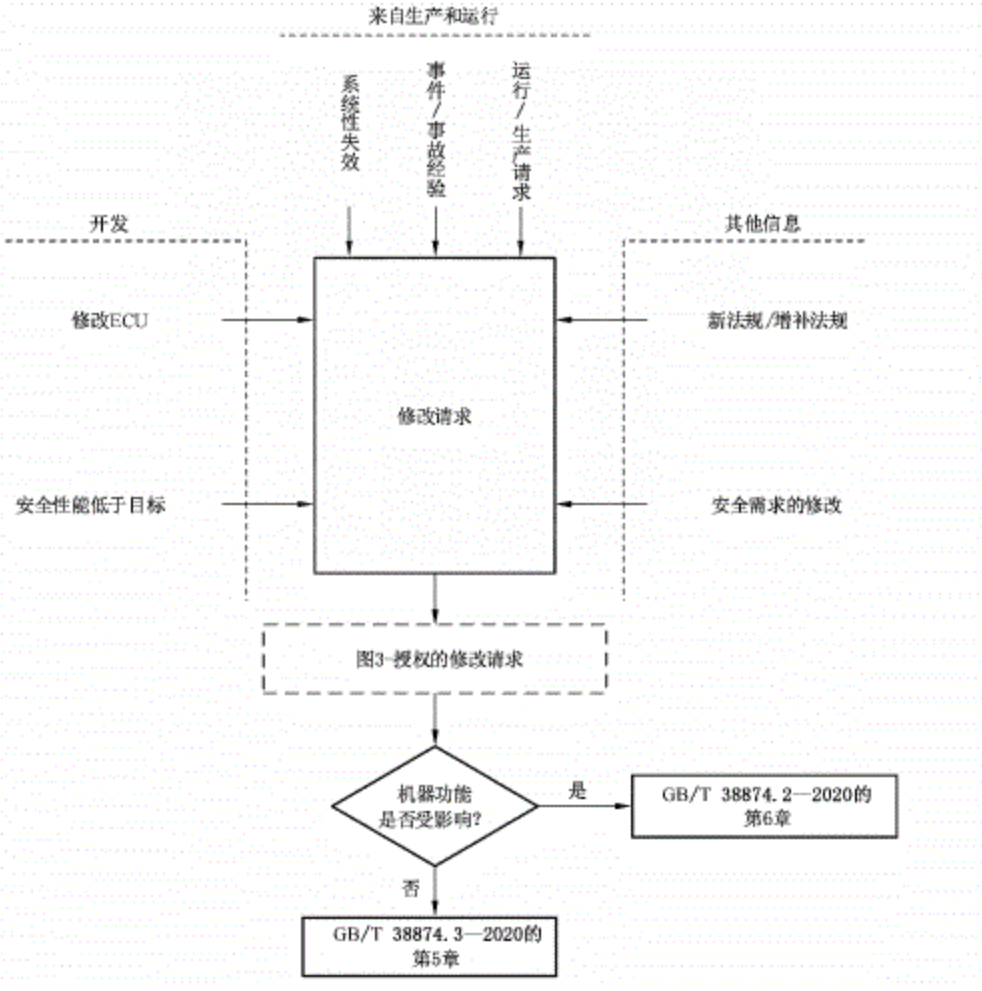

图 2 修改规程模型示例

库七七 www.kqqw.com 提供下载

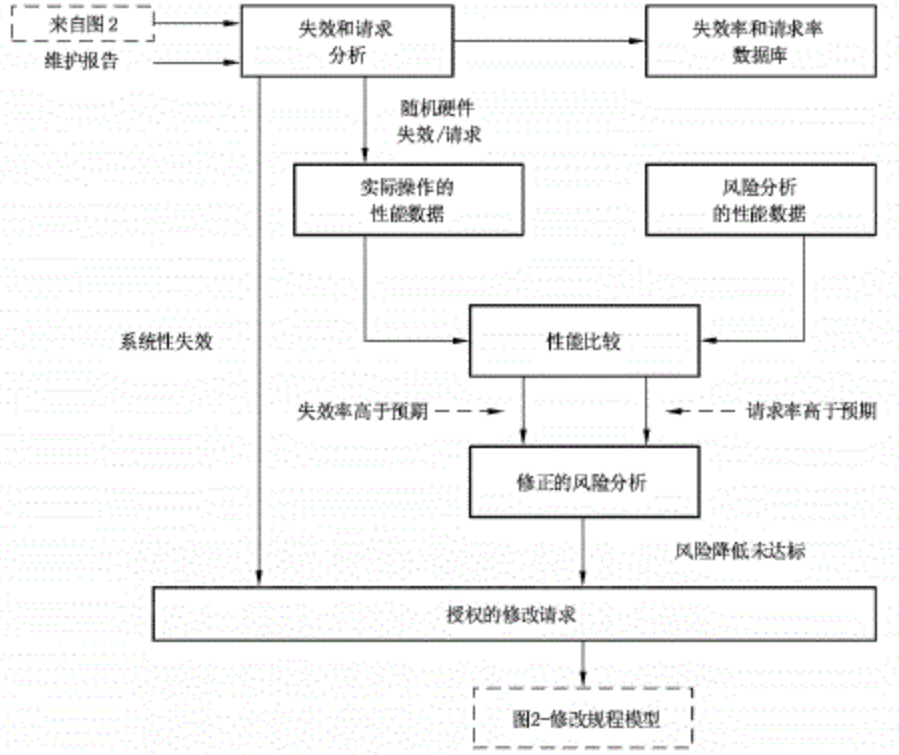

图 3　运行和维护管理模型示例

11.4.2　修改请求

修改请求应包含下列内容：

a)　修改原因；

b)　修改建议(硬件和软件)；

c)　确定修改可能导致的危险(影响分析)；

d)　机器间的兼容性。

注：请求修改的原因可为：

——功能安全低于指定值；

——系统故障经验；

——新安全法规或增补的安全法规；

——对受控设备或使用设备的修改；

——对总体安全需求的修改；

——对运行和维护性能进行分析，指出性能低于目标值；

——用户操作请求。

11.4.3　修改的影响评估

11.4.3.1　概述

负责人应决定已被修改的 UoO 是否需要风险分析(见 GB/T 38874.2—2020 的第 6 章)，或 UoO 是否未被修改(见 GB/T 38874.3—2020 的第 5 章)，这应在影响分析后确定(见图 2)。

如果对通道的 DC 或 $MTTF_{DC}$ 进行修改，则要求按照 GB/T 38874.2—2020 的第 6 章进行评估。如果未修改 DC 或 $MTTF_{DC}$，但微控制器改变(例如：微控制器由 16 位升级至 32 位)，则按照 GB/T 38874.3—2020 的第 6 章进行评估。

