

GuardLogix 5570 控制器系统

产品目录号 1756-L71S, 1756-L72S, 1756-L73S, 1756-L73SXT, 1756-L7SP, 1756-L7SPXT, 1756-L72EROMS,
Studio 5000 Logix Designer 应用程序



原版说明书的中文译本

重要用户信息

在安装、配置、操作或维护本产品之前，请阅读本文档以及“其他资源”章节所列的文档，了解关于安装、配置和操作本设备的信息。除了所有适用的规范、法律和标准的要求之外，用户还必须熟悉安装和接线说明。

包括安装、调整、投入运行、使用、装配、拆卸和维护等在内操作必须由经过适当培训的人员根据适用的操作守则来执行。

如果本设备的使用方式不符合制造商的规定，则可能会削弱设备的防护功能。

对于由于使用或应用此设备而导致的任何间接或连带损失，罗克韦尔自动化在任何情况下均不承担任何责任。

本手册中的示例和图表仅供说明之用。由于任何特定的安装都存在很多差异和要求，罗克韦尔自动化公司对于依据这些示例和图表所进行的实际应用不承担任何责任和义务。

对于因使用本手册中所述信息、电路、设备或软件而引起的专利问题，罗克韦尔自动化不承担任何责任。

未经罗克韦尔自动化公司的书面许可，不得部分或全部复制本手册的内容。

在整本手册中，我们在必要的地方做出了说明，以向您告知安全注意事项。

	警告： 标识在危险环境下可能导致爆炸，进而造成人员伤亡、财产损失或经济损失的行为或情况的信息。
	注意： 标识可能造成人员伤亡、财产损失或经济损失的行为或情况的信息。注意符号可帮助您确定危险情况，避免发生危险，并了解可能的后果。
重要事项	标识对成功应用和理解产品有重要作用的信息。

设备表面或内部的标签提供特定的预防措施。

	触电危险： 位于设备(例如，驱动器或电机)表面或内部的标签，提醒人们可能存在危险电压。
	烧伤危险： 位于设备(例如，驱动器或电机)表面或内部的标签，提醒人们表面可能存在高温危险。
	闪弧危险： 位于设备(例如，电机控制中心)表面或内部的标签，提醒相关人员可能出现闪弧。闪弧可导致重伤或死亡。佩戴适当的个人防护设备(PPE)。遵循所有安全工作惯例和个人防护设备(PPE)的规章要求。

Allen-Bradley, Armor, ArmorBlock, ArmorGuard, CompactBlock, CompactLogix, ControlFLASH, ControlLogix, ControlLogix-XT, FLEX, Guard I/O, GuardLogix, GuardLogix-XT, Kinetix, Logix5000, POINT Guard I/O, Rockwell Automation, Rockwell Software, RSLogix, SLIC, SmartGuard, Studio 5000, Studio 5000 Automation Engineering & Design Environment are trademarks belonging to Rockwell Automation, Inc
ControlNet、DeviceNet 和 EtherNet/IP 是开放设备网供应商协会的商标。不属于罗克韦尔自动化的商标是其各自所属公司的财产。

本手册中包含新增信息和更新信息。

新增和更新信息

下表给出了本版手册所做的变更。

主题	页码
酌情将术语“安全 I/O 模块”更改为更通用的“安全 I/O 设备”	整本手册
封面增加了 Armor™ GuardLogix® 产品目录号， 1756-L72EROMS	封面
SIL-3 认证组件列表中增加了 Kinetix® 5500 伺服驱动器的信息	16
通信接口模块列表中增加了 1756-EN2TRXT 模块	23
增加了存在重复 SNN 和节点地址组合时项目无法通过校验的注意事项	35
增加了 Kinetix 5500 Servo Drive User Manual (Kinetix 5500 伺服驱动器用户手册) 的引用链接，提供在安全应用项目中使用运动直接命令的信息	72
增加了 Guard I/O™ 模块的更新安全数据 (IEC 61508，第 2 版，2010 年)	附录 E
增加了 1734-IB8S，系列 B 和 1734-OB8S，系列 B 模块的安全数据	附录 E
更新了 1734-IE4S 模块的 PFH 数据	附录 E

备注:

变更摘要	重要用户信息	2
目录	新增和更新信息	3
前言	Studio 5000 环境	9
	术语	10
	其他资源	10
	章节 1	
安全完整性等级 (SIL) 原理	SIL 3 认证	13
	验证测试	14
	SIL 3 应用项目的 GuardLogix 架构	15
	GuardLogix 系统组件	16
	GuardLogix 认证	18
	GuardLogix PFD 和 PFH 技术规范	18
	安全完整性等级 (SIL) 符合性的分配与权重	19
	系统反应时间	19
	安全任务反应时间	20
	安全任务周期和安全任务看门狗	20
	发生设备故障时的联络信息	20
	章节 2	
GuardLogix 控制器系统	GuardLogix 5570 控制器硬件	21
	主控制器	22
	安全伙伴	22
	机架	22
	电源	22
	CIP 安全协议	22
	安全 I/O 设备	23
	通信网桥	23
	编程概述	25
	章节 3	
GuardLogix 控制系统的	概述	27
CIP 安全 I/O	CIP 安全 I/O 设备的典型安全功能	27
	诊断	28
	状态数据	28
	状态指示灯	28
	接通或断开延时功能	28
	反应时间	28
	CIP 安全 I/O 设备的安全注意事项	29
	所属关系	29
	安全 I/O 配置签名	29
	安全 I/O 设备更换	29

章节4	
CIP 安全和安全网络编号	可路由 CIP 安全控制系统..... 33
	唯一节点参考 34
	安全网络编号 34
	分配安全网络编号 (SNN) 时需考虑的因素 35
	安全消费者标签的安全网络编号 (SNN)..... 35
	出厂设备的安全网络编号 (SNN)..... 36
	带不同配置宿主的安全设备的安全网络编号 (SNN) 36
	复制安全项目时的安全网络编号 (SNN)..... 36
章节5	
安全标签、安全任务和安全程序的特性	标准与安全之间的区别 37
	SIL 2 安全应用项目..... 38
	安全任务中的 SIL 2 安全控制..... 38
	标准任务中的 SIL 2 安全控制..... 40
	SIL 3 安全 — 安全任务 41
	安全任务限制条件..... 41
	安全任务执行细节..... 42
	使用人机界面 43
	预防措施 43
	访问安全相关系统..... 44
	安全程序 45
	安全例程 45
	安全标签 46
	安全例程中的标准标签 (标签映射) 47
章节6	
安全应用项目开发	安全原理的假设条件..... 49
	应用程序开发和测试基础..... 50
	调试生命周期 51
	控制功能的技术规范 52
	创建项目 53
	测试应用程序 53
	生成安全任务签名..... 53
	项目验证测试 54
	确认项目 55
	安全验证 56
	锁定 GuardLogix 控制器..... 56
	下载安全应用程序 56
	上传安全应用程序 57
	在线编辑 57
	从非易失性存储器存储和加载项目 58
	数据的强制赋值..... 58
	禁止设备 58
	编辑安全应用项目 59
	执行离线编辑 60
	执行在线编辑 60
	修改影响测试 60

监视状态和处理故障

章节7

监视系统状态	63
CONNECTION_STATUS 数据	63
输入和输出诊断	64
I/O 设备连接状态	64
断电跳闸系统	65
获取系统值 (GSV) 和设置系统值 (SSV) 指令	65
GuardLogix 系统故障	66
不可恢复的控制器故障	66
不可恢复的安全故障	66
可恢复的故障	67

安全指令

用户自定义安全指令

附录A

附录B

创建和使用用户自定义安全指令	73
创建用户自定义指令测试项目	75
创建用户自定义安全指令	75
生成指令签名	75
下载并生成安全指令签名	76
SIL 3 用户自定义指令验证测试	76
确认项目	76
安全验证用户自定义指令	77
创建签名历史条目	77
导出和导入用户自定义安全指令	77
校验用户自定义安全指令签名	77
测试应用程序	78
项目验证测试	78
安全验证项目	78
其他资源	78

附录C

反应时间

系统反应时间	79
Logix 系统反应时间	79
简单输入 — 逻辑 — 输出链	80
使用生产者 / 消费者安全标签的逻辑链	81
影响 Logix 反应时间分量的因素	82
访问 Guard I/O 输入模块延迟时间设置	82
访问输入和输出安全连接反应时间限制	83
配置安全任务周期和看门狗	84
访问生产者 / 消费者标签数据	85

GuardLogix 安全应用项目的检查表	附录 D GuardLogix 控制器系统的检查表 88 安全输入检查表 89 安全输出的检查表 90 开发安全应用程序的检查表 91
GuardLogix 系统安全数据	附录 E PFD 值 93 PFH 值 94
RSLogix 5000 软件版本 14 及更高版本的安全应用项目指令	附录 F 断电跳闸系统 95 使用连接状态数据以程序方式启动故障 95
将 1794 FLEX I/O 模块、1756 SIL 2 输入和输出与 1756 GuardLogix 控制器组合使用，以符合 EN 50156 标准要求	附录 G SIL 2 双通道输入 (GuardLogix 控制器的标准侧) 101 使用 SIL 3 Guard I/O 输出模块的 SIL 2 输出 103 使用 1756 或 1794 SIL 2 输出模块的 SIL 2 输出 103 1756 GuardLogix 安全任务内的安全功能 104
	术语表
	索引

主题	页码
Studio 5000 环境	9
术语	10
其他资源	10

本手册旨在描述 GuardLogix 5570 控制器系统，该系统经过型式批准和认证，可在达到 (包括) SIL CL 3 等级 (依据 IEC 61508 和 IEC 62061) 以及 (包括) 性能等级 Ple (4 类) (依据 ISO 13849-1) 的安全应用项目中使用。

如果您负责基于 GuardLogix 5570 控制器的安全系统 (使用 Studio 5000® Logix Designer 应用程序，版本 21.000 或更高版本) 的开发、操作或维护，则应使用本手册。在操作基于 GuardLogix 5570 控制器的安全系统之前，您必须阅读并了解本手册给出的安全原理和要求。

如需了解 RSLogix™ 5000 项目中与 GuardLogix 5570 控制器相关的安全要求，请参见 GuardLogix Controllers Safety Reference Manual (GuardLogix 控制器安全标准手册，出版号：[1756-RM093](#))。

Studio 5000 环境

Studio 5000 自动化工程和设计环境将工程和设计元素组合在一个通用的环境中。Studio 5000 环境中的第一个元素是 Logix Designer 应用程序。Logix Designer 应用程序由 RSLogix 5000 软件更新换代而成，继续作为 Logix5000™ 控制器的编程产品，用于编写离散、过程、批处理、运动、安全和基于驱动器的各种解决方案。



Studio 5000 环境将成为罗克韦尔自动化工程设计工具和功能的基础。它是设计工程师开发控制系统所有元件所需的一站式软件。

术语

下表定义了在本手册中使用的术语。

表 1- 术语和定义

缩写词	术语全称	定义
1oo2	二选一	指出可编程电子控制器架构。
CIP	通用工业协议	一种由基于 Logix5000™ 的自动化系统在 Ethernet/IP™、ControlNet™ 和 DeviceNet™ 通信网络上使用的工业通信协议。
CIP 安全	通用工业协议 — 安全认证	CIP 的 SIL 3 等级版本
DC	诊断覆盖率	已检测到的故障率与总故障率之比。
EN	欧洲标准	欧洲官方标准。
GSV	获取系统值	一种检索指定控制器状态信息并将其放在目标地址标签中的梯形图逻辑指令。
PC	个人计算机	用于通过 Studio 5000 环境与基于 Logix 的系统进行通信并执行控制的计算机。
PFD	要求故障概率	系统无法执行其设计任务的平均概率。
PFH	每小时故障概率	系统每小时出现危险故障的概率。
PL	性能等级	ISO 13849-1 安全等级。
SNN	安全网络编号	标识安全网络某一部分的一个唯一编号。
SSV	设置系统值	一种设置控制器系统数据的梯形图逻辑指令。
--	标准	项目中任何与安全无关的对象、任务、标签、程序或组件等 (也就是说, 标准控制器通常指 ControlLogix 或 CompactLogix™ 控制器)。

其他资源

以下文档包含与罗克韦尔自动化产品相关的更多信息。

资源	说明
GuardLogix 5570 Controllers User Manual (GuardLogix 5570 控制器用户手册, 出版号: 1756-UM022)	提供如何在 Studio 5000 Logix Designer 项目中安装、配置、编程和使用 GuardLogix 5570 控制器的信息
GuardLogix Safety Application Instruction Set Reference Manual (GuardLogix 安全应用项目指令集参考手册, 出版号: 1756-RM095)	提供关于 GuardLogix 安全应用项目指令集的信息
Guard I/O DeviceNet Safety Modules User Manual (Guard I/O DeviceNet 安全模块用户手册, 出版号: 1791DS-UM001)	提供关于如何使用 Guard I/O DeviceNet 安全模块的信息
Guard I/O EtherNet/IP Safety Modules User Manual (Guard I/O EtherNet/IP 安全模块用户手册, 出版号: 1791ES-UM001)	提供关于如何使用 Guard I/O EtherNet/IP 安全模块的信息
POINT Guard I/O Safety Modules User Manual (POINT Guard I/O 安全模块用户手册, 出版号: 1734-UM013)	提供关于如何安装和使用 POINT Guard I/O™ 模块的信息
Kinetix 5500 Servo Drives User Manual (Kinetix 5500 伺服驱动器用户手册, 出版号: 2198-UM001)	提供关于如何安装和使用 Kinetix 5500 伺服驱动器的信息
Using ControlLogix in SIL 2 Applications Safety Reference Manual (在 SIL2 应用项目中使用 ControlLogix 安全参考手册, 出版号: 1756-RM001)	描述了在 SIL 2 安全控制应用项目中使用 ControlLogix 控制器和 GuardLogix 标准任务的要求
Logix5000 General Instruction Set Reference Manual (Logix5000 常规指令集参考手册, 出版号: 1756-RM003)	提供关于 Logix5000 指令集的信息
Logix Common Procedures Programming Manual (Logix 通用编程步骤手册, 出版号: 1756-PM001)	提供关于对 Logix5000 控制器进行编程的信息, 包括如何管理工程文件、安排标签、编写和测试例程以及处理故障
Logix5000 Controllers Add-On Instructions Programming Manual (Logix5000 控制器用户自定义指令编程手册, 出版号: 1756-PM010)	提供关于在 Logix 应用项目中创建和使用标准与用户自定义安全指令的信息
ControlLogix System User Manual (ControlLogix 系统用户手册, 出版号: 1756-UM001)	提供关于在非安全应用项目中使用 ControlLogix 控制器的信息
DeviceNet Modules in Logix5000 Control Systems User Manual (Logix5000 控制系统中的 DeviceNet 模块用户手册, 出版号: DNET-UM004)	提供关于在 Logix5000 控制系统中使用 1756-DNB 模块的信息

