

# 团 体 标 准

T/NJ 1524—2024

## 拖拉机自动化系统 安全设计原则

Automated system of tractor—Safety design principles

(公示稿)

2024-XX-XX发布

2024-XX-XX 实施

中国农业机械学会发布



## 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。

本文件由中国农业机械学会提出。

本文件由全国拖拉机标准化技术委员会（SAC/TC 140）归口。

本文件起草单位：中国一拖集团有限公司、洛阳拖拉机研究所有限公司、洛阳智能农业装备研究院有限公司、龙门实验室、江苏沿海农业机械检测有限公司、河南科技大学。

本文件主要起草人：王梦华、尹海峰、李奕辰、王建华、宋国风、王永、王贡献、冀保峰、邢守辰、廖汉平、高宏峰、刘超、杨志刚、付世玉、卢晓朦、郭东洋、赵欢乐。



# 拖拉机自动化系统 安全设计原则

## 1 范围

本文件给出了拖拉机自动化系统的术语和定义、安全要求和风险减小措施。  
本文件适用于拖拉机自动化系统的设计、试验验证及使用。

## 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 4269.1 农林拖拉机和机械、草坪和园艺动力机械 操作者操纵机构和其他显示装置用符号  
第1部分：通用符号

GB/T 4269.2 农林拖拉机和机械、草坪和园艺动力机械 操作者操纵机构和其他显示装置用符号  
第2部分：农用拖拉机和机械用符号

GB/T 9480 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

GB/T 15706 机械安全 设计通则 风险评估与风险减小

GB/T 38874（所有部分） 农林拖拉机和机械 控制系统安全相关部件

## 3 术语和定义

下列术语和定义适用于本文件。

### 3.1

**功能 function**

拖拉机或拖拉机系统定义的动作和行为。

### 3.2

**自动 automatic**

拖拉机功能遵循定义的规则的过程或部分过程。

注：自动通常可以通过极少的操作者交互完成过程，但可以不通过操作者交互完成过程。

### 3.3

**自动化 automated**

通过自动方式控制和操作拖拉机功能的系统、方法或技术。

### 3.4

**手动 manual**

在拖拉机的所有操作循环中，无自动功能，拖拉机的功能在手动模式下进行操作。

示例：由操作者手动控制把机具提离地面。

### 3.5

**无人化 autonomous**

在拖拉机的所有操作循环中，拖拉机的自动化功能在无人模式下进行操作。

示例1：机具离地高度，在拖拉机的所有操作循环中，无需操作者交互由拖拉机自动地保持在设定高度。

3.6

**手动模式 manual mode**

拖拉机的功能由操作者直接控制的拖拉机操作模式。

3.7

**无人模式 autonomous mode**

拖拉机根据定义的任务执行功能，无需操作者交互的拖拉机操作模式。

注1：拖拉机的无人模式状态可能需要人工交互，如：准备、配置、设置及编程。这类人工交互不应认为是手动模式。

3.8

**操作循环 operating cycle**

拖拉机根据定义的操作执行的完整任务组。

3.9

**操作者交互 operator interaction**

操作者提供信息或控制拖拉机功能。

示例：操作者交互的例子有：启动、维护及停止拖拉机功能；为拖拉机提供额外的处理信息等。

3.10

**危险功能 hazardous function**

拖拉机或拖拉机系统定义的能引起伤害的动作和行为。

注：危险功能有别于安全功能。安全功能是指拖拉机的功能失效导致风险增加的功能，风险是指伤害的严重度与伤害的可能性的组合。危险功能是指在正常操作、无失效的情况下，能引起伤害的拖拉机功能（如：拖拉机的驱动功能）。