库七七 www.kqqw.com 提供下载

评估还应考虑其他同时进行的产品修改或产品改进活动的影响。

11.4.3.2 修改示例

下列三个修改示例给出了每种情况下要求的响应。

a) 制动传感功能的变更

如果制动传感功能从双通道变为单通道,应复查类别等级。开发工作流程应继续从 GB/T 38874.2—2020 的第 7 章开始。

b) 时速限制从 40 km/h 变更到 50 km/h

机器时速限制从 40 km/h 增加到 50 km/h,可能影响到机器的不同功能。要求对风险分析进行完全重新评估。应按照 GB/T 38874.2—2020 的第 6 章再次开始复查。

c) 控制器升级

如果微控制器由 16 位升级至 32 位而每个通道的类别、DC 和 MTTF 不变,则评估起始点应从 GB/T 38874.3—2020 的第 5 章继续。

注 1:有必要进行全面的危险及风险分析,得到的性能等级可能与当前受控设备指定的性能等级不同。

注 2:最初开发的用于最终审查的测试程序,在未检查其有效性的情况下不能重新使用。

11.4.4 修改授权

对要求的修改或改造活动是否授权应取决于影响分析结果。

11.5 工作产品

本阶段的工作产品为按时间排序的文档。应及时建立文档和维护文档,并提供修改和改造的详细信息,包括下列内容:

——修改或改造请求;

——影响分析;

——数据与结果的重新验证与重新确认;