资源	说明
EtherNet/IP Modules in Logix5000 Control Systems User Manual (Logix5000 控制系统中的 EtherNet/IP 模块用户手册, 出版号: ENET-UM001)	提供关于在 Logix5000 控制系统中使用 1756-ENBT 模块的信息
ControlNet Modules in Logix5000 Control Systems User Manual (Logix5000 控制系统中的 ControlNet 模块用户手册, 出版号: CNET-UM001)	提供关于在 Logix5000 控制系统中使用 1756-CNB 模块的信息
Logix5000 Controllers Execution Time and Memory Use Reference Manual (Logix5000 控制器执行时间与内存使用参考手册, 出版号: 1756-RM087)	提供关于估计指令的执行时间和内存使用的信息
Logix Import Export Reference Manual (Logix 导入 / 导出参考手册, 出版号: 1756-RM084)	提供关于使用 Logix Designer 导入 / 导出实用工具的信息
Industrial Automation Wiring and Grounding Guidelines (工业自动化布线和接地指南, 出版号: 1770-4.1)	提供安装罗克韦尔自动化工业系统的常规指南。
产品认证网址: http://www.ab.com	提供符合性声明、认证及其他认证详情

可访问 <http://www.rockwellautomation.com/literature/> 查看或下载出版物。
如需订购技术文档的纸印本, 请联系当地的 Allen-Bradley® 经销商或罗克韦尔自动化销售代表。

备注:

安全完整性等级 (SIL) 原理

主题	页码
SIL 3 认证	13
验证测试	14
SIL 3 应用项目的 GuardLogix 架构	15
GuardLogix 系统组件	16
GuardLogix 认证	18
GuardLogix PFD 和 PFH 技术规范	18
安全完整性等级 (SIL) 符合性的分配与权重	19
系统反应时间	19
安全任务周期和安全任务看门狗	20
发生设备故障时的 联络信息	20

SIL 3 认证

GuardLogix 5570 控制器系统已通过型式批准，经认证可在符合 IEC 61508 和 IEC 62061 的高达 (包括) SIL CL3 等级的安全应用项目以及符合 ISO 13849-1 的高达 (包括) PL_e (4 类) 性能等级的安全应用项目中使用。SIL 要求基于认证时的现行标准。

重要事项	当 GuardLogix 控制器处于 “ 运行 ” 或 “ 程序 ” 模式，且应用程序尚未验证时，您应当负责保持安全条件。
------	---

此外，根据 Using ControlLogix in SIL 2 Applications Reference Manual (在 SIL 2 应用项目中使用 ControlLogix 的参考手册，出版号: [1756-RM001](#)) 所述， GuardLogix 控制器内的标准任务可用于标准应用项目或 SIL 2 安全应用项目。在这两种情况下均不得使用 SIL 2 或标准任务和变量来创建更高等级的安全回路。安全任务是经认证唯一用于 SIL 3 应用项目的任务。

使用 Studio 5000 Logix Designer 应用程序来创建 GuardLogix 5570 控制器的程序。

TÜV Rheinland 已经批准 GuardLogix 5570 控制器系统可用于高达 SIL CL3 等级的安全相关应用项目中，在这些应用项目中，断电状态被视为安全状态。本手册中包含的与 I/O 相关的所有示例均基于将断电作为典型机器安全和紧急关机 (ESD) 系统的安全状态这一前提。

重要事项	系统用户负责以下事项： - 对连接至 GuardLogix 系统的所有传感器或执行器进行设置、SIL 等级评定以及验证。 - 项目管理和功能测试 - 对安全系统的访问控制，包括密码处理 - 根据本安全参考手册和 GuardLogix 5570 Controllers User Manual (GuardLogix 5570 控制器用户手册，出版号：1756-UM022) 中的信息，对应用项目和设备配置进行编程
------	--

应用安全功能时，访问权限仅赋予经过培训、富有经验的合格授权人员。在 Logix Designer 应用程序中提供带密码的安全锁定功能。

如需了解关于如何使用安全锁定功能的信息，请参见 GuardLogix 5570 Controllers User Manual (GuardLogix 5570 控制器用户手册，出版号：[1756-UM022](#))。

验证测试

IEC 61508 要求用户执行系统中使用设备的各种验证测试。以用户自定义的时间执行验证测试。例如，验证测试可以每 1 年、每 15 年执行一次，或使用其他合适的时间周期。

GuardLogix 5570 控制器的验证测试时间间隔长达 20 年。系统的其他组件如安全 I/O 设备、传感器和执行器的验证测试时间间隔则较短。控制器应包含在安全系统的其他组件的功能验证测试中。

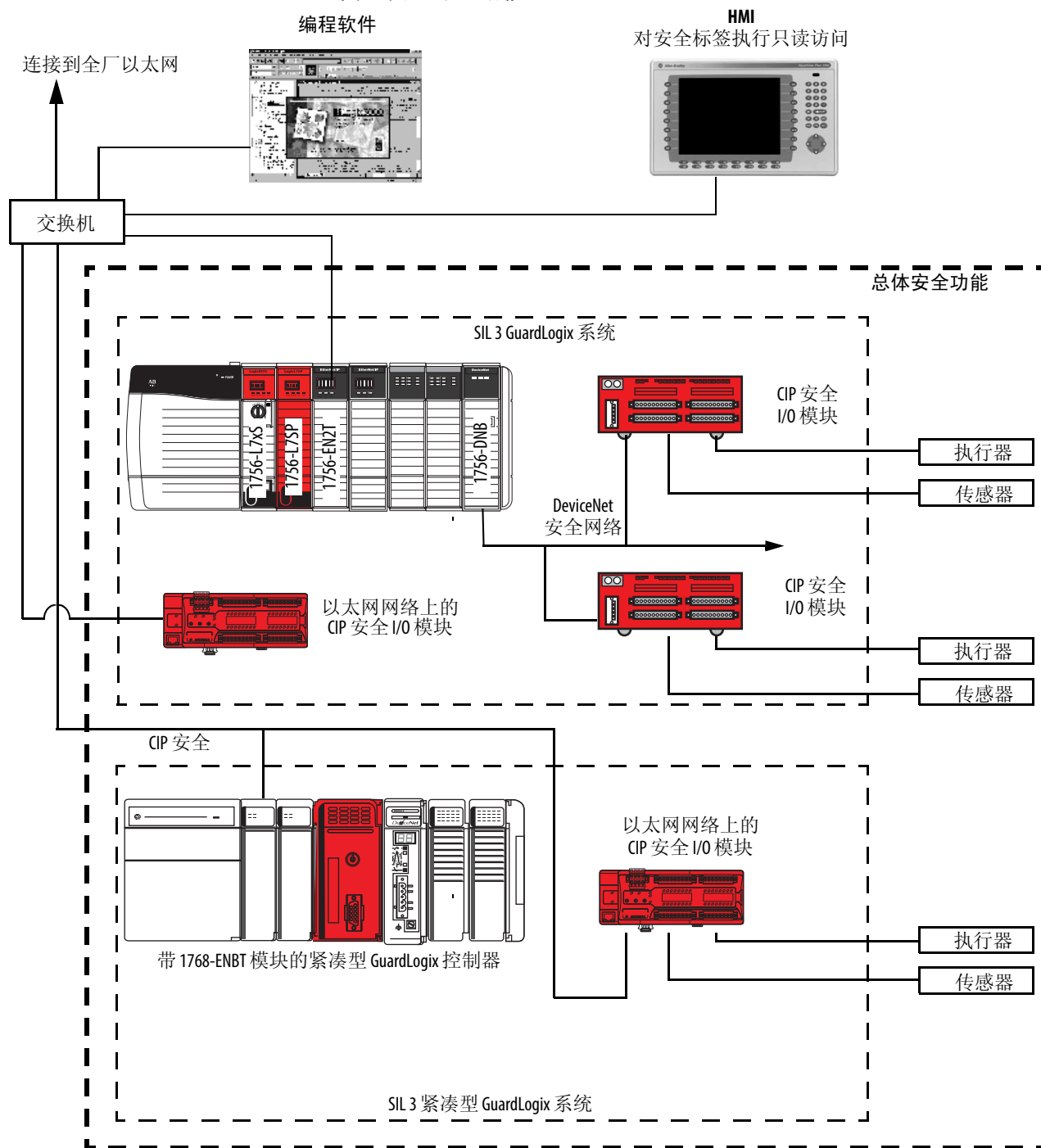
重要事项	验证测试间隔的时间帧取决于具体的应用。然而，这主要与安全 I/O 设备和现场仪表有关。
------	---

SIL 3 应用项目的 GuardLogix 架构

下图显示了一个典型的 SIL 功能，包括以下各项：

- 总体安全功能
- 总体安全功能的 GuardLogix 部分
- 在功能外工作时其他设备的连接方式 (例如, HMI)

图 1- 典型的 SIL 功能



GuardLogix 系统组件

本节中的表格列出了 SIL 3 认证 GuardLogix 组件以及可配合 SIL 3 GuardLogix 系统使用的非 SIL 3 认证组件。

有关 GuardLogix 控制器和 CIP 安全 I/O 设备的认证系列和固件版本的最新列表，请参见

<http://www.rockwellautomation.com/products/certification/safety/>。

在 <http://support.rockwellautomation.com/ControlFLASH™/> 上可获得固件版本信息。

表 2 - SIL 3 认证 GuardLogix 组件

设备类型	目录号	说明	安装说明	相关文档 ⁽³⁾
				用户手册
1756 GuardLogix 主控制器 (ControlLogix5570S)	1756-L71S	带 2 MB 标准内存，1 MB 安全内存的控制器	不适用 ⁽⁴⁾	- 带 Studio 5000 环境，版本 21 或更高版本：1756-UM022 - 带 RSLogix 5000 软件，版本 20 或以下版本：1756-UM020
	1756-L72S	带 4 MB 标准内存，2 MB 安全内存的控制器		
	1756-L73S	带 8 MB 标准内存，4 MB 安全内存的控制器		
	1756-L73SXT	带 8 MB 标准内存，4 MB 安全内存的控制器 (XT)		
1756 GuardLogix 安全伙伴 (ControlLogix5575P)	1756-L7SP	安全伙伴	不适用 ⁽⁴⁾	1756-UM020
	1756-L7SPXT	安全伙伴 (XT)		
1756 GuardLogix 主控制器 (ControlLogix5560S) ⁽¹⁾	1756-L61S	带 2 MB 标准内存、1 MB 安全内存的控制器	不适用 ⁽⁴⁾	1756-UM020
	1756-L62S	带 4 MB 标准内存、1 MB 安全内存的控制器		
	1756-L63S	带 8 MB 标准内存、3.75 MB 安全内存的控制器		
1756 GuardLogix 安全伙伴 (ControlLogix555P) ⁽¹⁾	1756-LSP	安全伙伴	不适用 ⁽⁴⁾	1768-UM002
1768 紧凑型 GuardLogix 控制器 (CompactLogix4xS) ⁽²⁾	1768-L43S	支持两个 1768 模块的控制器	不适用 ⁽⁴⁾	1791DS-UM001
	1768-L45S	支持四个 1768 模块的控制器		
DeviceNet 网络上的 CIP 安全 I/O 模块	有关认证系列和固件版本的最新列表，请参见 http://www.rockwellautomation.com/products/certification/safety/ 上的安全证书		1791DS-IN001 1791DS-IN002 1732DS-IN001	1791DS-UM001
EtherNet/IP 网络上的 CIP 安全 I/O 模块			1791ES-IN001	1791ES-UM001
POINT Guard I/O 模块			不适用 ⁽⁴⁾	1734-UM013
Kinetix 5500 伺服驱动器 (产品目录号以 —ERS2 结尾)	有关认证系列和固件版本的最新列表，请参见 http://www.rockwellautomation.com/products/certification/safety/ 上的安全证书		2198-IN001	2198-UM001

(1) 经认证可与 RSLogix 5000 软件 (版本 14、版本 16 及更高版本) 一起使用。

(2) 经认证可与 RSLogix 5000 软件 (版本 18 及更高版本) 一起使用。

(3) 通过访问 <http://www.rockwellautomation.com/literature>，可从罗克韦尔自动化获取这些出版物。

(4) 有关安装指南，请参见用户手册。

表 3 - 适合与 1756 GuardLogix 控制器安全系统一起使用的组件

设备类型	目录号	说明	系列 ⁽¹⁾	版本 ⁽¹⁾	相关文档 ⁽³⁾		
					安装说明	用户手册	
机架	1756-A4 1756-A7 1756-A10 1756-A13 1756-A17	4 槽机架 7 槽机架 10 槽机架 13 槽机架 17 槽机架	B	不适用	1756-IN005	不适用	
	1756-A4LXT 1756-A5XT 1756-A7XT 1756-A7LXT	4 槽 XT 机架 5 槽 XT 机架 7 槽 XT 机架 7 槽 XT 机架	B	不适用			
电源	1756-PA72	交流电源	C	不适用	1756-IN005	不适用	
	1756-PB72	直流电源	C				
	1756-PA75	交流电源	B				
	1756-PB75	直流电源	B				
	1756-PAXT	交流 XT 电源	B				
	1756-PBXT	直流 XT 电源	B				
通信模块	1756-ENBT 1756-EN2T 1756-EN2F 1756-EN2TR 1756-EN3TR	EtherNet/IP 网桥	A A A C B	3.006 2.005 2.005 10.007 10.007	ENET-IN002	ENET-UM001	
	1756-EN2TXT 1756-EN2TRXT	XT EtherNet/IP 网桥 (铜)	C C	5.007 10.006			
	1734-AENT	POINT I/O 以太网适配器	A	3.001	1734-IN590	1734-UM011	
	1756-DNB	DeviceNet 网桥	A	6.002	DNET-IN001	DNET-UM004	
	1756-CN2	ControlNet 网桥	A	12.001	CNET-IN005	CNET-UM001	
	1756-CN2R	ControlNet 网桥, 冗余介质	A	12.001			
	1756-CN2RXT	XT ControlNet 网桥, 冗余介质	B	20.020			
	编程软件	9324-xxxx	用于 GuardLogix 5560 控制器的 RSLogix 5000 软件	不适用	14 ⁽²⁾	不适用	请参见 在线帮助。
			用于 GuardLogix 5570 (XT) 控制器的 RSLogix 5000 软件		20		
9324-xxxx		用于 GuardLogix 5570 (XT) 控制器的 Studio 5000 环境	21				
存储卡	1784-CF128	用于 GuardLogix 5560 控制器的 128 MB CF 卡	不适用	不适用	不适用	不适用	
	1784-SD1	用于 GuardLogix 5570 控制器的 1 GB 安全数字 (SD) 卡					
	1784-SD2	用于 GuardLogix 5570 控制器的 2 GB 安全数字 (SD) 卡					

