

**中华人民共和国国家质量监督检验检疫总局**

**中 国 国 家 标 准 化 管 理 委 员 会**

发布

201X-XX-XX实施

201X-XX-XX发布

农林拖拉机和机械 控制系统有关安全部件 第1部分：设计与开发通则

**Tractors and machinery for agriculture and forestry—Safety-related parts of control system — Part 1: General principles for design and development**

（ISO25119-1:2010,IDT）

(征求意见稿)

**GB/T**XXXX.1—201X/ISO25119-1:2010

中华人民共和国国家标准

**ICS**65.060.01

**B** 90

1. 前 言

GB/T XXXX《农林拖拉机和机械 控制系统有关安全部件》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

1. 本部分是GB/T XXXX的第1部分。
2. 本部分按照GB/T 1.1—2009给出的规则起草。
3. 本部分使用翻译法等同采用ISO 25119-1:2010《农林拖拉机和机械 控制系统有关安全部件 第1 部分：设计与开发通则》（英文版）。
4. 为便于使用，本部分还对ISO 25119-1:2010做了下列编辑性修改：
5. ——“ISO 25119 的本部分”一词改为“本部分”；
6. ——用小数点“.”代替作为小数点的逗号“，”；
7. ——删除 ISO 25119-1:2010 的前言；
8. 本部分由中国机械工业联合会提出。
9. 本部分由全国农业机械标准化技术委员会（SAC/TC201）归口。
10. 本部分起草单位：
11. 本部分主要起草人：

农林拖拉机和机械 控制系统有关安全部件

第1部分：设计与开发通则

* 1. 范围

GB/T XXXX的本部分规定了控制系统有关安全部件（SRP/CS）设计与开发的通则，适用于农林拖拉机、农用自走机械、农用全挂及半挂机械、农用牵引机械。也可适用于市政机械（如：道路清扫机）。规定了实现安全功能的控制系统有关安全部件（SRP/CS）的特性及类别。

GB/TXXXX的本部分适用于电气/电子/可编程电子系统（E/E/PES）的有关安全部件。由于其涉及机械电子系统，本部分未规定用于特定场合的安全功能或类别。

GB/TXXXX的本部分不适用于非电气/电子/可编程电子系统（E/E/PES）（如：液压、机械及气压）。

注：见GB/T 15706中有关机械安全的设计准则。

* 1. 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 XXXX.2/ISO 25119-2:2010 农林拖拉机与机械 控制系统有关安全部件 第2部分：概念阶段

GB/T XXXX.3/ISO 25119-3:2010 农林拖拉机与机械 控制系统有关安全部件 第3部分：软硬件系列开发

GB/T XXXX.4/ISO 25119-4:2010 农林拖拉机与机械 控制系统有关安全部件 第4部分：生产、运行、修改与支持规程

* 1. 术语和定义

下列术语和定义适用于GB/TXXXX的本部分。



农业性能等级 agricultural performance level

AgPL

用于规定有关安全部件在预知条件下执行有关安全功能的能力等级。

注：适用于GB/T XXXX，每个危险状况的性能分为5个等级，即a、b、c、d及e。SRP/CS的功能安全，“a”为低，“e”为高。



农业性能等级要求 required agricultural performance level

AgPLr

每个有关安全功能达到要求的功能安全所需的性能等级。



类别 category

依据控制系统安全部件的防止故障能力及在故障状态下的后续行为对控制系统有关安全部件的分类，其能力通过部件的结构布置和/或可靠性达到。



通道 channel

输入、逻辑及输出元件的系列组合。



共因失效 common-cause failure

CCF

单一事件引起的不同类型的失效，这些失效相互间没有因果关系。

注：共因失效不应与共模失效相互混淆（见 GB/T 15706）



控制能力 controllability

涉及个体处于危险状况下避免伤害的可能性。



危险失效检测率 dangerous detected failure rate

λdd

可实现故障检测的部件的危险失效率。



危险失效 dangerous failure

即使有关安全功能通过其它（冗余）系统部件（由于性能等级的降低）维持，控制系统有关安全部件（SRP/CS）不再保持要求的性能等级的失效。



危险失效率 dangerous failure rate

λd

单位时间内所有部件危险失效的比率。



诊断覆盖率 diagnostic coverage

DC

危险失效检测率λdd与总的危险失效率λd的比值，表达式为：

****

1. 诊断覆盖率适用于高风险功能系统的整体或部件，如:传感器和/或逻辑系统和/或终端部件。
2. 注DC值按表1定义。
3. 对包含几个部件的SRP/CS，使用平均值DCavg表示（见 GB/T XXXX-2，附录C）