——修改和改造活动影响的所有文档。

12 SRS/CS、子系统和组件的供应商规程

12.1 目的

本阶段的目的是描述分布式开发时 SRP/CS 的机器制造商、供应商和分供应商间关系的规程和责任。

12.2 概述

SRS/CS 机器制造商和供应商应共同遵循 GB/T 38874 规程。应明确界定机器制造商和供应商之间的责任。可有转包关系。在分布式开发项目或供应商负全责的开发项目中,由供应商建立关于计划、执行和归档的安全相关规范。

这不适用于标准组件的采购,也不适用于非安全相关组件的开发。

12.3 前提条件

本阶段的前提条件为:

——机器制造商/供应商开发的协议草案;通过协议界定在开发活动及工作产品中制造商和供应商的责任;

库七七 www.kqqw.com 提供下载

——供应商报价：为通用文档，不包含基于 GB/T 38874 的前提条件。

12.4 要求

12.4.1 概述

与分布式开发的机器制造商和供应商之间有关的活动应包括下列各项，有异议时可协商解决：

——项目启动；

——项目计划；

——项目执行；

——功能安全的评估；

——安全确认；

——记录；

——认证措施；

——SOP 后的活动。

12.4.2 要求范围

对机器制造商和供应商的相关要求适用于基于 GB/T 38874 开发系统的所有 SRP/CS。但在下列情况下的主要组件除外：

a) 特定系统安全需求未分配到主要组件；

b) 主要组件的技术和质量规范符合分配的系统安全需求。

12.4.3 供应商选择

选择供应商时，应考虑下列因素：

——评估与记录供应商是否有完善的质量管理体系；

——供应商在开发 SRP/CS、子系统或系统等方面的经验和能力。应对归档的功能安全管理过程进行检查，或由机器制造商和供应商共同商定该过程。

选择供应商时，应考虑所有相关部门的建议（例如：开发、质量、后勤部门）。

12.4.4 项目启动

项目启动时，应为机器制造商和供应商指定项目和子项目的功能安全负责人。

机器制造商项目经理应向供应商介绍产品开发过程和功能安全过程的相关部分。

应与供应商共同确定 GB/T 38874 需要执行的过程。应明确划分工作产品的责任。

机器制造商和供应商之间的协议中应说明与分包商的关系。

12.4.5 项目计划

机器制造商和供应商应对项目计划达成一致，包括计划表和关键节点。

机器制造商和供应商应共同协调其质量保障活动。

如果供应商向分包商下订单，供应商应按照 GB/T 38874 或类似标准管理这些分包商。

供应商应制定安全计划。

机器制造商应告知供应商所有影响功能和技术安全的需求变更，这些变更应符合更改管理规定。

12.4.6 项目执行

在整个项目期间，机器制造商和供应商应监控产品质量。

库七七 www.kqqw.com 提供下载

在供应商或分包商责任范围内项目活动中发生的安全相关事件、事故以及威胁项目的风险，供应商应向机器制造商报告。

供应商应标识不可实现的功能安全需求。在此情况下应修改功能安全概念。

机器制造商或供应商所进行的任何修改，如果影响采购系统的安全性或者影响到为证明其符合GB/T 38874 而采取的计划措施，应通知其他相关方进行影响分析。

12.4.7 开发合作方功能安全的认证措施

在安全寿命周期所有阶段，机器制造商和供应商应对其负责的功能安全进行评估。

供应商应向机器制造商报告功能安全的评估结果。

12.4.8 系统确认

系统确认应考虑整个机器的集成需求，应就哪些集成工作由机器制造商完成达成一致。

负责人应根据项目确认计划进行系统确认并归档。

12.5 工作产品

应按照 GB/T 38874 编制文档。

在项目的计划、执行和完成期间获取的安全相关信息应由供应商记录，确认产品满足规定的安全要求。供应商应向机器制造商提供足够的文档，使其认定产品满足规定的安全要求，并完成文档。