(1) 该版本或更高版本。

(2) RSLogix 5000 软件版本 15 不支持 GuardLogix 安全控制器。

(3) 通过访问 <http://www.rockwellautomation.com/literature>, 可从罗克韦尔自动化获取这些出版物。

GuardLogix SIL 3 系统未使用的 SIL 3 系统机架插槽可用于扩展通过低压和 EMC 指令认证的其他 ControlLogix (1756) 模块。

重要事项 只有与其他 Logix-XT 系统组件一起使用得当时, ControlLogix-XT™ 系统组件才能用于极端环境条件。如果将 ControlLogix-XT 组件与传统的 ControlLogix 或 GuardLogix 系统组件一起使用, 将无法满满足极端环境防护等级的要求。

有关“可编程控制 — ControlLogix 产品系列”的证书, 请参见 <http://www.rockwellautomation.com/products/certification/cc/>。

GuardLogix 认证

ControlLogix Controllers Technical Data (ControlLogix 控制器技术数据, 出版号: [1756-TD001](#)) 列出了产品技术规范以及被审批产品的机构认证信息。如果产品已经获得机构认证, 则在产品标签上会打上认证标识。有关符合性声明、证书和其他认证的详细信息, 请参见 <http://www.rockwellautomation.com/products/certification/> 网站的“Product Certification”(产品认证) 链接。

GuardLogix PFD 和 PFH 技术规范

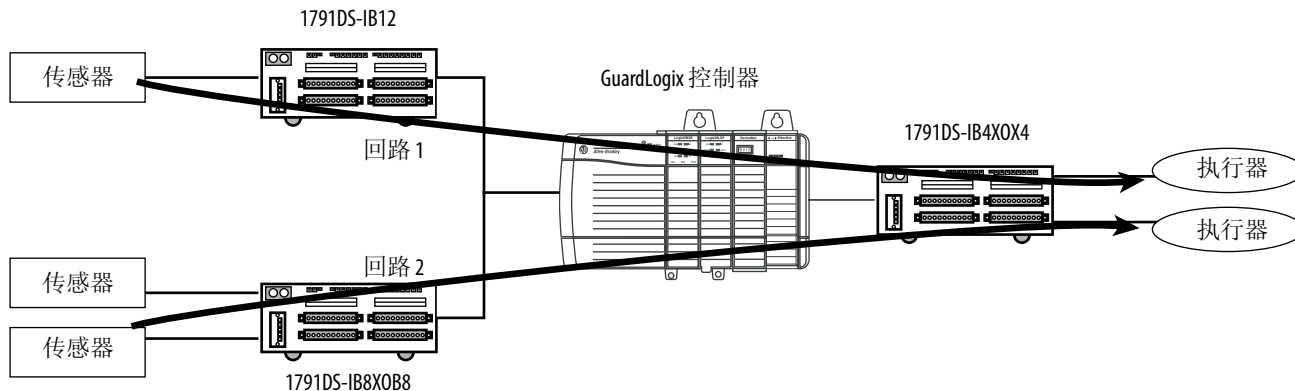
可将安全相关系统分类为在低要求模式下或在高要求 / 连续模式下工作。IEC 61508 对分类进行了量化, 具体说明为: 在低要求模式下操作安全系统的频率要求每年不大于 1 次, 或在高要求 / 连续模式下操作安全系统的频率要求每年大于 1 次。

低要求安全相关系统的安全完整性等级 (SIL) 值直接与其平均故障概率的数量级有关 (以理想地执行所要求的安全功能), 或者简单的说, 与要求故障概率 (PFD) 有关。高要求 / 连续模式安全相关系统的 SIL 值与每小时发生的危险故障概率 (PFH) 直接相关。

PFD 和 PFH 值与构成安全相关系统的三个主要元件相关 (传感器、逻辑元件和执行器)。在逻辑元件内, 还有输入、处理器和输出元件。

对于 PFD 和 PFH 值以及 Guard I/O 模块的验证测试间隔, 请参见附录 E, [GuardLogix 系统安全数据](#)。

图 2 - PFH 示例



为确定 PFH 示例中所示的简单示例系统中的每个安全回路的逻辑元件 PFH，将回路中的每个组件的 PFH 值累加求和。“[安全回路的 PFH 公式](#)”表给出了 PFH 示例图中所示的每个安全回路的 PFH 值的简单计算示例。

表 4- 安全回路的 PFH 公式

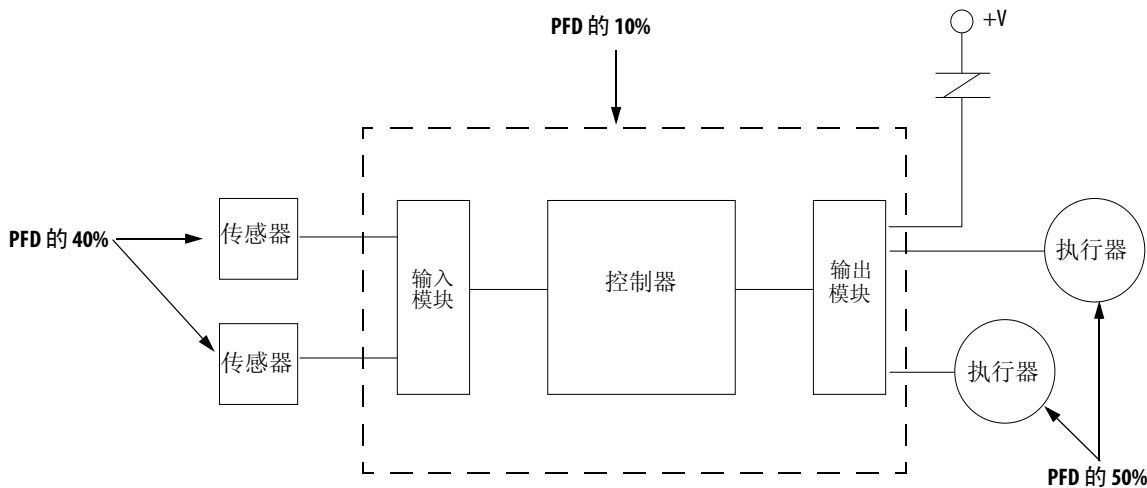
对于以下回路	将以下组件的 PFH 值累加求和
回路 1 的总 PFH =	1791DS-IB12 + GuardLogix 控制器 + 1791DS-IB4XOX4
回路 2 的总 PFH =	1791DS-IB8XOB8 + GuardLogix 控制器 + 1791DS-IB4XOX4

当计算 PFH 值时，必须考虑应用项目的特殊要求，包括测试时间间隔。

安全完整性等级 (SIL)
符合性的分配与权重

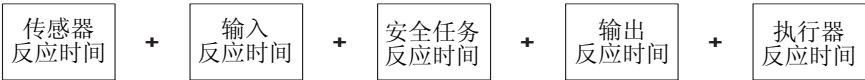
可以保守地假设 GuardLogix 控制器和 I/O 系统增加 10% 的可靠性负担。根据安全相关系统的 SIL 评估，SIL 3 系统可能需要采用关键传感器和输入设备的多路输入以及与双执行器串联的双路输出。

图 3- 可靠性负担



系统反应时间

系统反应时间是指从安全相关事件作为系统的输入到系统将相应的输出设为安全状态之间的时间。系统故障也会影响系统的反应时间。系统反应时间是下列反应时间之和。



每个反应时间都随各种因素而发生变化，例如，I/O 设备的类型和程序中使用的指令。

安全任务反应时间

安全任务反应时间是指从控制器获取任何输入变化到输出生产者设置好已处理输出之间的最大延时。它小于或等于安全任务周期和安全任务看门狗之和。

安全任务周期和安全任务看门狗

安全任务周期是安全任务执行的时间间隔。

安全任务看门狗是允许的最长安全任务处理时间。如果安全任务处理时间超过安全任务看门狗时间，则控制器中会发生不可恢复的安全故障，输出自动跳转到安全状态(断开)。

定义安全任务看门狗时间时，必须使该时间小于或等于安全任务周期。

安全任务看门狗时间在 Logix Designer 应用程序的任务属性窗口中设置。该数值可以在线修改，与控制器模式无关，但当控制器处于安全锁定状态或一旦创建了安全任务签名时，则无法修改该数值。

发生设备故障时的 联络信息

如果有任何 SIL 3 认证设备发生故障，请联系当地的 Allen-Bradley 经销商，采取以下措施：

- 您可将设备退回罗克韦尔自动化，以正确记录受影响的产品目录号的故障，并生成故障记录。
- 您可请求故障分析(必要时)，尝试确定故障原因。

GuardLogix 控制器系统

主题	页码
GuardLogix 5570 控制器 硬件	21
CIP 安全协议	22
安全 I/O 设备	23
通信网桥	23
编程概述	25

有关适用于安全完整性等级 (SIL) 3 应用项目的组件的简要列表，请参见第 16 页上的表格。如需了解更多详细信息和最新信息，请参见 <http://www.rockwellautomation.com/products/certification/safety/>。

在安装 GuardLogix 5570 控制器时，应遵照 GuardLogix 5570 Controllers User Manual (GuardLogix 5570 控制器用户手册，出版号：[1756-UM022](#)) 中的信息。

GuardLogix 5570 控制器 硬件

GuardLogix 控制器由一个主控制器 (ControlLogix 557xS) 和一个安全伙伴 (ControlLogix 557SP) 组成。这两个模块使用 1oo2 架构来创建符合 SIL 3 等级的控制器。下文对此进行了描述。

主控制器和安全伙伴执行控制器中所有安全相关组件的上电和运行时功能诊断测试。

如需了解状态指示灯操作的详细信息，请参见 GuardLogix 5570 Controllers User Manual (GuardLogix 5570 控制器用户手册，出版号：[1756-UM022](#))。

重要事项	状态指示灯并非用于安全功能的可靠指示。仅在调试或故障处理期间将它们用于常规诊断。不得尝试使用状态指示灯来确定运行状态。
------	---

有关 GuardLogix 安全控制器产品目录号列表，请参见第 16 页的表 2。有关适用于安全应用项目的标准 ControlLogix 组件列表，请参见第 17 页的表 3。

主控制器

主控制器是一种处理器，用于执行标准和安全控制功能，并与安全伙伴通信，以实现 GuardLogix 控制系统中的安全相关功能。主控制器包含中央处理器、I/O 接口和内存。

安全伙伴

为了满足 SIL 3 要求，必须在紧靠主控制器右侧的插槽中安装一个安全伙伴。安全伙伴是一种协同处理器，它为系统中的安全相关功能提供冗余。

主控制器配置安全伙伴。只需要将用户程序下载到主控制器一次。安全伙伴的运行模式由主控制器控制。

机架

机架提供模块和 1756 GuardLogix 系统之间的物理连接。任何故障（虽然不太可能发生）均被检测为系统中一个或多个有源组件的故障。因此，机架与安全讨论无关。

GuardLogix-XT™ 控制器必须使用 ControlLogix-XT 机架才能实现极端环境防护等级。

电源

ControlLogix 电源的 SIL 3 操作不需要附加配置或接线。任何故障均被检测为 GuardLogix 系统中一个或多个有源组件的故障。因此，电源与安全讨论无关。

GuardLogix-XT 控制器必须使用 ControlLogix-XT 电源才能实现极端环境防护等级。

CIP 安全协议

GuardLogix 控制器之间的安全相关通信通过生产者和消费者安全标签来实现。这些安全标签使用 CIP 安全协议，用于在通信期间保持数据的完整性。

如需了解关于安全标签的更多信息，请参见[章节 5，安全标签、安全任务和安全程序的特性](#)。

安全 I/O 设备

如需了解与 GuardLogix 控制器一起使用的 CIP 安全 I/O 设备的信息，[请参见章节 3](#)。

通信网桥

[表 5](#) 列出了可用于在 EtherNet/IP、DeviceNet 和 ControlNet 网络上通过 CIP 安全协议进行通信的通信接口模块。

表 5 - 系统的通信接口模块

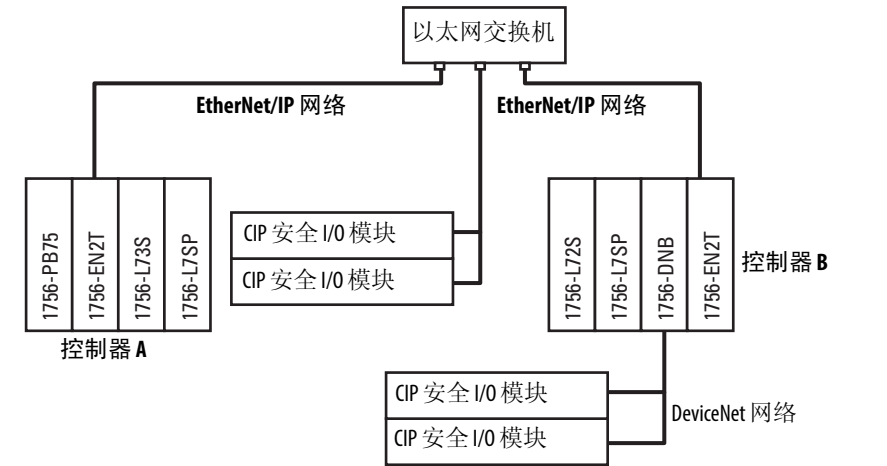
GuardLogix 系统	通信模块
1756	• 1756-ENBT、1756-EN2T(R)、1756-EN2F 或 1756-EN3TR EtherNet/IP 网桥 • 1734-AENT POINT I/O 以太网适配器 • 1756-DNB DeviceNet 网桥 • 1756-CN2 ControlNet 网桥 • 1756-CN2R 冗余 ControlNet 网桥
1756 -XT	• 1756-EN2TXT、1756-EN2TRXT EtherNet/IP 网桥 - XT (铜) • 1756-CN2RXT 冗余 XT ControlNet 网桥
1768	• 1768-ENBT • 1734-AENT POINT I/O 以太网适配器 • 1768-CNB • 1768-CNBR

重要事项 由于 CIP 安全控制系统的设计，CIP 安全网桥设备和表中所列网桥一样，不需要通过 SIL-3 认证。

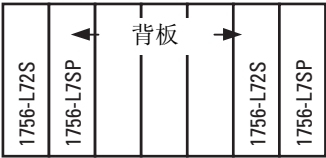
EtherNet/IP 网络

GuardLogix 控制器之间的对等安全通信可通过在 EtherNet/IP 网络上使用 EtherNet/IP 网桥来实现。EtherNet/IP 网桥允许 GuardLogix 控制器控制 EtherNet/IP 网络上的 CIP 安全 I/O 设备并与其交换安全数据。