表1 诊断覆盖率（DC）

|  |  |
| --- | --- |
| **级别指示** | **范围** |
| 低 | DC＜60﹪ |
| 中 | 60﹪≤DC＜90﹪ |
| 高 | 90﹪≤DC |



诊断测试间隔 diagnostic test interval

具有指定的诊断覆盖率的有关安全系统在线故障检测时间间隔。



E/E/PES-系统架构 E/E/PES-system architecture

关键功能在电控单元（ECU）中的配置，以及在硬件、软件中的分类，包括通信。



环境条件 environmental condition

系统使用中所处的物理环境。



暴露量 exposure

个体处于有潜在危害状况的持续时间及频率。



失效 failure

产品丧失执行要求功能的能力。

1. GB/T XXXX系列标准不适用于不影响可控过程可用性的失效。
2. 失效后，产品出现故障。
3. “失效”是事件，“故障”是状态，两者应区分开。
4. 失效概念不适用于仅由软件组成的产品。

故障 fault

产品不能执行要求功能的表现状态，因预防维护或其它计划性活动，或缺少外部资源造成不能完成要求功能的情况除外。

1. 故障通常由产品自身的失效引起，但没有前期失效也会存在故障。
2. 在GB/T XXXX中，故障为随机故障。

功能 function

定义的单个或多个电子控制单元行为。



功能概念 functional concept

达到期望的行为所必须的基本功能及功能之间的交互。

注：在安全寿命周期的概念阶段开发。



功能要求 functional requirement

对E/E/PES系统的期望功能的要求。



功能安全 functional safety

系统运行时不能使操作者或围观者面临不可预知伤害的风险。



功能安全概念 functional safety concept

达到期望行为所必须的有关安全功能及交互的全部集合。

注：在安全寿命周期的概念阶段开发。



功能安全要求 functional safety requirement

对E/E/PES系统有关安全功能的要求。



硬件安全要求 hardware safety requirement

应用于有关安全硬件的要求，作为技术安全要求的一部分。



伤害 harm

身体损害。



危险 hazard

潜在的伤害源。



危险状态 hazardous situation

指人员暴露于一种或多种危险的环境，这类暴露会造成直接或长期的影响。



预定使用 intended use

（机器的）与操作手册提供的信息相一致的使用。



检查 inspection

用于复查产品质量的系统的、正式的验证方法。

注：在检查过程，一个或多个检查员将核对工作产品是否符合要求。一个检查领导组织并主持检查工作。工作产品的作者参与检查，但不能领导检查过程。



机器寿命 life of the machine

寿命周期 life cycle

机器从生产到报废的时间间隔。



手动复位 manual reset

控制系统有关安全部件内的功能，用于机器重启前，手动恢复一个或多个有关安全功能。



制造商 manufacturer

机器制造商machine manufacturer

农林拖拉机、农用自走机械、农用全挂及半挂机械、农用牵引机械、市政机械等的制造者。

参见 供应商（3.50）



平均危险失效时间 mean time to dangerous failure

MTTFd

危险失效预期时间的平均值。

1. 根据低、中、高三个范围进行定义。见表2。
2. 应用于GB/T XXXX，重要的是应逐个考虑SRP/CS的每个通道的MTTFd（MTTFdC）。
3. MTTFd是λd的倒数。

表2 平均危险失效时间

|  |  |
| --- | --- |
| **级别指示** | **范围** |
| 低 | 3年＜MTTFd＜10年 |
| 中 | 10年＜MTTFd＜30年 |
| 高 | MTTFd＞30年 |