13 技术文档

13.1 目的

以文档形式提供所需信息(见表 A.1)，使整个安全寿命周期的每个阶段可有效开展，并且可再现。

13.2 要求

13.2.1 文档保留

在整个安全生命周期的每个阶段，应根据公司文档保留规定的保存文档。

注 1：每个相关方仅需掌握符合 GB/T 38874 要求的特定活动所必需的信息。

注 2：公司信息保留规定需符合国家法律法规。

13.2.2 文档结构

有效的文档应包括：

——功能安全管理；

——功能安全评估的执行。

文档还应具有下列特点：

——准确、简洁；

——易被使用者理解；

——使其他人理解其遵循的过程；

——符合预期目的；

——易访问及易维护；

——文档结构有利于检索相关信息；

库七七 www.kqqw.com 提供下载

——可标识出最新修订版本。

GB/T 38874 的文档要求主要关注信息而非物理文档。如果未在相关子条款中明确声明，则信息不需要包含在物理文档中。

必要文档的各条目可合并到一个文档中。

库七七 www.kqqw.com 提供下载

附 录 A
（资料性附录）
技术文档检查单

技术文档检查单见表 A.1。

表 A.1 技术文档检查单

阶段/措施		见 GB/T 38874 的章条号
整个安全寿命周期内的管理		**GB/T 38874.1—2020 中第 6 章**
	安全计划	GB/T 38874.1—2020 中 6.4.6.3
功能安全评估		**GB/T 38874.1—2020 中第 7 章**
	验证措施 （接受、有条件接受、驳回、待定条款、负责人）	GB/T 38874.1—2020 中 7.4.2
概念——UoO 的定义		**GB/T 38874.2—2020 中第 5 章**
	UoO 和环境条件	GB/T 38874.2—2020 中 5.3.1
	UoO 的限制及与其他 UoO 的接口	GB/T 38874.2—2020 中 5.3.2
	应力源	GB/T 38874.2—2020 中 5.3.3
	其他确认事项	GB/T 38874.2—2020 中 5.3.4
功能安全概念		**GB/T 38874.2—2020 中第 7 章**
	安全目标	GB/T 38874.2—2020 中 7.3.1
	功能安全需求和关联的 $AgPL_r$	GB/T 38874.2—2020 中 7.3.2
	所选类别	GB/T 38874.2—2020 中附录 A
	$MTTF_{DC}$ 的结果	GB/T 38874.2—2020 中附录 B
	DC 的结果	GB/T 38874.2—2020 中附录 C
	CCF 的结果	GB/T 38874.2—2020 中附录 D
	SRL 的结果	GB/T 38874.2—2020 中 7.3.5
系统设计		**GB/T 38874.3—2020 中第 5 章**
	技术安全概念规范	GB/T 38874.3—2020 中 5.4.2.2
	状态和时间	GB/T 38874.3—2020 中 5.4.2.2.2
	安全架构、接口和边界条件	GB/T 38874.3—2020 中 5.4.2.2.3
硬件		**GB/T 38874.3—2020 中第 6 章**
	硬件架构设计、类别和 AgPL	GB/T 38874.3—2020 中 6.4
	硬件安全需求	GB/T 38874.3—2020 中 6.4
	硬件安全确认测试计划	GB/T 38874.3—2020 中 6.6
	硬件安全确认测试规范	GB/T 38874.3—2020 中 6.6
	硬件安全确认测试结果	GB/T 38874.3—2020 中 6.6
	硬件系统集成测试计划	GB/T 38874.3—2020 中 6.6
	硬件系统集成测试规范	GB/T 38874.3—2020 中 6.6
	硬件系统集成测试结果	GB/T 38874.3—2020 中 6.6