图 4 - 通过 EtherNet/IP 网桥和 EtherNet/IP 网络进行的对等通信



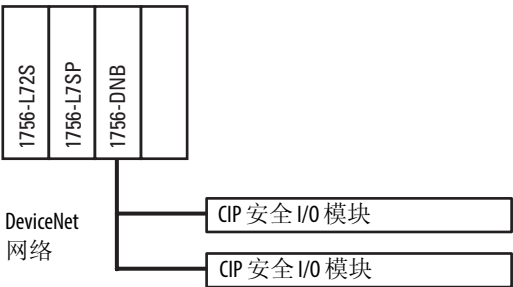
提示 也可通过背板在同一个机架中的两个 GuardLogix 控制器之间实现对等安全通信。



DeviceNet 安全网络

DeviceNet 网桥允许 GuardLogix 控制器控制 DeviceNet 网络上的 CIP 安全 I/O 模块并与其交换安全数据。

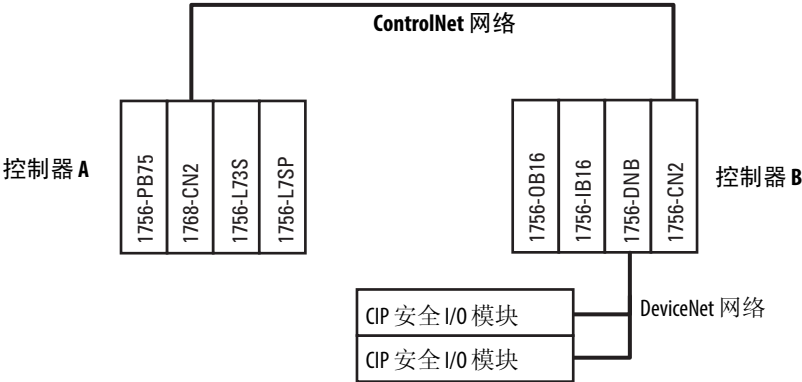
图 5 - 通过 DeviceNet 网桥进行通信



ControlNet 网络

ControlNet 网桥允许 GuardLogix 控制器通过 ControlNet 网络与其他 GuardLogix 控制器或远程 CIP 安全 I/O 网络相互生产和消费安全标签。

图 6 - 通过 ControlNet 网桥进行通信



编程概述

使用 Studio 5000 Logix Designer 应用程序对 GuardLogix 5570 控制器进行编程。

使用 Logix Designer 应用程序定义 I/O 设备和控制器的位置、所属关系和配置以及创建、测试和调试程序逻辑。在 GuardLogix 安全任务中仅支持继电器梯形图逻辑。

如需了解安全项目可用的逻辑指令集的信息，请参见[附录 A](#)。

授权人员可以更改安全程序，但只能使用第 59 页的“[编辑安全应用项且](#)”中所述的其中一种过程。

备注:

GuardLogix 控制系统的 CIP 安全 I/O

主题	页码
概述	27
CIP 安全 I/O 设备的典型安全功能	27
反应时间	28
CIP 安全 I/O 设备的安全注意事项	29

概述

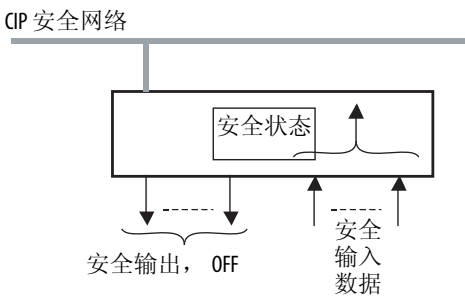
在操作包含 CIP 安全 I/O 设备的 GuardLogix 5570 安全系统之前，必须阅读、了解并遵照在第 16 页“[SIL 3 认证 GuardLogix 组件](#)”表中列出的出版物所提供的安装、操作和安全信息。

CIP 安全 I/O 设备可以连接至安全输入和输出设备 (例如，传感器和执行器)，允许由 GuardLogix 控制器监视这些设备。对于安全数据，通过安全连接使用 CIP 安全协议来执行 I/O 通信；安全逻辑则在 GuardLogix 控制器中处理。

CIP 安全 I/O 设备的典型安全功能

CIP 安全 I/O 设备将以下状态视为安全状态处理：

- 安全输出：OFF
- 到控制器的安全输入数据：OFF



将 CIP 安全 I/O 设备用于当安全输出变为 OFF 时，处于安全状态的应用项目。

诊断

当接通电源时，CIP 安全 I/O 设备执行自诊断，并在操作期间定期执行自诊断。如果检测到诊断故障，则将安全输入数据（输入到控制器）和本地安全输出设为其安全状态 (OFF)。

状态数据

除安全输入和输出数据外，CIP 安全 I/O 设备还支持状态数据以监视设备和 I/O 电路是否正常。如需了解特定产品功能，请参见设备的产品文档。

状态指示灯

CIP 安全 I/O 设备包括状态指示灯。如需了解关于状态指示灯操作的详细信息，请参见特定设备的产品文档。

接通或断开延时功能

某些 CIP 安全 I/O 设备可能支持输入信号的接通延时和断开延时功能。根据应用项目的不同，计算系统反应时间时，可能需要将断开延时、接通延时或两者同时包括在内。

如需了解系统反应时间的信息，请参见[附录 C](#)。

反应时间

输入反应时间是从输入终端上的信号发生变化到将安全数据发送到 GuardLogix 控制器之间的时间。

输出反应时间是从 GuardLogix 控制器接收安全数据到输出终端改变状态之间的时间。

如需了解关于确定输入和输出反应时间的信息，请参见特定 CIP 安全 I/O 设备的产品文档。

如需了解关于计算系统反应时间的信息，请参见[附录 C](#)。

CIP 安全 I/O 设备的安全注意事项

如有必要，在安全网络上安装各设备之前，必须使用一个节点或 IP 地址来调试所有设备和通信速率。

所属关系

GuardLogix 系统中的每个 CIP 安全 I/O 设备分别属于各个 GuardLogix 控制器。可根据需要使用多个 GuardLogix 控制器和多个 CIP 安全 I/O 设备，对机架或网络没有限制条件。当一个控制器拥有一个 I/O 设备时，它按用户定义来存储设备的配置数据。该配置控制设备在系统中的工作方式。

从控制角度看，安全输出设备只能由一个控制器控制。每个安全输入设备也从属于单个控制器；但是，安全输入数据可以由多个 GuardLogix 控制器共享（消费）。

安全 I/O 配置签名

配置签名定义了设备配置。可以读取并监视签名。配置签名是用于识别设备配置的唯一签名。当使用 GuardLogix 控制器时，无需监视该签名。GuardLogix 控制器自动监视签名。

安全 I/O 设备更换

替换安全设备要求正确配置替换设备，且用户必须验证替换设备的操作。

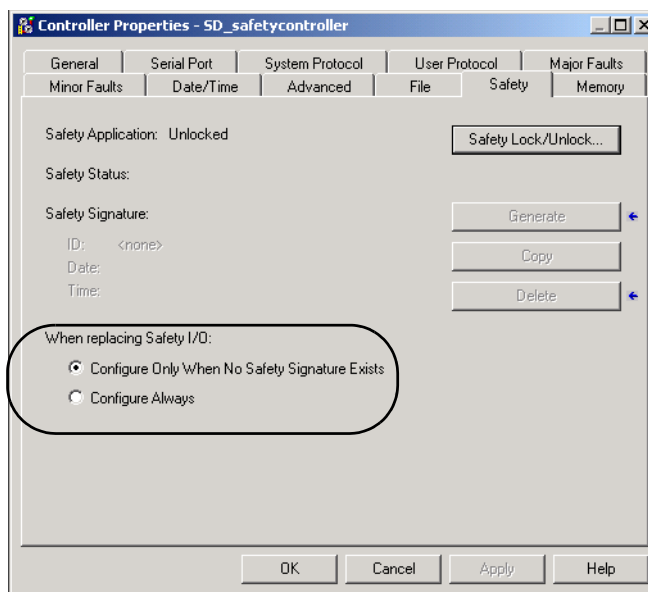


注意：在设备替换或功能测试期间，系统的安全性不得依赖于受影响设备的任何一部分。

在 Logix Designer 应用程序 Controller Properties (控制器属性) 对话框的 Safety (安全) 选项卡中提供了用于 I/O 设备替换的两个选项：

- Configure Only When No Safety Signature Exists (仅当不存在安全签名时配置)
- Configure Always (始终配置)

图 7- 安全 I/O 替换选项



Configure Only When No Safety Signature Exists (仅当不存在安全签名时配置)

该设置表示只有在安全任务没有安全任务签名，且替换设备处于出厂状态时，即安全设备中不存在安全网络编号时， GuardLogix 控制器才配置安全设备。

如果安全任务带有一个安全任务签名，则只有在以下条件为真时 GuardLogix 控制器才会配置替换 CIP 安全 I/O 设备：

- 设备已经具有正确的安全网络编号。
- 设备的电子匹配功能正确。
- 节点或 IP 地址正确。

Configure Always (始终配置)

如果设备处于出厂状态，即替换安全设备中不存在安全网络编号，且节点编号与 I/O 设备匹配功能与控制器配置一致，则 GuardLogix 控制器将始终尝试配置替换 CIP 安全 I/O 设备。



注意：只有在设备的替换和功能测试期间，不依赖可选路由的整个 CIP 安全控制系统来保持 SIL 3 特性时，才启用 Configure Always (始终配置) 功能。

如果依赖 CIP 安全控制系统的其它部分来保持 SIL 3，则确保禁用控制器的 Configure Always (始终配置) 功能。

您应当负责执行一个过程来确保在设备替换期间保持正确的安全功能。



注意：除遵循 GuardLogix5570 Controllers User Manual (GuardLogix5570 控制器用户手册，出版号：[1756-UM022](#)) 中给出的设备替换步骤外，在启用了 Configure Always (始终配置) 功能时，不得将处于出厂状态的任何设备置于任何 CIP 安全网络上。

备注:

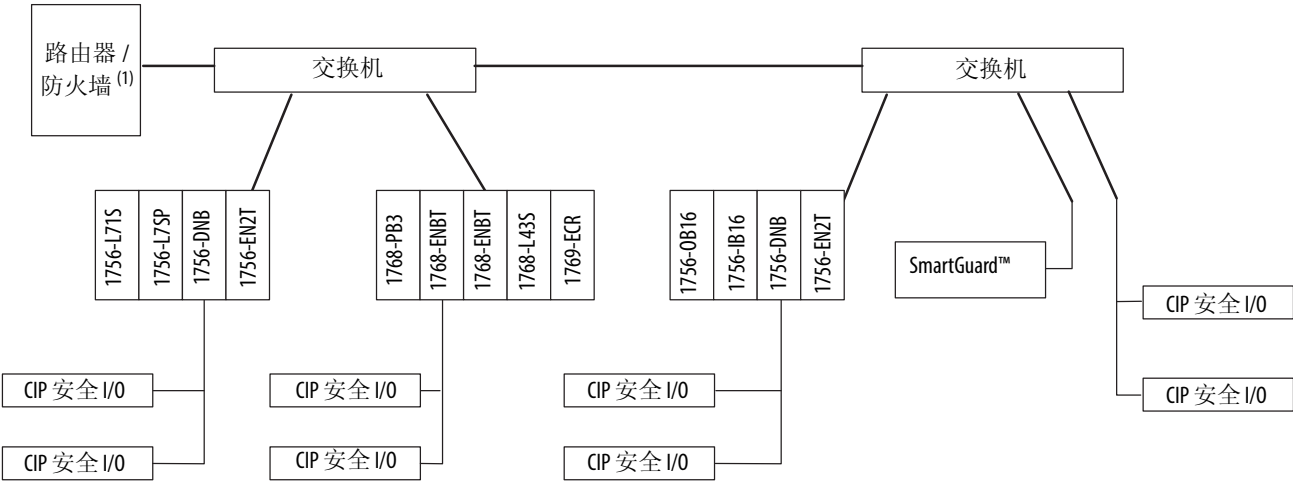
CIP 安全和安全网络编号

主题	页码
可路由 CIP 安全控制系统	33
分配安全网络编号 (SNN) 时需考虑的因素	35

可路由 CIP 安全控制系统

为了解 CIP 安全控制系统以及安全网络编号 (SNN) 的安全要求，您必须首先了解 CIP 控制系统中的通信路由方式。CIP 安全控制系统表示一组互连的 CIP 安全设备。可路由系统表示在 CIP 安全控制系统内从发信端到目标端的数据包潜在错误路由的范围。系统会进行隔离，确保没有其他连接接入系统。例如，由于下面图 8 的系统无法通过一个更大的全厂以太网主干网互连到其他 CIP 安全系统，因此，它给出了一个可路由 CIP 安全系统的范围。

图 8 - CIP 安全系统示例



(1) 配置路由器或防火墙来限制流量。

唯一节点参考

CIP 安全协议是一种终端节点到终端节点的安全协议。CIP 安全协议允许通过非认证网桥、交换机和路由器将 CIP 安全报文发送到 CIP 安全设备或从 CIP 安全设备接收 CIP 安全报文。

为防止非认证网桥、交换机或路由器出错而导致危险，可路由 CIP 安全控制系统内的每个终端节点必须有一个唯一的节点参考。该唯一的节点参考是安全网络编号 (SNN) 和节点的节点地址的组合。

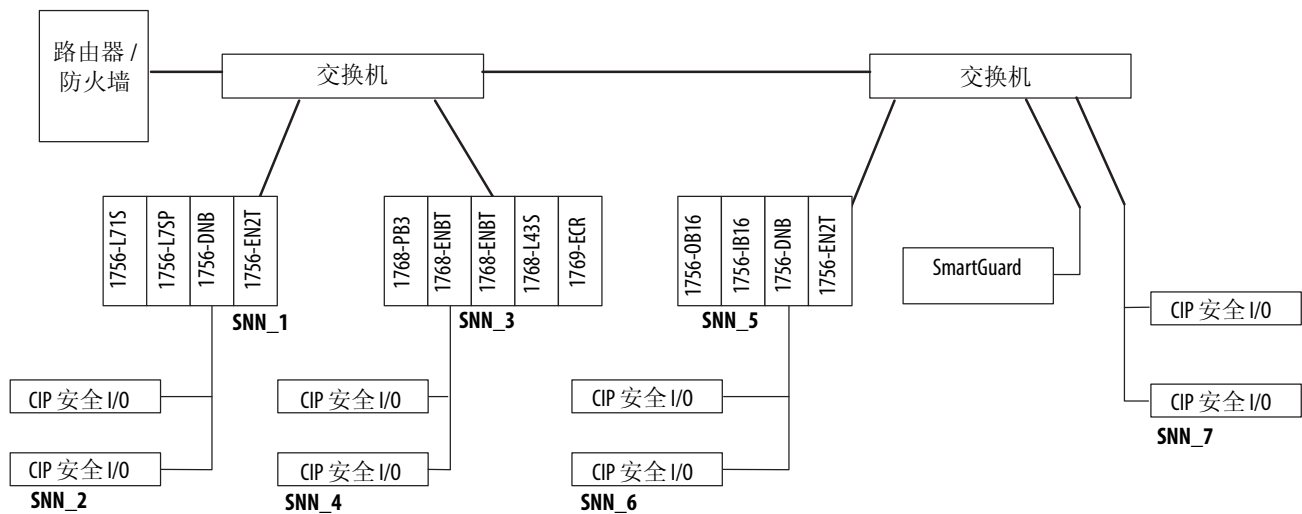
安全网络编号

安全网络编号 (SNN) 由软件自动分配或由用户手动分配。包含安全 I/O 节点的各 CIP 安全网络必须至少有一个唯一 SNN。包含一个或多个安全设备的各机架必须至少有一个唯一的 SNN。分配给每个安全网络或网络子网的安全网络编号必须唯一。