监控 monitoring

自动监控 automatic monitoring

当一个部件或元件执行其功能的能力降低，或过程条件改变产生危险时，确保保护措施启动的自动功能。



抑制 muting

控制系统有关安全部件临时地自动暂停有关安全功能。



可编程电子系统 programmable electronic system

PES

使用一个或多个可编程电子装置用于控制、保护或监控的系统。

注：由系统所有的元件组成，包括电源、传感器及其它输入装置、数据高速通道及其它通信通道、执行器及其它输出装置。



保护措施 protective measure

由设计者执行的（内部设计、安全防护及配套措施、使用资料）和用户执行的（组织、安全工作规程、监督、工作许可、系统、附加安全措施、个人防护装置、培训）预期达到功能安全的措施。



可预见的合理误用 reasonably foreseeable misuse

没有按设计者预定的方法而是按照容易预见的行为习惯使用机器。



响应时间 response time

从错误发生到达到安全状态的最大持续时间。



风险 risk

伤害发生的概率及其严重程度的组合。



风险分析 risk analysis

机器的限制规范、危险识别及风险评估的组合。



风险评估 risk assessment

组成风险分析及风险评价的整个过程。



风险评价 risk evaluation

在风险分析的基础上判断面临的风险是否能够承受。



安全状态 safe state

具有可接受风险等级的系统操作模式。

例如：预期的操作模式、备份操作模式或关闭模式。



安全目标 safety goal

对避免给定危险方法的描述。

1. 这是最高级的安全要求，来自于危险分析和风险评估。
2. 一个项目可能有多个安全目标。

有关安全功能 safety-related function

功能失效后会立即导致风险增加的机器功能。



控制系统有关安全部件 safety-related part of a control system

SRP/CS

对输入信号响应并产生有关安全输出信号的控制系统的部件或子部件。

注：组合控制系统有关安全部件在有关安全信号的启动点开始（如：主动凸轮和滚筒的位置开关），在电源控制元件输出的位置结束（如：接触器的主触点），包括监控系统。



严重度 severity

对处于危险中个体的最可能伤害程度的度量。



软件要求等级 software requirement level

SRL

有关安全部件在预知条件下执行软件有关安全功能的能力。

注：SRL分为四组：SRL=B，1，2和3。



软件安全要求 software safety requirement

应用于有关安全软件的要求，作为技术安全要求的一部分。



供应商 supplier

农林拖拉机、农用自走机械、农用全挂及半挂机械、农用牵引机械、市政机械等机械部件和备件的制造者及供应者。

参见 制造商（3.31）



对称通道 symmetric channel

双通道或冗余通道系统中对单通道MTTFdC的数值组合。



系统性失效 systematic failure

确定与某个原因有关的，只有通过修改设计或制造工艺、操作程序、文件或其他关联因素才能消除的失效。

1. 无改进措施的维修保养通常不能消除这种失效。
2. 通过失效原因的模拟可以诱发系统失效。

例如：安全要求规范，硬件设计、制造、安装及操作，或软件设计及运行中的人为错误。



技术安全概念 technical safety concept

实现功能安全概念及将其分配到系统架构中所必须的技术安全要求的全部集合。

注：这是系统规范的一部分，在系统设计阶段定义。



技术安全要求 technical safety requirement

将给定的技术安全概念应用于SRP/CS的要求。



观察单元 unit of observation

电气、电子、电子可编程的系统或功能。

注：观察单元可以包含分布于多重系统的有关安全功能。



走查 walk-through

用于复查产品质量的系统化的、非正式的验证方法。

注：在走查过程，工作产品的生产者给一个或多个评估员提供每一步的报告。其目的是达到对工作产品共同的理解，发现工作产品中的错误、失误、差异或问题。走查的严格度低于检查。