3.11

**障碍物 obstacle**

和拖拉机接触或碰撞后能导致伤害或被拖拉机伤害的实体或地面条件。

注：导致伤害的实体，如：树木、岩石等；被伤害的实体，如动物、人等。

3.12

**障碍物保护系统 obstacle protective system**

拖拉机对收到的来自障碍物探测部件或系统（如：传感器、感知系统、监督系统）信息进行响应的系统，以尽可能地避免和障碍物的接触。

3.13

**感知系统 perception system**

用于收集和处理拖拉机作业环境信息的拖拉机系统。

3.14

**监督系统 supervisory system**

具有状况认知和对拖拉机的操作进行决策的系统。

3.15

**状况认知 situational awareness**

基于感知系统获得的感知信息和拖拉机的状态信息确定拖拉机和环境的交互，以及拖拉机和环境交互的影响。

3.16

**警告区 warning zone**

对存在的障碍物需要警告的区域，如拖拉机没有发出警告，则障碍物将可能进入危险区。

3.17

**危险区 hazard zone**

障碍物的存在可能引起潜在伤害的区域。

3. 18

**无人操作区 autonomous operating zone**

拖拉机以无人模式进行操作的指定区域。

3. 19

**活动状态 active state**

拖拉机的自动化功能处于工作的拖拉机系统状态。

3. 20

**禁用状态 disabled state**

拖拉机的自动化功能处于禁用的拖拉机系统状态。

3. 21

**可用状态 enabled state**

拖拉机的自动化功能处于接收到确认命令或信息后可用的拖拉机系统状态。

3. 22

**降级状态 impaired state**

拖拉机的自动化功能在当前状态下不再处于完全安全的状态。

3. 23

**安全状态 safe state**

即使在控制系统失效或部分失效时，操作者或旁观者仍处于可接受的风险等级的系统操作状态。

3. 24

**听觉警报 audible alarm**

听觉能够探测到的信号。

3. 25

**视觉警报 visual alarm**

视觉能够探测到的信号。

3. 26

**警告时间 warning period of time**

拖拉机功能启动前指定的提醒时间。

3. 27

**本地操作者 local operator**

通过本地操作位或远程操作位控制拖拉机，也可以通过通知系统获取拖拉机信息的操作者。

3. 28

**本地操作位 local operator station**

拖拉机上指定的操作者为拖拉机提供信息或控制拖拉机的位置。

3. 29

**远程操作者 remote operator**

通过远程操作位控制拖拉机，也可以通过通知系统获取拖拉机信息的操作者。

3. 30

**远程操作位 remote operator station**

操作者为拖拉机提供信息或控制拖拉机的不位于拖拉机上的位置。

3. 31

### **通知系统 notification system**

为操作者提供注意拖拉机及操作状态信息的系统。

### **3.32**

### **使用场景 use case**

拖拉机使用的特定场景，包括拖拉机型式、操作条件、功能范围、系统边界和操作的设计区域。

### **3.33**

### **启动 start-up**

拖拉机或拖拉机的部分功能的接通。

## **4 安全要求和风险减小措施**

### **4.1 总则**

拖拉机自动化功能应按GB/T 15706规定的原则进行设计，拖拉机自动化功能的危险性依赖于使用场景，应按GB/T 15706给出的原则进行风险评估。对于评估后的拖拉机危险自动化功能（以下简称危险功能）应按GB/T 38874（所有部分）的规定进行设计，确定合适的软硬件性能等级，并考虑4.2规定的保护或风险减小措施。

### **4.2 设计原则**

#### **4.2.1 操作者在位系统**

配备操作者在位系统，用于探测操作者是否处于本地操作位或远程操作位。

**示例 1：**在自动化拖拉机的部分操作循环中，当拖拉机工作在无人模式时，座椅开关用于探测操作者是否处于本地操作位。

**示例 2：**无人化拖拉机工作在无人模式下，通过位于远程操作位的通知系统和操作者交互的行为监控或应答，探测远程操作者是否处于远程操作位。

#### **4.2.2 启动**

在设计中应考虑以下保护或风险减小措施：

- a) 启动时，危险功能应处于禁用状态；
- b) 启动时，在无人模式下为操作者提供把系统状态改变为可用状态的命令。

**示例：**拖拉机需要操作者的设置、上电及无人模式设置的确认。经确认后，拖拉机将进入无人模式的可用状态（如：就绪、待命或休眠）。在收到有效信号或命令后，拖拉机进入无人模式的活动状态。

#### **4.2.3 状态、模式和动作**

在设计中应考虑以下保护或风险减小措施：

- a) 为操作者提供用于改变危险功能状态和模式的手段，如接触开关、软按键或其它类似装置；
- b) 在特定条件下，危险功能自动从活动状态退出（如：传感器信号不足或丢失、操作者在位系统指示操作者不再处于操作位）。
- c) 在无人模式下，为操作者提供从本地操作位或远程操作位改变危险功能活动状态到安全状态的手段；
- d) 在无人模式下，提供仅能由操作者使用的启动危险功能进入活动状态的命令；
- e) 在无人模式下，为本地操作者提供从可用状态改变到活动状态的命令；



- f) 在无人模式下，在危险功能启动前，为危险功能提供一定的警告时间；
- g) 在无人模式下，当障碍物保护系统探测到危险区有障碍物和/或在特定条件（如：特定控制的手动移动、传感器信号不足或丢失、操作者在位系统指示操作者不再处于操作位）下，危险功能将自动维持在安全状态；
- h) 在无人模式下，在退出活动状态后，为操作者提供重新进入活动状态或重启危险功能的命令。