提示

可以将多个 SNN 分配给 CIP 安全子网或包含多个安全设备的机架。但是，为了简单起见，建议每个 CIP 安全子网配有且只有一个唯一的 SNN。该建议同样适用于每个机架。

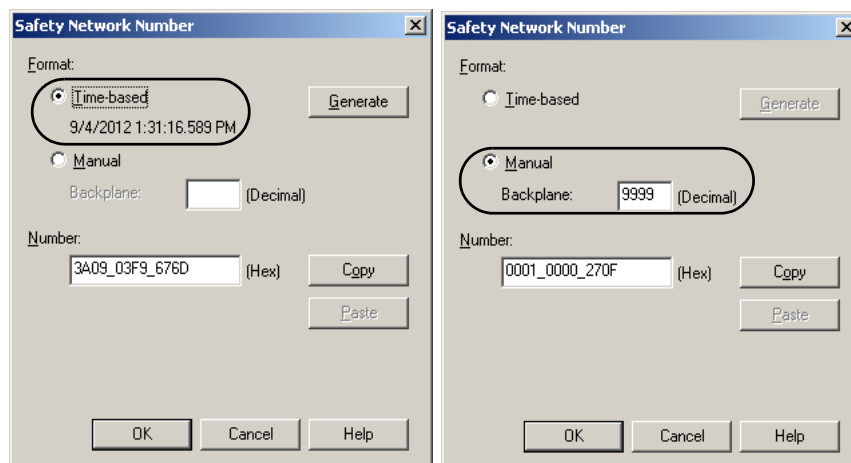
图 9 - 带多个 SNN 的 CIP 安全示例



每个 CIP 安全设备必须配置一个 SNN。必须使用目标设备的 SNN 来配置向另一个安全设备发起安全连接的任何设备。如果在执行系统的功能安全测试之前，CIP 安全系统处于启动过程，则发出端设备可用于设置设备的唯一节点参考。

系统使用的 SNN 是一个 6 字节的十六进制数。可以用两种格式之一设置和查看 SNN：基于时间或手动。当选择基于时间的格式时，SNN 表示当地日期和时间。当选择手动格式时，SNN 表示网络类型和一个范围为 1...9999 的十进制数值。

图 10 - SNN 格式



当创建新的 GuardLogix 安全控制器项目并添加新的安全 I/O 设备时，自动分配基于时间的 SNN。

在以下情况下要求手动分配 SNN：

- 当使用安全消费者标签时
- 如果项目消费的安全输入数据来自于配置为其他安全设备所拥有的设备
- 当将安全项目复制到同一个可路由 CIP 安全系统内的另一个硬件装置时

重要事项	如果手动分配 SNN，请务必十分小心，确保系统扩展不会导致 SNN 和节点地址组合重复。如果项目包含重复的 SNN 和节点地址组合，将发生校验错误。
-------------	--

分配安全网络编号 (SNN) 时需考虑的因素 SNN 的分配取决于多个因素，包括控制器或 CIP 安全 I/O 设备的配置。

安全消费者标签的安全网络编号 (SNN)

当将包含生产者安全标签的安全控制器添加到 I/O 配置树形目录时，必须输入生产控制器的 SNN。可以从生产控制器项目复制 SNN，然后将其粘贴到已添加到 I/O 配置树形目录的新控制器中。

如需了解关于如何复制和粘贴 SNN 的信息，请参见 GuardLogix 5570 Controllers User Manual (GuardLogix 5570 控制器用户手册，出版号：[1756-UM022](#))。

出厂设备的安全网络编号 (SNN)

出厂 CIP 安全 I/O 设备没有 SNN。当拥有设备的 GuardLogix 控制器将配置发送到该设备时，SNN 即被设置。

重要事项

若要将 CIP 安全 I/O 设备添加到一个已配置的 GuardLogix 系统 (SNN 位于 GuardLogix 控制器中)，替换 CIP 安全 I/O 设备必须具备正确的 SNN，然后才能将其添加到 CIP 安全网络上。

带不同配置宿主的安全设备的安全网络编号 (SNN)

当 CIP 安全 I/O 设备属于另一个 GuardLogix 控制器 (控制器 B)，然后将其添加到其他 GuardLogix 项目 (控制器 A 项目) 时，Logix Designer 应用程序根据当前项目分配 SNN。由于当前项目 (控制器 A 项目) 不是真正的配置拥有者，因此需要将原始 SNN (控制器 B 项目) 复制到控制器 A 项目的配置中。通过标准的复制和粘贴命令可以轻松完成该操作。结果是 CIP 安全 I/O 设备同时向两个 GuardLogix 控制器生成数据。最多可以复制和粘贴 16 个控制器。

如需了解关于如何更改、复制和粘贴 SNN 的信息，请参见 GuardLogix 5570 Controllers User Manual (GuardLogix 5570 控制器用户手册，出版号：[1756-UM022](#))。

复制安全项目时的安全网络编号 (SNN)



注意：如果复制一个安全项目以用于具有不同硬件的其他项目或用于其他物理位置，且新项目位于同一可路由 CIP 安全系统中，则必须在第二个系统中更改每个 SNN。SNN 值不得重复。

如需了解关于更改 SNN 的信息，请参见 GuardLogix 5570 Controllers User Manual (GuardLogix 5570 控制器用户手册，出版号：[1756-UM022](#))。

安全标签、安全任务和安全程序的特性

主题	页码
标准与安全之间的区别	37
SIL 2 安全应用项目	38
SIL 3 安全 — 安全任务	41
使用人机界面	43
安全程序	45
安全例程	45
安全标签	46

标准与安全之间的区别 由于采用的是 Logix 系列控制器，可在 GuardLogix 控制系统中同时使用标准 (非安全相关) 和安全相关组件。

可通过 GuardLogix 项目内的标准任务执行标准自动化控制。GuardLogix 控制器提供与其他 ControlLogix 系列控制器相同的功能。GuardLogix 控制器与标准控制器的区别在于它能提供符合 SIL 3 等级的安全任务。

然而，在应用项目的标准部分和安全相关部分之间要求提供一个逻辑且清晰可见的区别。Logix Designer 应用程序通过安全任务、安全程序、安全例程、安全标签和安全 I/O 设备来区别。可通过 GuardLogix 控制器的安全任务实现 SIL 2 和 SIL 3 级别的安全控制。

SIL 2 安全应用项目

可使用 GuardLogix 控制器的安全任务来执行 SIL 2 安全控制。

由于 GuardLogix 控制器是 ControlLogix 系列处理器的一部分，可通过 GuardLogix 控制器使用标准任务或安全任务执行 SIL 2 安全控制。由于大部分应用项目的 SIL 2 安全功能的百分比高于 SIL 3 安全功能，该功能提供唯一且多功能的安全控制选项。

安全任务中的 SIL 2 安全控制

GuardLogix 安全任务可用于提供 SIL 2 和 SIL 3 安全功能。如果需要同时执行 SIL 3 安全功能和 SIL 2 安全功能，则必须满足本章“[SIL 3 安全 — 安全任务](#)”、“[安全程序](#)”和“[安全例程](#)”部分规定的要求以及本节列出的 SIL 2 要求。

SIL 2 安全逻辑

从 GuardLogix 安全控制角度看，SIL 2 和 SIL 3 安全相关设备之间的最大区别在于 SIL 2 通常是单通道，而 SIL 3 通常是双通道。当使用 Guard 安全相关 I/O (红色模块) (要求在安全任务中使用) 时，SIL 2 安全输入可以是单通道，这有助于降低复杂度和减少所需的模块数量。

安全系统设计者将确保正确实施所有安全功能。必须考虑以下因素：

- 现场设备选型 (正确选型，识别和消除所有设备故障)
- 考虑安全需求 (低需求 IEC 61511 或高需求 ISO 13849)
- 考虑测试时间间隔 (满足应用项目要求所需的诊断和验证测试)
- 通过正确的文档来识别和证实所使用的任何故障排除措施

重要事项

如果在安全任务内同时使用 SIL 2 和 SIL 3 安全功能的组合，则必须防止 SIL 2 输入信号直接控制 SIL 3 安全功能。使用特定的安全任务程序或例程分隔 SIL 2 和 SIL 3 安全功能。

在安全任务内，Logix Designer 应用程序包含一组安全相关的梯形图逻辑指令。GuardLogix 控制器还具有针对特定应用的 SIL 3 级安全指令。所有这些逻辑指令可以在 Cat 1...4 和 SIL 1...3 安全功能中使用。

对于只采用 SIL 2 安全功能的情况，不要求使用安全任务签名。但是，如果在安全任务内使用任意一个 SIL 3 安全功能，则要求使用安全任务签名。

对于 SIL 2 应用项目，我们建议您在完成测试后立即安全锁定安全任务。锁定安全任务后会启用更多的安全功能。还可使用 FactoryTalk® Security 和 Logix Designer 例程源代码保护功能来限制对安全相关逻辑的访问。

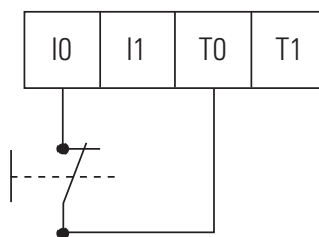
如需了解关于如何生成安全任务签名和安全锁定安全任务的更多信息，请参见 GuardLogix 5570 Controllers User Manual (GuardLogix 5570 控制器用户手册，出版号：[1756-UM022](#))。

SIL 2 安全输入

CompactBlock™ Guard I/O (1791 系列)、ArmorBlock® Guard I/O (1732 系列) 和 POINT Guard I/O (1734 系列) 安全输入模块支持单通道 SIL 2 安全输入电路。由于这些模块也可用于 SIL 3 操作，倘若您遵照这些准则，则允许在同一个模块上组合使用 SIL 2 和 SIL 3 电路。

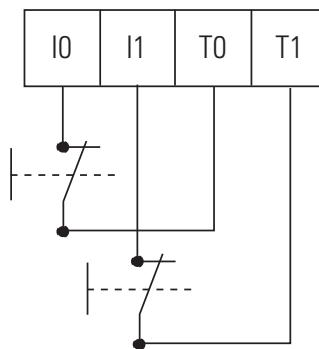
以下两个接线示例显示了如何将 SIL 2 安全电路连接到 Guard I/O 安全输入模块。这些示例使用位于所有 1791 和 1732 安全输入模块上的板载测试源 (T0...Tx)。

图 11- 输入接线



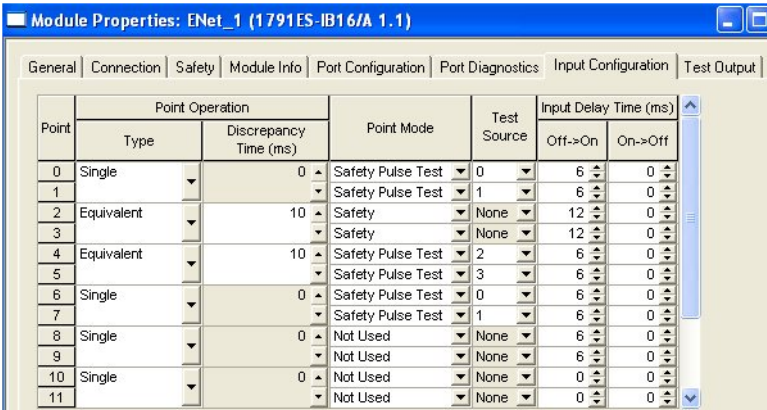
成对的 Guard I/O 模块组输入用于实现 Cat 3、Cat 4 和 SIL 3 安全功能。当在 Cat 1、Cat 2 和 SIL 2 安全功能中使用，模块输入仍应按图示成对使用。图中显示两个 SIL 2 安全功能，分别使用测试源 T0 和 T1 将它们连接至输入 I0 和 I1。

图 12- 成对输入接线



对于 Cat 1、Cat 2 和 SIL 2 安全功能，Guard I/O 安全模块需要在 GuardLogix 项目内进行特定配置。在该示例中，输入 0、1、6、7、8、9、10 和 11 属于 Cat 1、2 或 SIL 2 安全功能的一部分。输入 2、3、4、5 属于 Cat 3、Cat 4 或 SIL 3 安全功能的一部分。

图 13 - 输入配置



字段	值
类型	Single (单一)
Discrepancy Time (差异时间)	不适用
Point Mode (点模式)	Safety Pulse Test (安全脉冲测试)
Test Source (测试源)	根据现场设备与模块的物理连接方式来设置数值。为确保测试源正确启用，请打开并查看 Test Output (测试输出) 选项卡上的设置。
Input Delay Time (输入延时)	由用户基于现场设备特性输入内容

重要事项	板载脉冲测试输出 (T0...Tx) 通常与具有机械触点的现场设备一起使用。如果使用了带电子输出的安全设备 (馈送安全输入)，则它们必须具有合适的安全级别。
------	--

重要事项	如果使用 GuardLogix 安全应用项目指令，请确保将安全输入模块配置成单一模块，而不是同等或互补模块。这些指令可以提供 PLd (Cat. 3) 或 PLe (Cat. 4) 安全功能所需的所有双通道功能。 参见 GuardLogix Safety Application Instruction Set Reference Manual (GuardLogix 安全应用项目指令集参考手册，出版号：1756-RM095)。
------	---

标准任务中的 SIL 2 安全控制

由于 ControlLogix 系列控制器内置了优质而又丰富的诊断功能，您可在标准任务内执行 SIL 2 安全功能。这也适用于 GuardLogix 控制器。

若要在 GuardLogix 标准任务内执行 SIL 2 安全控制，必须遵照 Using ControlLogix in SIL 2 Applications Safety Reference Manual (在 SIL 2 应用项目中使用 ControlLogix 的安全参考手册，出版号：[1756-RM001](#)) 中规定的要求。