工作产品 work product

设计或开发行为的输出。

* 1. 缩略语

下列缩略语适用于本标准。

AgPL 农业性能等级（agricultural performance level）

AgPLr 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）

DCavg 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）

EUC 可控设备（equipment under control）

FMEA 失效模式和影响分析（failure mode and effects analysis）

FMECA 失效模式影响及危害度分析（failure mode effects and criticality analysis）

EPROM 可擦除可编程只读存储器（erasable programmable read-only memory）

FSM 功能安全管理（functional safety management）

FTA 故障树分析（ fault tree analysis）

HAZOP 危险和可操作性研究（hazard and operability study）

HIL 硬件在环（hardware in the loop）

MTTF 平均失效时间（mean time to failure）

MTTFd 平均危险失效时间（mean time to dangerous failure）

MTTFdC 单通道平均危险失效时间（mean time to dangerous failure for each channel）

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

QM 质量措施（quality measures）

RAM 随机存取存储器（random-access memory）

SOP 开始生产（start of production）

SRL 软件要求等级（software requirement level）

SRP 有关安全部件（safety-related parts）

SRP/CS 控制系统有关安全部件（safety-related parts of control systems）

SRS 有关安全系统（safety-related system）

* 1. 完整安全寿命周期的管理
     1. 目的

本条陈述的主要目的是定义对完整安全寿命周期的各阶段负责的或在各阶段内对活动负责的相关人员、部门及机构的责任。这涉及确保项目功能安全等级要求的必须的活动及安全功能等级确认措施签署的活动。另一个目的是定义在完整安全寿命周期内的管理活动。

E/E/PES应当在完全考虑控制系统有关安全部件设计的风险分析、风险评估及迭代过程的情况下设计和制造（见图 1）。

注：GB/T XXXX仅涉及E/E/PES安全方面的评估。

* + 1. 概述
       1. 安全寿命周期概念介绍

安全寿命周期（见图2）把最重要的有关安全活动组合到概念阶段、系列开发阶段和开始生产（SOP）阶段。这些活动在GB/T XXXX.2 和 GB/T XXXX.3中详细描述。贯穿于寿命周期所有阶段的这些活动的计划、协调及验证是中心管理任务。

注：在概念阶段、系列开发阶段及SOP阶段之后的活动将在GB/T XXXX.2，GB/T XXXX.3 和 GB/T XXXX.4中详细描述。

* + - 1. 外部功能安全措施

这些措施不受系统定义中描述的观察单元的影响。外部功能安全包括相关人员（身体、语音等）或环境的特性，在系统定义中描述。在风险分析中，应考虑外部功能安全。

1. 外部功能安全效果的证明不属于GB/T XXXX的范围。
2. 在GB/T XXXX中不考虑如机械及液压等其它技术。这些包含于功能安全评估中，这些技术的功能安全确认不属于GB/T XXXX的范围。
   * 1. 前提条件

必要的前提条件是经过验证的质量保证计划（如：GB/T18305或等效标准）及完整项目计划。

* + 1. 要求——贯穿安全寿命周期的功能安全管理活动
       1. 功能安全理念

管理者及所有成员的一个任务是创建一种理念，使功能安全受到适当的关注。可这样进行，例如：

——通过明确地叙述安全功能目标和在机构内的相互交流，

——为达到功能安全对过程状态的复查。

* + - 1. 持续改进

管理应推动持续改进过程，方法包括：

——创建执行GB/T XXXX要求的具体企业规范，

——提供有助于有关安全活动的工具、模板、数据库及其它资源，

——获得项目中发现的有关安全部件问题的反馈并把发现的问题传递给新项目组成员。

* + - 1. 培训和资格认证

要求有适当资质的人员在安全寿命周期执行任务。目的在于保持以下各方面熟练度的均衡。

——技术安全概念，

——方法论，

——与要求相关的功能安全过程的知识和信息。

* + - 1. 开发期间的安全管理

目标是在开发过程中协调相关人员、部门和/或供应商之间的有关安全问题。

* + - 1. 安全责任分配

把功能安全并入属于GB/T XXXX范围的项目的活动计划及执行是负责观察单元机构或个人的中心管理任务。

最初，合并功能安全的责任属于项目经理。来自于此的任务可以是委派的。关于安全计划及有关安全缺陷的修改和相关的交流渠道与决策应清晰定义。

在这种情况下，应确保项目人员对承担的任务有足够的、有效的资质和能力。要求的培训和经验与AgPL及观察单元的复杂度有关。合适的有资质人员可以承担多种任务。特别地，该任务可以由具备合适资质的开发者执行。