#### 4.2.4 视觉指示

在设计中应考虑以下保护或风险减小措施：

- a) 为操作者提供指示危险功能的视觉指示器。
- b) 在无人模式下，提供指示当前状态的视觉警报；
- c) 在无人模式下，提供危险功能（如：驱动功能）在警告时间、启动期间、启动后和工作期间的视觉警报；
- d) 为没有配备本地操作位的无人化拖拉机提供指示手动模式的视觉警报；  
示例：没有配备本地操作位的无人化拖拉机以手动模式准备切换到无人模式。
- e) 在无人模式下，当障碍物保护系统探测到危险区有障碍物时，提供视觉警报。

#### 4.2.5 听觉指示

在设计中应考虑以下保护或风险减小措施：

- a) 为操作者提供听觉指示器，当危险功能进入或退出活动状态时发出声响。
- b) 在无人模式下，提供指示进入各个状态的听觉警报；
- c) 在无人模式下，提供危险功能（如：驱动功能）在警告时间、启动期间、启动后和工作期间的听觉警报；
- d) 为没有配备本地操作位的无人化拖拉机提供以手动模式启动危险功能（如：驱动功能）的听觉警报；
- e) 在无人模式下，当障碍物保护系统探测到危险区有障碍物时，提供听觉警报。

#### 4.2.6 障碍物

在设计中应考虑以下保护或风险减小措施：

- a) 为危险功能提供障碍物保护系统；
- b) 仅当障碍物保护系统处于活动状态时，允许使用危险功能；
- c) 提供的障碍物保护系统，在无人模式下应：
  - 确保危险功能启动前，其相关危险区没有障碍物；
  - 确保危险功能在启动和操作过程中，当探测到其相关危险区有障碍物时，能自动地改变到安全状态；
  - 和危险功能的最大操作速度协调一致，以确保当探测到其相关危险区有障碍物时有足够的响应；
  - 确保在定义的危险功能警告区边界内的障碍物的足够探测（应考虑作物、尘土、雾、雨和雪等因素的影响）。

#### 4.2.7 操作区

在设计中应考虑以下保护或风险减小措施：

- a) 在无人模式下，提供诸如感知系统等手段，以防止拖拉机偏离无人操作区边界；

- b) 在无人模式下，4.2.7a) 中提供的手段应和危险功能的最大操作速度协调一致；
- c) 在无人模式下，仅当拖拉机位于定义的无人操作区内时，允许使用危险功能。

#### 4.2.8 监控

在设计中应考虑以下保护或风险减小措施：

- a) 提供的通知系统允许操作者对拖拉机和其特定功能进行适当的监控；
- b) 在无人模式下，通知系统和拖拉机的通信中断（定义的时间值）时，拖拉机自动地从活动状态或可用状态改变到安全状态。

#### 4.2.9 故障和失效

##### 4.2.9.1 总则

危险功能的设计应按照GB/T 38874（所有部分）的规定进行。

可使用监督系统探测系统的故障和失效，并采取相应的响应措施。

在设计中应考虑为视觉和听觉警报提供诊断（如：启动功能测试、电路电流检测），在视觉和听觉警报有故障的条件下，应通报操作者，且无人操作模式禁止使用，直至故障消除。

故障和失效应包括危险功能的电源供电。

##### 4.2.9.2 通信失效

系统应提供仅允许有意的和安全通信的措施。对于通信失效的响应应符合GB/T 38874（所有部分）的规定。

如危险功能的系统部件间的通信失效，系统应进入定义的安全状态。

通讯失效到危险功能停止前的可接受的时间应依据使用场景和使用信息确定。当通讯失效时间超出可接受的时间时，危险功能应进入定义的安全状态。

##### 4.2.9.3 故障

在设计中应考虑以下保护或风险减小措施：

- a) 当故障导致危险功能处于降级状态，则系统自动进入安全状态；
- b) 在无人操作模式下当故障导致危险功能处于降级状态，则系统自动退出无人模式，并进入安全状态。

#### 4.3 视觉和听觉警报

##### 4.3.1 总则

为便于检查视觉和听觉警报，应为操作者提供诸如接触开关、软按键或其它类似装置等手段。

##### 4.3.2 视觉警报

在设计中应考虑以下保护或风险减小措施：

- a) 如配置有视觉警报，则其应能被操作者和临近的人员观察到。
- b) 视觉警报应采用以下颜色指示无人模式的状态：
  - 白色（电源接通，禁用状态，常亮）；白色视觉警报允许用于4.3.2e)中的障碍物探测和手动模式的其它功能指示；
  - 绿色（可用或活动状态，常亮）；绿色视觉警报允许用于4.3.2e)中的障碍物探测，不允