库七七 www.kqqw.com 提供下载

表 A.1（续）

阶段/措施		见 GB/T 38874 的章条号
系列开发——软件		**GB/T 38874.3—2020 中第 7 章**
	软件项目计划	GB/T 38874.3—2020 中 7.1.5
	软件安全需求规格说明	GB/T 38874.3—2020 中 7.2.5
	非安全相关需求规格说明	GB/T 38874.3—2020 中 7.2.5
	验证报告或软件安全需求规格说明	GB/T 38874.3—2020 中 7.2.5
	软件架构	GB/T 38874.3—2020 中 7.3.5
	软件架构验证报告	GB/T 38874.3—2020 中 7.3.5
	软件详细设计	GB/T 38874.3—2020 中 7.4.5
	软件	GB/T 38874.3—2020 中 7.4.5
	软件部件设计和代码验证报告	GB/T 38874.3—2020 中 7.4.5
	软件部件测试计划	GB/T 38874.3—2020 中 7.5.5
	软件部件测试规范	GB/T 38874.3—2020 中 7.5.5
	软件部件测试报告	GB/T 38874.3—2020 中 7.5.5
	软件集成测试计划	GB/T 38874.3—2020 中 7.6.5
	软件集成测试规范	GB/T 38874.3—2020 中 7.6.5
	软件集成测试报告	GB/T 38874.3—2020 中 7.6.5
	软件安全测试计划	GB/T 38874.3—2020 中 7.7.5
	软件安全测试规范	GB/T 38874.3—2020 中 7.7.5
	软件安全测试报告	GB/T 38874.3—2020 中 7.7.5
	软件参数配置	GB/T 38874.3—2020 中 7.8.5
安全确认与验证		**GB/T 38874.4—2020 中第 6 章**
	确认与验证计划	GB/T 38874.4—2020 中 6.4.4
	确认与验证测试规范	GB/T 38874.4—2020 中 6.4.5
	确认与验证文档	GB/T 38874.4—2020 中 6.5
配置管理		**GB/T 38874.4—2020 中第 7 章**
	SRP/CS 的列表，并参考给定配置的相关文档	GB/T 38874.4—2020 中 7.4
SOP 发布		**GB/T 38874.4—2020 中第 8 章**
	产品发布文档	GB/T 38874.4—2020 中 8.4.2
生产计划		**GB/T 38874.1—2020 中第 9 章**
	安全生产步骤文档(生产计划)	GB/T 38874.1—2020 中 9.4.1
	测试和调整准则(安全相关)	GB/T 38874.1—2020 中 9.4.2
	不依从规程文档	GB/T 38874.1—2020 中 9.4.6

库七七 www.kqqw.com 提供下载

表 A.1（续）

阶段/措施		见 GB/T 38874 的章条号
生产、生产测试		**GB/T 38874.1—2020 中第 9 章** **GB/T 38874.4—2020 中第 9 章**
	安全生产计划的文档	GB/T 38874.4—2020 中 9.4.1
	安全相关测试计划的文档	GB/T 38874.4—2020 中 9.4.2
	不依从程序	GB/T 38874.4—2020 中 9.4.6
	产品安全相关准则的可追溯性	GB/T 38874.1—2020 中 9.4.7
	储存和运输条件	GB/T 38874.4—2020 中 9.4.7
维护（现场监控、维护、维修和报废）		**GB/T 38874.1—2020 中 8.4.3** **GB/T 38874.4—2020 中 10.4**
	维修说明	GB/T 38874.4—2020 中 10.4.3
	用户使用说明	GB/T 38874.4—2020 中 10.4.5
修改/变更管理		**GB/T 38874.4—2020 中第 11 章**
	修改或改造请求（经授权）	GB/T 38874.4—2020 中 11.5
	影响分析	GB/T 38874.4—2020 中 11.5
	数据和结果的重新确认与重新验证	GB/T 38874.4—2020 中 11.5
	修改和改造活动影响的所有文档	GB/T 38874.4—2020 中 11.5

库七七 www.kqqw.com 提供下载

参 考 文 献

[1] ISO 3600 Tractors, machinery for agriculture and forestry, powered lawn and garden equipment—Operator's manuals—Content and format

[2] ISO 9001 Quality management systems—Requirements

[3] ISO 12100 Safety of machinery—General principles for design—Risk assessment and risk reduction

[4] IATF 16949:2016 Quality management systems—Particular requirements for the application of ISO 9001:2008 for automotive production and relevant service part organizations

[5] IEC 61000-4-1 Electromagnetic compatibility (EMC)—Part 4-1: Testing and measurement techniques—Overview of IEC 61000- 4 series

[6] IEC 61496-1 Safety of machinery—Electro-sensitive protective equipment—Part 1: General requirements and tests

[7] HSE Guidelines on Programmable Electronic Systems in Safety-related Applications, Part 1 (ISBN 0 11 883906 6) and Part 2 (ISBN 0 11 883906 3)