* + - 1. 任务分配

下面是对功能安全基本任务的概述。

功能安全管理任务是项目经理指定的产品安全经理或安全团队经理的责任。

质量管理系统对实现安全管理活动是必须的。功能安全管理任务包括开发过程所有阶段的有关安全活动结果的及时正确的交付。单个任务的执行可以委派。

* + - 1. 开发过程全部安全管理活动计划
         1. 概述

计划安全寿命周期的开发阶段的所有安全活动，应至少包括以下内容：

——达到功能安全的程序及策略；

——分配及委派安全活动时，应确保人员和机构有足够有效的资质；

——开发合作者间的安全责任规范；

——提供项目中制定的支持程序；

——启动风险分析，按照GB/T XXXX.2，第6条；

——开发活动中的安全要求的执行，按GB/T XXXX.2，第7条和GB/T XXXX.3，第6-7条；

——开发合作者通过评估、复查及审核的方法确认履行了安全要求；

——安全要求的验证及确认计划，按照GB/T XXXX.4，第6条；

——功能安全确认的活动规范（审核、复查、评估）；

——全部项目管理活动融入项目安全管理中。

* + - * 1. 编写安全文档

安全文档的编写应使其它人能够理解遵循的过程。文档的保存应符合公司的文件保存要求。

* + - * 1. 安全计划



图1 控制系统有关安全部件设计的迭代过程



a这里的和其它有色的方框中的第一个数字表示GB/T XXXX的第几部分，斜线分开的第二个数字表示该部分的第几条，如：“2/5”表示GB/T XXXX.2，第5条。

b如果机器的功能不受影响，转到GB/T XXXX.3，第5条。

c如果机器的功能受影响，按照GB/T XXXX.2，第6条，执行危险和风险分析。

图2 安全寿命周期

目的

安全计划用于有关安全活动要求的系统化计划编制和资源分配。应考虑的范围在系统定义中描述，应考虑整个寿命周期。

安全计划应适应项目需要。对特定项目不是必需的一些活动或额外的活动也应当包含在内。

安全计划由产品安全经理编写，由项目经理实施。

有关安全活动应融入整个项目计划，并分配要求的资源。

安全计划的内容

安全计划应包括寿命周期定义的所有活动、支持活动、评估及管理活动。如果需要应进一步细分。

有关安全活动在安全计划中描述，下列活动的特性有必要描述：

——目的；

——前提条件—从其它活动、输入文档所得的结果；

——负责人；

——必要的资源；

——持续时间、截止日期；

——结果文档。

安全计划的格式

安全计划可以是单独的文档或集成于总的项目计划；如采用后者，有关安全活动应标示清楚。

安全计划可以包含对其他计划的引用。一般情况下，在多个文件中首选引用，而不是对活动进行并行描述。

安全计划应受到版本和更改管理的约束。

过程内的活动裁剪（适应于AgPL）

所有活动的特性总是取决于每个项目的AgPL及功能安全计划。

另外，如有正当理由，不适用于特定项目寿命周期的整个阶段及活动可以取消。

当编辑安全计划时，应注意使所有活动的具体特性适应项目的AgPL及状况要求。

如果个别的活动被取消或被简化执行，则应明确说明正当理由。

功能安全验证

确保功能安全的活动应包括安全审核、安全复查、安全评估，见表3。

表3 验证措施—安全审核、安全复查和安全评估

|  |  |  |  |
| --- | --- | --- | --- |
| 验证措施 | 审核 | 复查 | 评估 |
| 科目 | 功能安全要求的过程的执行 | 特定有关安全活动的结果（见表4的复查点） | 整个观察单元，在“系统定义”阶段描述 |
| 范围和深度 | 审核员设置 | 复查前制定计划 | 范围是功能安全要求的所有技术方法及过程的完整验证；  深度由评估者确定 |
| 寿命周期中的执行 | 在每一个活动完成前以及要求的程序执行期间 | 在每个有关安全活动完成后 | 和开发并行，或分组进行，  在系列发布前完成 |
| 职责 | 充分的验证程序 | 复查的正确执行 | 承担功能安全的连带责任 |
| 结果 | 审核报告（可以是评估的一部分） | 复查草案（可以是评估的一部分） | 观察单元功能安全的声明 |