SIL 3 安全 — 安全任务

创建 GuardLogix 项目时会自动创建一个安全任务。该安全任务具有以下附加特性：

- GuardLogix 控制器是唯一支持安全任务的控制器。
- 安全任务无法删除。
- GuardLogix 控制器支持单个安全任务。
- 在安全任务内，可使用由多个安全例程组成的多个安全程序。
- 在安全任务内不能调度或执行标准例程。

安全任务是一种周期性定时任务，它具有用户可选择的任务优先级和看门狗。在大多数情况下，控制器的最高优先级是安全任务，并且必须将用户自定义的程序看门狗设置成能容许安全任务执行期间的波动。

安全任务限制条件

用户指定安全任务周期和安全任务看门狗。安全任务周期是安全任务执行的周期。安全任务看门狗是从所调度的安全任务开始执行到任务完成所允许的最大时间。

如需了解关于安全任务看门狗的更多信息，请参见[附录 C](#)，[反应时间](#)。

安全任务周期被限制为最大 500 ms，且不能在线修改。请确保安全任务在被再次触发之前具有足够的时间来完成。如果上一次触发的安全任务仍在执行期间又被触发，则会发生安全任务看门狗超时，这是 GuardLogix 控制器中一种不可恢复的安全故障。

如需了解更多信息，请参见[附录 7](#)，[监视状态和处理故障](#)。

安全任务执行细节

除下列内容外，安全任务的执行方式与标准周期性任务的执行方式相同：

- 安全任务在主控制器和安全伙伴建立控制伙伴关系且协调系统时间 (CST) 同步后才开始执行。而标准任务则在控制器跳转到“运行”模式后立即开始执行。
- 虽然安全输入和安全消费者标签的请求数据包间隔 (PRI) 的可配置范围为 6...500 ms，但只有在开始执行安全任务时才更新安全输入标签和安全消费者标签。这表示即使 I/O RPI 快于安全任务周期，数据在安全任务执行期间也不发生改变。只有在安全任务开始执行时会读取一次数据。
- 在开始执行安全任务时，安全输入值被冻结。因此，在执行单个安全任务时不更新与定时器相关的指令，如 TON 和 TOF。它们在各任务执行期间将保持精确的时间，但累计时间在执行安全任务过程中将不发生改变。



注意：该特性有别于标准 Logix 任务执行，但与 PLC 或 SLC™ 特性类似。

- 对于映射到安全标签的标准标签，在安全任务开始时将标准标签值复制到安全内存，且标签值在执行安全任务期间保持不变。
- 在安全任务执行结束时更新安全输出标签（输出和生产者）值。
- 安全任务以指定的时间间隔响应模式变化（例如，从“运行”变为“程序”或从“程序”变为“运行”）。因此，安全任务执行模式跳转可能需要一个以上任务周期，但通常小于两个周期。

重要事项

当安全解锁且没有安全任务签名时，控制器会防止安全任务和通信命令对安全内存同时执行写访问。因此，在通信更新完成之前，安全任务可保持关闭。更新所需的时间因标签大小而异。因此，可能发生安全连接和安全看门狗超时。（例如，如果在将安全任务速率设为 1 ms 时执行在线编辑，则会发生安全看门狗超时）。

为了补偿因通信更新引起的保持关闭时间，应将安全看门狗时间增加 2 ms。

当控制器被安全锁定或存在安全任务签名时，不会发生本注意事项中所述的情况。

使用人机界面

在 SIL 级别 GuardLogix 系统中使用 HMI 设备时，应遵照以下预防措施和指南。

预防措施

您必须在 HMI 设备上采取预防措施并实施特定的技术。这些预防措施包括但不限于以下内容：

- 受限访问和安全性
- 技术规范、测试和验证
- 关于数据和访问的限制
- 关于数据和参数的限制

如需了解关于如何使 HMI 设备适应典型 SIL 回路的更多信息，请参见 [第 15 页的图 1](#)。

在 HMI 和控制器内的应用软件中使用适当的技术。

访问安全相关系统

HMI 相关功能包括两项主要操作：读数据和写数据。

读取安全相关系统中的参数

读数据不受限制，因为读取不影响安全系统的特性。但是，所读取数据的数量、频率和大小会影响控制器的可用性。为避免出现安全相关的误跳闸，应通过良好的通信惯例来限制通信处理对控制器造成的影响。不得将读速率设为最大可能的速率。

更改 SIL 级别系统中的参数

只有在以下限制条件下才允许通过一个外部（即在安全回路外）设备（例如，HMI）对安全相关回路的参数进行更改：

- 只有经过专门培训的授权人员（操作员）才能通过 HMI 更改安全相关系统的参数。
- 通过 HMI 对安全相关系统进行更改的操作员应负责由此对安全回路造成的影响。
- 您必须清晰地记录要更改的变量。
- 在通过 HMI 进行安全相关更改时，必须采取透明、全面和明晰的操作步骤。
- 只有在发生以下一系列事件的情况下，安全相关系统中的更改才会被接受：
 - a. 新变量必须发送两次到两个不同的标签；即不能使用一条命令写入两个值。
 - b. 控制器中正在执行的安全相关代码必须检查两个标签是否相等，并确保它们处于范围内（边界检查）。
 - c. 必须读回两个新变量，并将它们显示在 HMI 设备上。
 - d. 必须由经过培训的操作员目测两个变量是否相同，以及变量值是否正确。
 - e. 必须由经过培训的操作员在 HMI 画面上手动确认变量值正确，继而向安全逻辑发送一条命令，允许在安全功能中使用新值。

在任何一种情况下，操作员都必须确认更改的有效性，之后方可接受更改并在安全回路中应用。

- 在安全验证过程中测试所有更改。

- 充分记录通过 HMI 执行的所有安全相关更改，包括以下内容：
 - 授权
 - 影响分析
 - 执行
 - 测试信息
 - 版本信息
- 针对安全相关系统的更改必须符合 IEC 61511 标准中关于过程安全的规定 — 第 11.7.1 节：操作员接口要求。
- 针对安全相关系统的更改必须符合 IEC 62061 中关于机器安全的规定。
- 与其他应用软件开发一样，开发人员必须遵循优良的开发技术和流程，包括操作员接口的验证和测试以及操作员接口对程序其他部分的访问。在控制器应用软件中，创建一个可由 HMI 访问的表格，并仅限制对所需数据点的访问。
- 类似于控制器程序，在系统经过验证和测试后，需要对 HMI 软件进行安全设置和维护，以符合 SIL 等级。

安全程序

安全程序只能在安全任务中调度，除此以外，它们具有标准程序的所有属性。安全程序也可以定义程序作用域安全标签。安全程序可以是预先计划的，也可以是非计划的。

安全程序只能包含安全组件。安全程序中的所有例程都是安全例程。安全程序不能包含标准例程或标准标签。

安全例程

安全例程只能位于一个安全程序中，除此以外，它们具有标准例程的所有属性。可以将一个安全例程指定为主例程。可以将另一个安全例程指定为故障例程。只有经过安全认证的指令才能在安全例程中使用。

如需了解安全指令列表的信息，请参见[附录 A](#)。



注意：若要保持 SIL 3 等级，必须确保安全逻辑没有尝试读或写标准标签。

安全标签

GuardLogix 控制系统支持在同一个项目中使用标准和安全标签。然而，编程软件在操作上区别标准标签和安全标签。

安全标签具有标准标签的所有属性，此外，它还具有用于提供 SIL 3 数据完整性的附加机制。

表 6- 安全标签的有效数据类型

• AUX_VALVE_CONTROL	• DINT	• MUTING_FOUR_SENSOR_BIDIR
• BOOL	• DIVERSE_INPUT	• MUTING_TWO_SENSOR_ASYM
• CAM_PROFILE	• EIGHT_POS_MODE_SELECTOR	• MUTING_TWO_SENSOR_SYM
• CAMSHAFT_MONITOR	• EMERGENCY_STOP	• MOTION_INSTRUCTION
• CB_CONTINUOUS_MODE	• ENABLE_PENDANT	• PHASE
• CB_CRANKSHAFT_POS_MONITOR	• EXT_ROUTINE_CONTROL	• PHASE_INSTRUCTION
• CB_INCH_MODE	• EXT_ROUTINE_PARAMETERS	• REAL
• CB_SINGLE_STROKE_MODE	• FBD_BIT_FIELD_DISTRIBUTE	• REDUNDANT_INPUT
• CONFIGURABLE_ROUT	• FBD_CONVERT	• REDUNDANT_OUTPUT
• CONNECTION_STATUS	• FBD_COUNTER	• SAFETY_MAT
• CONTROL	• FBD_LOGICAL	• SERIAL_PORT_CONTROL
• COUNTER	• FBD_MASK_EQUAL	• SFC_ACTION
• DCA_INPUT	• FBD_MASKED_MOVE	• SFC_STEP
• DCI_MONITOR	• FBD_TIMER	• SFC_STOP
• DCI_START	• FIVE_POS_MODE_SELECTOR	• SINT
• DCI_STOP	• INT	• STRING
• DCI_STOP_TEST	• LIGHT_CURTAIN	• THRS_ENHANCED
• DCI_STOP_TEST_LOCK	• MAIN_VALVE_CONTROL	• TIMER
• DCI_STOP_TEST_MUTE	• MANUAL_VALVE_CONTROL	• TWO_HAND_RUN_STATION

Logix Designer 应用程序可防止在安全程序中直接创建无效标签。如果导入的标签无效，则无法对其进行验证。

重要事项	在安全应用项目中禁止在标准和安全标签之间使用别名。
------	---------------------------

归为安全标签的标签可以是控制器作用域或程序作用域标签。控制器作用域安全标签可以由标准或安全逻辑或其他通信设备读取，但只能由安全逻辑或另一个 GuardLogix 安全控制器写入。程序作用域安全标签只能由本地安全例程访问。这些例程位于安全程序内。

与安全 I/O 和生产者或消费者安全数据关联的标签必须是控制器作用域安全标签。

重要事项	任何控制器作用域安全标签都可由任何标准例程读取，但更新速率则取决于安全任务的执行。这表示安全标签以安全任务周期速率更新，这与标准标签的特性不同。
------	--

安全例程中的标准标签 (标签映射)

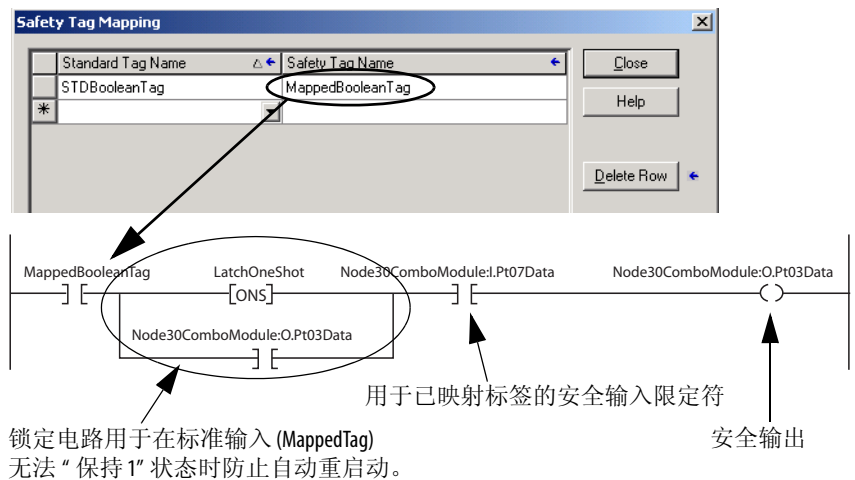
控制器作用域标准标签可映射到安全标签，为您提供一种用于同步标准和安全动作的机制。



注意：当在安全例程中使用标准数据时，应提供一种可靠的方法来确定以合适的方式使用数据。在安全标签中使用标准数据并不能使该数据成为安全数据。不得通过标准标签数据直接控制安全输出。

该示例阐述了如何通过安全数据来鉴定标准数据。

图 14- 通过安全数据鉴定标准数据



备注:

安全应用项目开发

主题	页码
安全原理的假设条件	49
应用程序开发和测试基础	50
调试生命周期	51
下载安全应用程序	56
上传安全应用程序	57
在线编辑	57
从非易失性存储器存储和加载项目	58
数据的强制赋值	58
禁止设备	58
编辑安全应用项目	59

安全原理的假设条件

安全原理假设以下条件：

- 如果您负责创建、操作和维护应用程序，则您必须在安全系统方面具备充分的资质、经过专门的培训并且拥有丰富的经验。
- 您可以正确应用逻辑，这表示能够检测到编程错误。通过严格遵守技术规范、编程和命名规则来检测编程错误。
- 执行应用程序的关键分析，并采取所有可能的措施来检测故障。
- 通过手动检查安全任务签名确认所有应用程序下载。
- 在启动安全相关系统运行之前，对整个系统执行完整的功能测试。

表 7- 控制器模式

控制器模式	安全任务状态	安全等级 ⁽¹⁾ (达到并包括)	备注 (已经将一个有效的程序下载到控制器。)
程序	解锁 无签名		• I/O 连接已建立 • 当前没有扫描安全任务逻辑。
运行	解锁 无签名	(仅用于开发目的)	• 允许强制 • 允许在线编辑。 • 安全内存已隔离, 但尚未提供保护 (读 / 写)。 • 当前正在扫描安全任务逻辑。主控制器和伙伴控制器处理逻辑, 交叉比较逻辑输出。将逻辑输出写入到安全输出。
运行	解锁 无签名	PLd/Cat. 3 可靠控制 SIL CL2	• 不允许进行新的强制。保持已有的强制。 • 不允许在线编辑。 • 安全内存已被保护 (只读)。 • 安全任务逻辑已扫描完毕。 • 主控制器和伙伴控制器处理逻辑, 交叉比较逻辑输出。将逻辑输出写入到安全输出。
运行	解锁 带签名	Ple/Cat. 4 可靠控制 SIL CL3	• 不允许强制。(必须撤消强制, 以生成安全任务签名。) • 不允许在线编辑。 • 安全内存已被保护 (只读)。 • 安全任务逻辑已扫描完毕。 • 主控制器和伙伴控制器处理逻辑, 交叉比较逻辑输出。将逻辑输出写入到安全输出。 • 安全任务签名未受保护, 可由访问控制器的任何人员删除。
运行	解锁 带签名	Ple/Cat. 4 可靠控制 SIL CL3	• 不允许强制。(必须撤消强制, 以生成安全任务签名。) • 不允许在线编辑。 • 安全内存已被保护 (只读)。 • 安全任务逻辑已扫描完毕。 • 主控制器和伙伴控制器处理逻辑, 交叉比较逻辑输出。将逻辑输出写入到安全输出。 • 安全任务签名已被保护。用户必须输入解锁密码解锁控制器, 然后才能删除安全任务签名。