许用于手动模式的其它功能指示；

——红色或蓝色（错误，常亮）；禁止红色或蓝色警报闪烁；禁止同一蓝色或红色警报用于手动或无人模式的其它功能指示。

- c) 无人模式下，在危险功能启动前、启动中、启动后和工作过程中，视觉警报应用琥珀色、以60次/min~85次/min的频率闪烁，视觉警报应至少提前一个警告时间。如果使用多个指示灯，所有指示灯应同步闪烁。允许使用同一琥珀色光源用于无人模式下的障碍物探测的临时指示和无人化拖拉机的手动模式指示；
- d) 对于没有配备本地操作位的无人化拖拉机的手动模式指示，视觉警报应用琥珀色、以60次/min~85次/min的频率闪烁，如果使用多个指示灯，所有指示灯应同步闪烁。在以下情况下允许使用连续常亮无闪烁的琥珀色指示灯：
  - 危险功能处于禁用状态；
  - 额外的视觉警报闪烁琥珀色光源和常亮无闪烁琥珀光源组合使用。
- e) 在无人操作模式下，视觉警报应使用白色、绿色或琥珀色的任一个或三者的组合闪烁光源指示探测到障碍物保护系统危险区有障碍物或障碍物正在进入危险区。闪烁频率应高于125次/min，闪烁持续时间或闪烁持续时间的循环次数应由制造商按照GB/T15706的规定经风险评估后确定。

#### 4.3.3 听觉警报

在设计中应考虑以下保护或风险减小措施：

- a) 如配置有听觉警报，则其应能被操作者和临近的人员听到。
- b) 如配置有听觉警报，听觉警报应以一致的、且不同的时间间隔、持续周期及重复的持续周期循环的声音分别指示进入以下无人操作模式的状态，该听觉警报应和4.3.3c)、4.3.3d)和4.3.3e)所用的警报不相同：
  - 电源接通，禁用状态；
  - 可用或活动状态；
  - 错误。
- c) 在无人操作模式下，在危险功能启动前、启动中、启动后和工作过程中，应以一致的危险功能听觉警报进行指示，该警报应至少提前一个警告时间周期。危险拖拉机功能听觉警报在时间间隔、持续周期及重复的持续周期循环方面应和4.3.3b)和4.3.3e)所用的听觉警报不相同。允许使用4.3.3d)中所用的听觉警报；
- d) 对于没有配备本地操作位的无人化拖拉机的手动模式指示，在危险功能启动前、启动后应以一致的危险功能听觉警报进行指示，危险功能听觉警报在时间间隔、持续周期及重复的持续周期循环方面应和4.3.3b)和4.3.3e)所用的听觉警报不相同。允许使用4.3.3c)中所用的听觉警报；
- e) 在无人模式下，应以一致的听觉警报指示探测到障碍物保护系统的危险区有障碍物或障碍物正在进入危险区。该警报在时间间隔、持续周期及重复的持续周期循环方面应和4.3.3b)、4.3.3c)和4.3.3d)所用的听觉警报不相同。

#### 4.4 标签和标识

自动化系统所用符号应符合GB/T 4269.1和GB/T 4269.2的规定。指示器应明晰和易于辨认。

#### 4.5 使用信息

使用说明书应按GB/T 9480 的规定编制，应至少为自动化系统提供以下使用信息：

- a) 拖拉机预期的使用场景（如：拖拉机类型、农田、作物、土壤、环境、作业条件）；
  - b) 禁止使用的信息（如：在公共道路上的操作）；
  - c) 所有操作模式的禁止条件信息（如：地面条件、气候条件、作物类型）；
  - d) 视觉和听觉警报信息，指示的含义和将要采取的措施；
  - e) 拖拉机的标志和标识信息；
  - f) 服务、维护、检查和标定信息；
  - g) 在本地操作位上控制危险功能进入可用状态、活动状态或超越危险功能的操作信息；
  - h) 在本地操作位上控制拖拉机从无人模式转换为手动模式和从手动模式转换为无人模式的操作信息；
  - i) 在远程操作位上控制拖拉机的操作规程最小的要求信息；
  - j) 在无人模式下危险功能允许的拖拉机最大作业速度；
  - k) 安全状态描述信息。
-