* + 1. 工作产品

完整安全周期管理的工作产品如下：

——验证措施——在系列开发中用于审核过程的指导方法；

——安全计划。

* 1. 功能安全评估
     1. 目的

本阶段的目的是对观察单元及其中执行的功能所能达到的功能安全性进行检查和评估。

* + 1. 概述

对功能安全负有责任的机构（如：制造商或供应商）执行功能安全的评估。也可以委派一人负责评估活动。对在观察单元开发中涉及的各个机构，评估应当覆盖机器安全寿命周期的所有阶段（系统及安全概念、设计、执行、综合等级测试、系统发布、生产、操作）。相关机构应向制造商/供应商或负责人公开所有相关评估文档。

* + 1. 前提条件

至少，研发机构中的负责下述领域的代表应参加安全评估：

——系统负责人；

——系统开发人员；

——功能安全专家。

安全评估结果应文档化。文档的保存应符合制造商的文档保存规定和相关法律要求。

* + 1. 要求
       1. 功能安全评估的注意事项

注意事项由下列要求组成。

a）应当遵守在6.4.2中列出的用于验证措施的管理要求。

b）负责开发的机构应为安全评估提供一定程度的支持（充分的准备和足够可用的人力资源）。

c）安全评估人员应能访问到在硬件及软件寿命周期执行活动的所有人员，以及所有相关的信息及工具。

d）对在观察单元开发中涉及的各个部门，安全评估应包括机器安全寿命周期的所有阶段（系统及安全概念、设计、执行、综合等级测试、系统发布、生产、操作）。

e）如果工具用于开发、执行或测试，则应对它们的应用进行评估或验证。

f）安全评估可以和开发并行或分组进行。

g）安全评估应考虑以下方面：

1）前一次评估后进行的工作，

2）执行进一步评估的计划/策略，

3）在安全评估结论中给出：接受、有条件接受或拒绝建议。

* + - 1. 验证

以下要求应用于验证。

验证措施应包含在安全计划中。应定义观察单元及结果的格式。应书面明确验证执行的独立性。

验证计划由验证执行人员编制，并被对验证范围负责的人员接受。

验证结果应文档化。特别地，应声明关于接受、有条件接受或拒绝。待定条款应写明，并指定负责人及确认解决方法。

如果在复查及评估结论后，观察单元有改变，则复查或评估应重新进行或修正。

复查、审核及评估的执行应参考AgPL。应复查下列活动。

a）以AgPL=a开始:危险及风险分析。

b）另外，AgPL=b:

——安全要求，有关安全功能详细的等级；

——安全分析——系统FMEA，部件FMEA。

c）另外，AgPL =c:

——安全计划；

——定量安全分析；

——安全测试和测试范围——确认及验证计划。

d）另外，AgPL =d:

——安全要求——SRS；

——安全分析，如：FTA、FMEA；

——安全测试和测试范围——有关安全系统（SRS）参考测试案例；

——安全审核；

——功能安全评估。

e）另外，AgPL = e:

——安全分析，使用分析方法，如FMEA及FTA，考虑CCF机制；

——安全测试及测试范围——测试案例复查（确定是否包括所有案例）。

验证度取决于AgPL等级（见表 4）

表4 验证度

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 验证度 | AgPL = a | AgPL = b | AgPL = c | AgPL = d | AgPL = e |
| 危险分析和风险评估复查 | U2a | U2 | U2 | U3 | U3 |
| 安全计划复查  独立于计划制定者 | - | - | U1 | U2 | U3 |
| 安全要求复查  独立于制定者和安全要求的执行者 | - | U1 | U1 | U1 | U1 |
| V & V（验证和确认）计划复查  独立于计划制定者 | - | - | U1 | U1 | U2 |
| 安全分析（FMEA，FTA）复查  独立于分析者  独立于观察单元的开发者 | - | U1 | U1 | U1  U2 | U1  U3 |
| 安全测试及试验的复查  独立于测试的计划及行为 | - | - | U1 | U1 | U1 |
| 安全文档复查  独立于计划的制定者 | - | - | U1 | U2 | U3 |
| 安全审核  独立于安全功能要求和该工作有关的人员 | - | - | - | U2 | U3 |
| 安全计划评估 | - | - | - | U2 | U3 |
| - 无验证要求。验证措施的执行按6.4.2管理。  U1 其它人员  U2 其它团队（不是同一直接领导）  U3 其它部门或第三方（独立于开发部门，如：独立管理、独立资源、独立于发布责任部门、独立机构） | | | | | |
| a 要求独立复查，尤其在进行C0或S0评估的情况。见GB/T XXXX.2。 | | | | | |