(1) 为了实现该等级, 必须遵守本出版物中规定的安全要求。

应用程序开发和测试基础

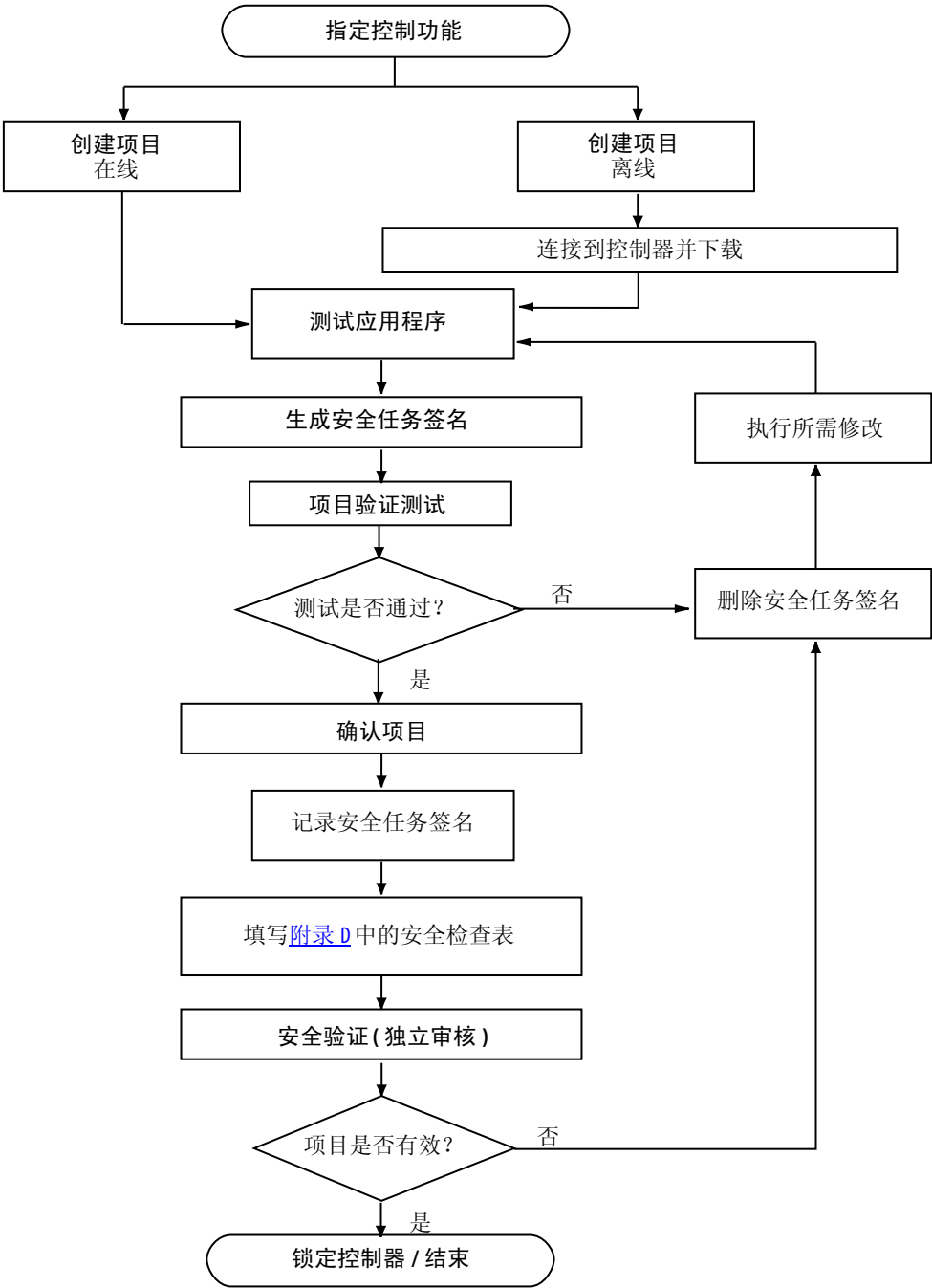
建议用于特定 SIL CL3 系统的应用程序应该由系统集成商或经过安全应用项目培训并具备相关经验的用户来开发。开发人员必须遵守良好的设计惯例:

- 使用功能技术规范, 包括流程图、时序图和顺序图。
- 执行安全任务逻辑审查。
- 执行应用程序验证。

调试生命周期

下面的流程图给出了调试 GuardLogix 系统所需的步骤。下文说明了以粗体显示的条目。

图 15- 调试系统



控制功能的技术规范

必须创建控制功能的技术规范。使用该技术规范来校验程序逻辑是否正确，以及是否完全满足应用项目的功能和安全控制要求。根据应用项目的不同，技术规范可以各种形式表示。但是，必须详细说明技术规范，包括以下内容(若适用)：

- 操作顺序
- 流程图和时序图
- 顺序图
- 程序说明
- 程序打印输出
- 针对各步骤(包括步进条件)以及所要控制的执行器的书面说明，包括以下各项：
 - 输入定义
 - 输出定义
 - I/O 接线图和参考
 - 工作原理
- 步进条件和所要控制的执行器的矩阵或表，包括顺序图和时序图
- 定义边界条件，例如，运行模式和紧急停机

技术规范 I/O 部分必须包含现场电路的分析，即，传感器和执行器类型。

- 传感器(数字或模拟)
 - 标准操作中的信号(数字传感器的休眠电流原理，传感器 OFF 表示无信号)
 - 确定 SIL 等级所要求的冗余性
 - 差异监视和可视化，包括诊断逻辑
- 执行器
 - 标准操作中的位置和激活(通常为 OFF)
 - 当关闭电源或发生电源故障时的安全反应/定位
 - 差异监视和可视化，包括诊断逻辑

创建项目

在编写应用程序时使用的逻辑和指令必须具备以下特点：

- 易于理解
- 易于跟踪
- 易于更改
- 易于测试

审查和测试所有逻辑。隔离安全相关逻辑和标准逻辑。

标记程序

通过以下项目可清晰识别应用程序：

- 名称
- 日期
- 版本
- 任何其他用户标识

测试应用程序

该步骤包含在准备项目验证测试期间正确运行应用程序所需的“运行”和“程序”模式、在线或离线编辑、上传和下载以及非正式测试的任意组合。

生成安全任务签名

安全任务签名是识别每个项目 — 包括其逻辑、数据和配置的唯一标识。安全任务签名由 ID (标识号)、日期和时间组成。

如果以下所有条件均为真，则可生成安全任务签名：

- Logix Designer 应用程序与控制器联机。
- 控制器处于程序模式。
- 控制器已安全解锁。
- 控制器没有安全强制或待定的在线安全编辑。
- 安全任务状态正常。

一旦应用程序测试完成，必须生成安全任务签名。在生成安全任务签名后，编程软件自动上传该签名。

重要事项	为了确认每次下载的完整性，必须在初次创建后手动记录安全任务签名，并在每次下载后检查安全任务签名，以确保它与原始签名一致。
-------------	--

只有在 GuardLogix 控制器安全解锁，并且 (若在线) 钥匙开关处于 REM 或 PROG 位置时才能删除安全任务签名。

当存在安全任务签名时，不允许在安全任务内执行以下动作：

- 安全组件的在线 / 离线编程或编辑
- 强制安全 I/O
- 数据处理 (除通过例程逻辑或另一个 GuardLogix 控制器外)

项目验证测试

若要检查应用程序是否符合技术规范，必须生成一组涵盖应用程序的适当测试案例。测试案例组必须归档保存，以作为测试技术规范。

必须包括一组测试，以证明在应用逻辑中使用的计算 (公式) 的有效性。等效范围测试属于可接受的测试。这些测试在所定义的数值范围内、在界限位置或在无效数值范围内执行。所需的测试案例数量取决于所使用的公式，且必须包含临界值对。

此外还必须包括源设备 (现场设备) 的主动模拟，因为这是校验系统中传感器和执行器是否正确接线的唯一方法。通过手动操控传感器和执行器来校验所编程的功能是否正确运行。

此外还必须包括用于校验对接线故障和网络通信故障的反应的测试。

项目验证包括故障例程、输入和输出通道的功能验证测试，以确保安全系统正确运行。

若要在 GuardLogix 控制器上执行项目验证测试，则必须完全测试应用项目。必须切换每个安全功能所涉及的每个传感器和执行器。从控制器角度看，这表示切换进入控制器的 I/O 点，而不必是实际激励器。确保测试所有关机功能，因为通常在正常操作过程中不执行这些功能。此外，请务必注意项目验证测试仅对测试的特定应用项目有效。如果将控制器移动到另一个应用项目，则还必须在新应用程序环境中对控制器执行启动和项目验证测试。

确认项目

必须打印或查看项目，并比较已上传的安全 I/O 和控制器配置、安全数据和安全任务程序逻辑，以确保在安全应用程序中下载、测试和保持正确的安全组件。

如果应用程序包含一个使用指令签名封装的用户自定义安全指令，则还必须将指令签名、日期 / 时间和安全指令签名与封装用户自定义指令时记录的数值进行比较。

如需了解关于在 SIL 3 应用项目中创建和使用用户自定义安全指令的信息，请参见[附录 B](#)，[用户自定义安全指令](#)。

下面的步骤阐述了其中一种用于确认项目的方法。

1. 当控制器处于“程序”模式，保存项目。
2. 当出现 Upload Tag Values (上传标签值) 提示时，选择 Yes (是)。
3. 当 Logix Designer 应用程序离线时，以新名称保存项目，例如 Offlineprojectname.ACD，其中 projectname 是项目名称。

这就是经过测试的新主项目文件。

4. 关闭项目。
5. 从当前目录移走原始项目归档文件。
可以删除该文件或将该文件存储到归档位置。必须执行该步骤，因为当 Logix Designer 应用程序在该目录中查找 projectname.ACD 时，它将该文件与控制器项目关联，并且将不执行实际上传操作。
6. 当控制器仍处于“程序”模式时，从控制器上传项目。
7. 将已上传的项目另存为 Onlineprojectname.ACD，其中 projectname 是项目名称。
8. 当出现 Upload Tag Values (上传标签值) 提示时，选择 Yes (是)。
9. 使用 Logix Designer 程序比较实用工具来执行以下比较：
 - 比较 GuardLogix 控制器和 CIP 安全 I/O 设备的所有属性。
 - 比较安全任务、安全程序和安全例程的所有属性。
 - 比较安全例程中的所有逻辑。

安全验证

在批准系统运行之前，需要由独立的第三方来审核安全系统。
IEC 61508 SIL 3 要求进行独立的第三方认证。

锁定 GuardLogix 控制器

GuardLogix 控制器系统可以被安全锁定，以防止修改安全控制组件。但是，安全锁定控制器不是 SIL 3 应用项目的要求。安全锁定功能仅适用于安全组件，例如，安全任务、安全程序、安全例程、安全签名、用户自定义安全指令、安全 I/O 和安全任务签名。但是，仅仅进行安全锁定并不能满足 SIL 3 要求。

当控制器处于安全锁定状态时，不能修改任何安全特性。当控制器被安全锁定时，不允许在安全任务中执行以下动作：

- 在线 / 离线编程或编辑
- 强制安全 I/O
- 数据处理 (除通过例程逻辑或另一个 GuardLogix 控制器外)
- 创建或编辑用户自定义安全指令
- 生成或删除安全任务签名

控制器的缺省状态是安全解锁。无论在线或离线，也无论是否具有程序原始源代码，均可将安全应用项目置于安全锁定状态。但是，不能出现任何安全强制或待定安全编辑。当钥匙开关处于 RUN 位置时，无法更改安全锁定或解锁状态。

若要附加一层防护，可使用单独的密码来安全锁定或解锁控制器。密码为可选。

下载安全应用程序

下载后，除非存在安全任务签名，否则要求进行应用项目测试。

重要事项	为了确认每次下载的完整性，必须在初次创建后手动记录安全任务签名，并在每次下载后检查安全任务签名，以确保它与原始签名一致。
-------------	--

只有在离线项目的安全任务签名、硬件系列和操作系统版本与目标 GuardLogix 控制器中包含的对应各项一致，且控制器的安全任务状态正常时，才允许下载到安全锁定的 GuardLogix 控制器。

重要事项	如果安全任务签名不一致，且控制器被安全锁定，则必须解锁控制器才能下载。在这种情况下，下载到控制器时会删除安全任务签名。因此，必须重新验证应用项目。
------	---



注意：USB 端口仅用于临时本地编程，并非用于永久性连接。

上传安全应用程序

如果 GuardLogix 控制器包含安全任务签名，则安全任务签名会随项目一起上传。这表示上传后，将覆盖对离线安全数据的所有修改。

在线编辑

如果没有安全任务签名，且控制器安全解锁，则可对安全例程执行在线编辑。

提示	在线时无法编辑标准或用户自定义安全指令。
当控制器被安全锁定或存在安全任务签名时，不能存在待定编辑。当控制器被安全锁定时，可以存在在线编辑。但是，它们不能被组合或取消。	
提示	标准例程中的在线编辑不受安全锁定或解锁状态的影响。

如需了解编辑应用程序的更多信息，请参见第 59 页。

从非易失性存储器 存储和加载项目

GuardLogix 5570 控制器支持通过存储卡进行固件升级、用户程序存储和提取。在 GuardLogix 系统中，只有主控制器将存储卡作为非易失性存储器使用。

当在存储卡上存储安全项目时，罗克韦尔自动化建议将加载模式选为“远程程序”，即加载后控制器应进入的模式。在实际机器操作之前，要求操作员干预以启动机器。

只有在下列情况下才能从非易失性存储器启动加载：

- 当由存储在非易失性存储器中的项目指定的控制器类型与您的控制器类型一致时
- 当非易失性存储器中项目的主版本和次版本与控制器的版本和次版本一致时
- 当控制器不处于“运行”模式时

只有当存储在非易失性存储器的项目的安全任务签名与控制器上的项目一致时，才允许将项目加载到安全锁定的控制器。如果签名不一致或控制器安全解锁且没有安全任务签名，则必须首先解锁控制器，然后才能尝试通过非易失性存储器更新控制器。

重要事项	如果解锁控制器，并启动从非易失性存储器加载，则在完成加载后，安全锁定状态、密码和安全任务签名将被设为非易失性存储器中所包含的数值。
------	---

数据的强制赋值

当项目安全解锁且不存在安全任务签名时，可以对 I/O、生产者或消费者安全签名中包含的所有数据 (包括 CONNECTION_STATUS) 进行强制赋值。但是，在安全项目可以被安全锁定或可以生成安全任务签名之前，必须在所有安全签名上卸载强制赋值，而不仅仅是禁用强制赋值。当项目被安全锁定或存在安全任务签名时，不能对安全签名进行强制赋值。