* + 1. 工作产品

功能安全评估的工作产品包含验证措施文档：

——接受；

——有条件接受；

——拒绝；

——待定条款；

——责任人。

* 1. 开始生产（SOP）后的安全管理活动
     1. 目的

本阶段的目的是定义SOP后的功能安全的负责人、部门及机构。这涉及确保项目功能安全等级要求的必须的活动及安全功能等级确认措施签署的常规活动。

* + 1. 概述

见第5条。

* + 1. 前提条件

制造商应执行质量管理系统。

* + 1. 要求
       1. 生产及修改程序管理

在SOP后的寿命周期阶段，应采取组织措施，以达到所有产品的功能安全及在机器寿命周期的维护。达到和维护所有产品在机器寿命周期的功能安全的技术要求通常在观察单元的开发阶段规定，并按照修改程序修改。

* + - 1. 生产准备、生产进行及生产线末端检查的任务

生产/安装/调整及人员培训要求的执行应列出和监控。另外，和安全要求及文档相关的批量一致性应予以检查。

* + - 1. 机器安全操作及报废的任务

应执行下列任务。

——在操作手册中起草并包括特定内容和警示内容。

——列出对维护及制造厂维护人员的要求，并监控他们的执行情况。

——提供对观察到的故障的反馈。

——列出有关报废的安全要求（见 GB/T XXXX.4,第9条）。

——在质量管理系统中，考虑在V模型中放置项目里程碑（见 GB/T XXXX.3,图1）。

——在V模型的每个阶段应有验证措施。

——考虑在整个项目过程中，改进已有的V模型。

* + 1. 工作产品

SOP后的安全管理活动的工作产品是为操作手册准备的特定内容和警示内容。

* 1. 有关安全系统的生产与安装
     1. 目的

本阶段的目的是为SRS开发生产和安装的计划。另一个目标是确保要求的功能安全在生产过程能得到相关产品制造商或过程的负责人/机构的维护（机器制造商、供应商、分供应商等）。

* + 1. 概述

通过在生产计划及核查中加入有关安全特性，本阶段定义了确保功能安全在生产过程得到维护所要求的步骤。

* + 1. 前提条件

应获得下列资料：

——装配记录——受装配影响的组件或功能的文档；

——测试记录和标准——涉及测试程序的文档及有关安全功能的测试标准；

——产品发布——为生产、测试及安装发布的文档；

——产品监控——有关安全特性的要求和部件的有关安全特性连同其规范在机器生产商的生产过程中的在线维护。

* + 1. 要求
       1. 生产计划

考虑装配指导的生产计划应编制并包含以下内容：

——有关安全组件及特性的识别；

——生产步骤的顺序及方法；

——设备/工具。

* + - 1. 测试计划

考虑测试指导的测试计划应编制并包含以下内容：

——有关安全组件及特性的识别；

——测试步骤的顺序及方法；

——测试设备/工具，测试标准。

* + - 1. 生产及测试

生产及测试应由有资质的人员按生产及测试计划执行。

* + - 1. 工序能力

工序能力应借助于标准工业要求来确保。设备/工具及测试设备的工序能力也应通过通常的工业实践来确保。测试设备应经过适当的测试设备检查过程。

* + - 1. 文档

测试应按文档化的测试计划执行。测试文档至少应包括以下资料：测试日期、测试者、唯一的部件标识及测试结果，包括观察到的行为和期望行为的偏差。

* + - 1. 不依从性

应有不依从测试标准的判定程序。仅在证明过程可控时允许返修。

* + - 1. 可追溯性

产品有关安全部件给定的配置的可追溯性应能在生产过程中维持。

* + - 1. 储存及运输条件

在定义储存和准备产品运输条件时，应考虑有关安全标准（见 GB/T XXXX.4:201X的9.4.6）。

* + - 1. 修改

对由生产引起的产品修改，应使用影响分析确定寿命周期的应返回阶段和应重复阶段（见 GB/TXXXX.4:201X，第10条）。

注：对于工序的修改——无产品修改——见GB/T XXXX.4:201X的第8条。

* + 1. 工作产品

有关安全系统的生产与安装的工作产品是

——有关安全生产步骤的文档（生产计划），

——测试及调整标准（有关安全的），

——不依从性文档，

——用于有关安全标准的产品可追溯性。

附录A

（资料性附录）

特定项目安全计划的结构示例

A.1 概述

标题：项目/安全计划（“项目标识”）。

在系统概念阶段开始时，由管理部门指定项目计划的制定与编写者（项目经理，项目安全经理）。

A.2 更改记录

执行项目的所有部门及人员都应遵守安全计划。文档一旦更改不能撤销。

表A.1 介绍了更改记录的示例。

表A.1 更改记录

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 版本 | 更改 | 姓名 | 部门 | 日期 |
| 1. |  |  |  |  |  |
| 2. |  |  |  |  |  |
| 3. |  |  |  |  |  |
| ... |  |  |  |  |  |

A.3 整个项目的目标

详细项目目标说明应包含功能简要描述。

定义和接受通用条件以便与部件供应商合作。

A.4 进度表

进度表可以和其它进度表或文档链接。

A.5 项目机构

A.5.1项目团队机构

项目团队机构建立项目团队名单链接。

项目团队名单介绍所有相关人员（包括用户和分包商）的作用及相互关系。或者，人员名单也可以直接包含在安全计划中（见5.4.7）。

用户和分供商间的关系可以用可视图表来表示。

A.5.2 项目团队成员

项目人员及任务的命名，如表A.2. 和 A.3所示。

表A.2 项目团队成员

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 姓名 | 任务 | 部门 | 职位 | 电话 |
|  | 整个项目的项目经理 |  |  |  |
|  | 系统定义/系统规范 |  |  |  |
|  | 系统分析 |  |  |  |
|  | 硬件开发 |  |  |  |
|  | 传感器系统硬件开发 |  |  |  |
|  | 软件开发 |  |  |  |
|  | 田间试验 |  |  |  |

表A.3 任务

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 姓名 | 安全人员任务 | 资格 | 职位 | 电话 |
|  | 为项目安全经理提供支持 | 如：项目管理经验；了解团队成员的CV。 |  |  |
|  | 项目安全经理（同项目经理）  维护安全计划 |  |  |  |
|  | 供应方安全经理 |  |  |  |
|  | 为保证功能安全与供应方联系 |  |  |  |
|  | 为降低风险（功能安全）负责与分包商联系 |  |  |  |

A.5.3 安全管理

A.5.3.1 概述

安全管理要求应包含在A.5.3.2中，若有管理指南，应在管理指南中描述，并绑定到该项目中。

A.5.3.2 在项目级别之上的功能安全管理活动

下列活动分配给负责功能安全管理的人员：

——确保应用标准的获得；

——审核过程和标准操作规程；

——监控和分析(来自田间的)错误消息；

——比较计算的失效率与来自田间的经验值；

——修改与改进过程；

——培训进度表；

——为质量管理或FSM系统培训员工；

——发起有关安全更改。

A.5.3.3 和项目级别相关的功能安全管理活动

下列活动分配给负责功能安全管理的项目经理：

——协助定义项目团队；

——定义团队成员的职责范围；

——更新项目模板；

——使用项目模板；

——评估故障预防措施；

——（在FMEA中）评估故障检测措施；

——观察对（硬件及软件）模型、集成及系统测试的测试覆盖率；

——追踪要求；

——核查完整的复查；

——核查和履行本标准的要求。

参考文献

[1]GB/T 9480-2001 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（ISO3600:1996，IDT）

[2]GB/T19001-2008质量管理体系 要求(ISO 9001,2008 IDT）

[3]GB/T 15706 机械安全 设计通则 风险评估与风险减少（ISO12100，IDT）

[4]GB/T16856-2008 (所有部分) 机械安全 风险评价（ISO14121:2007，IDT）

[5]GB/T18305-2016 质量管理体系 汽车生产件及相关服务件组织应用GB/T19001-2008的特别要求(ISO/TS16949,2009 IDT）

[6]GB/T 17626 电磁兼容 试验和测量技术 抗扰度试验总论（IEC 61000-4-1，IDT）

[7] EN 61496-1, *Safety of machinery — Electro-sensitive protective equipment — Part 1: General requirements and tests*

[8] *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)