提示	无论处于安全锁定或解锁状态，都可以在标准标签上安装和卸载强制赋值。
----	-----------------------------------

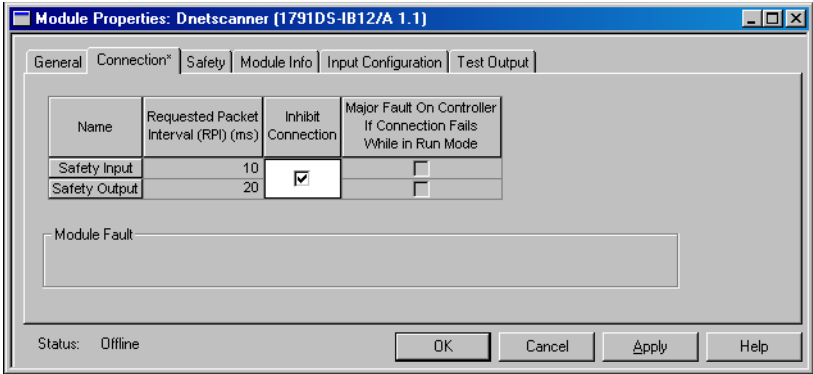
禁止设备

如果应用程序被安全锁定或存在安全任务签名，则无法禁止或启用 CIP 安全 I/O 设备或生产者控制器。

按以下步骤操作来禁止某个特定的安全 I/O 设备。

1. 在 Logix Designer 应用程序中，右击该设备，然后选择 Properties (属性)。
2. 在 Module Properties (模块属性) 对话框中，单击 Connection (连接) 选项卡。

3. 选中 Inhibit Connection (禁止连接), 然后单击 Apply (应用)。



一旦选中了复选框，设备则被禁止。如果禁止通信设备，则也会禁止所有下游设备。

编辑安全应用项目

- 下列规则适用于在 Logix Designer 应用程序中更改安全应用程序：
- 只有经过专门培训的授权人员才能执行程序编辑。这些人员应采取所有可用的监管手段，例如，使用控制器钥匙开关和软件密码保护。
 - 当经过专门培训的授权人员执行程序编辑时，他们在修改过程中承担核心安全责任。这些人员还必须保持安全应用项目运行。
 - 在线编辑时，必须使用一种交互保护机制来保持系统的安全。
 - 必须充分记录所有程序编辑，包括以下内容：
 - 授权
 - 影响分析
 - 执行
 - 测试信息
 - 版本信息
 - 如果只有标准例程存在在线编辑，则在返回正常操作之前，不需要验证这些编辑。
 - 必须根据定时和标签映射，确保对标准例程所作的修改可以被安全应用项目接受。
 - 如下所述，可以在离线或在线时编辑程序的逻辑部分。

执行离线编辑

当仅对标准程序单元执行离线编辑，且在下载后安全任务签名一致时，可恢复操作。

当离线编辑影响安全程序时，必须在继续操作之前，根据影响分析重新验证应用项目的所有受影响的元素。

第 61 页上的流程图阐述了离线编辑的过程。

执行在线编辑

当在线编辑影响安全程序时，必须在继续操作之前，根据影响分析重新验证应用项目的所有受影响的元素。第 61 页上的流程图阐述了在线编辑的过程。

提示 将在线编辑限制为小幅程序修改，例如设定值更改或小幅逻辑添加、删除和修改。

在线编辑受 GuardLogix 控制器的安全锁定和安全任务签名功能的影响。

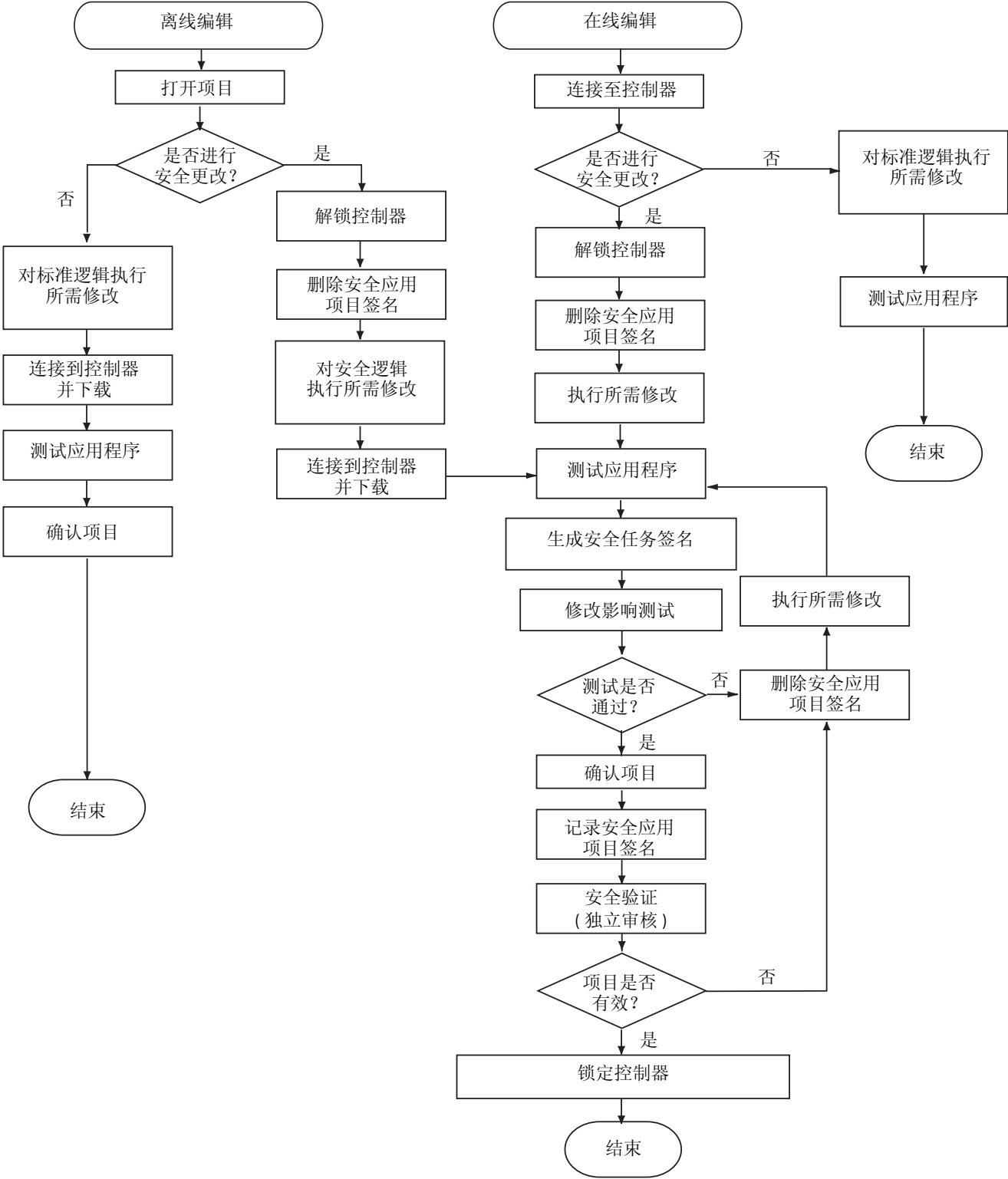
如需了解更多信息，请参见第 53 页的“[生成安全任务签名](#)”和第 56 页的“[锁定 GuardLogix 控制器](#)”。

如需了解关于在在线时如何在 Logix Designer 应用程序中编辑梯形图逻辑的详细信息，请参见 Logix5000 Controllers Quick Start (Logix5000 控制器快速入门，出版号：[1756-QS001](#))。

修改影响测试

必须规划对已验证软件的任何修改、增强或调整，并分析对功能安全系统的影响。必须按影响分析所述，执行软件安全生命周期的所有相应阶段。必须至少执行所有受影响软件的功能测试。必须记录对软件技术规范的所有修改。此外，还必须记录测试结果。如需了解详细信息，请参见 IEC 61508-3 的第 7.8 节：软件修改。

图 16- 在线和离线编辑过程



备注:

监视状态和处理故障

主题	页码
监视系统状态	63
GuardLogix 系统故障	66

GuardLogix 架构提供多种检测和响应系统内部故障的方法。处理故障的第一种方法就是确保已经完成了应用项目的检查表 (参见[附录 D](#))。

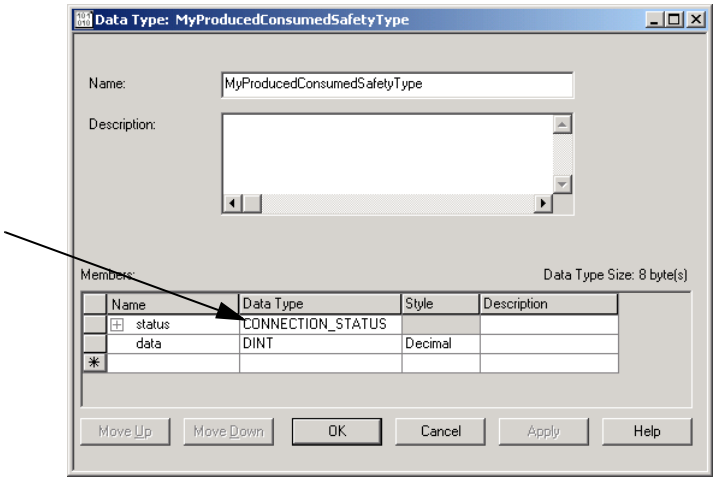
监视系统状态

您可查看安全标签连接的状态。此外还可通过查询各种设备对象来确定当前操作状态。确定哪些数据最适合用于启动关机序列是您的责任。

CONNECTION_STATUS 数据

与安全输入数据和生产者 / 消费者安全标签数据关联的标签结构体的第一个成员包含连接状态。该成员是一种预定义数据类型，被称为 CONNECTION_STATUS。

图 17 - Data Type (数据类型) 对话框



CONNECTION_STATUS 数据类型的前两位包含设备的 RunMode 和 ConnectionFaulted 状态位。下表给出了 RunMode 和 ConnectionFaulted 状态的各种组合。

表 8- 安全连接状态

RunMode 状态	ConnectionFaulted 状态	安全连接操作
1= 运行	0= 有效	数据正在由生产设备有效地控制。生产设备处于“运行”模式。
0= 空闲	0= 有效	连接有效，生产设备处于“空闲”状态。安全数据被复位到零。
0= 空闲	1= 故障	安全连接发生故障。生产设备的状态未知。安全数据被复位到零。
1	1	无效状态。



注意：如果连接丢失，且系统跳转到安全状态，则无法将安全 I/O 连接和生产者 / 消费者连接自动配置成使控制器发生故障。因此，如果需要检测设备故障以确保系统保持 SIL 3 等级，必须监视安全 I/O CONNECTION_STATUS 位，并通过程序逻辑启动故障。

输入和输出诊断

Guard I/O 模块提供脉冲测试和监视功能。如果模块检测到故障，则将出错的输入或输出设为其安全状态，并向控制器报告故障。故障指示通过输入或输出状态给出，并在故障清除后使故障指示保持一段可配置的时间。

重要事项	您负责提供应用逻辑来锁定这些 I/O 故障，并确保系统正确重新启动。
------	------------------------------------

I/O 设备连接状态

CIP 安全协议提供安全系统中每个 I/O 设备的状态。如果检测到输入连接故障，则操作系统将所有设备输入设为其断电 (安全) 状态，相关输入状态变为故障。如果检测到输出连接故障，则操作系统将相关输出状态设为故障。输出设备使输出断电。

重要事项	您负责提供应用逻辑来锁定这些 I/O 故障，并确保系统正确重新启动。
------	------------------------------------

断电跳闸系统

GuardLogix 控制器是断电跳闸系统的一部分，这表示零是安全状态。某些 (但并非全部) 安全 I/O 设备故障会导致所有设备输入或输出被设为零 (安全状态)。与特定输入通道相关的故障导致该特定通道被设为零；例如，与通道 0 相关的脉冲测试故障导致将通道 0 输入数据设为安全状态 (0)。如果故障与设备有关，而与特定通道无关，则组合状态位显示故障状态，并将所有设备数据设为安全状态 (0)。

如需了解关于如何使用 GuardLogix 安全应用项目指令的信息，请参见本手册的[附录 F](#) 以及 GuardLogix Safety Application Instructions Safety Reference Manual (GuardLogix 安全应用项目指令安全标准手册，出版号：[1756-RM095](#))。

获取系统值 (GSV) 和设置系统值 (SSV) 指令

GSV 和 SSV 指令允许您获取 (GSV) 和设置 (SSV) 存储在设备对象中的控制器系统数据。当输入 GSV/SSV 指令时，编程软件显示每个指令的有效对象类别、对象名称和属性名称。将 GSV 和 SSV 指令与安全组件一起使用时存在一些限制条件。

重要事项	安全任务无法对标准属性执行 GSV 或 SSV 操作。 可由标准任务写入的安全对象属性仅用于诊断用途。 它们不影响安全任务执行。
-------------	--

如需了解关于通过 GSV 和 SSV 指令可访问的安全属性的更多信息，请参见 GuardLogix 5570 Controllers User Manual (GuardLogix 5570 控制器用户手册，出版号：[1756-UM022](#))。

如需了解关于使用 GSV 和 SSV 指令的一般信息，请参见 Logix5000 Controllers General Instructions Reference Manual (Logix5000 控制器通用指令集参考手册，出版号：[1756-RM003](#))。

GuardLogix 系统故障

GuardLogix 系统的故障可分成以下三类：

- 不可恢复的控制器故障
- 不可恢复的安全故障
- 可恢复的故障

如需了解关于处理故障的信息，请参见 GuardLogix 5570 Controllers User Manual (GuardLogix 5570 控制器用户手册，出版号：[1756-UM022](#))。

不可恢复的控制器故障

如果控制器的内部诊断失败，则发生不可恢复的控制器故障。当在主控制器或安全伙伴中发生不可恢复的控制器故障时，会失去伙伴关系，导致另一方生成不可恢复的看门狗超时故障。标准任务和安全任务停止执行，且安全 I/O 跳转到安全状态。

从不可恢复的控制器故障恢复操作需要下载应用程序。

不可恢复的安全故障

当发生不可恢复的安全故障时，控制器在控制器作用域故障处理程序中记录故障，并关闭安全任务，包括安全 I/O 和安全逻辑。

若要从不可恢复的安全故障恢复操作，可以从安全任务签名重新初始化安全内存（当清除故障时自动发生），或在没有安全任务签名时，通过显式下载安全项目来重新初始化。

可以通过控制器作用域安全故障处理程序来清除故障日志条目，从而可以忽略安全故障。这样标准任务便可以继续运行。



注意：忽略安全故障并不会清除该故障。如果忽略安全故障，您则有责任证明这样做可以保持 SIL 3 等级。

可恢复的故障

由安全程序中的用户编程错误引起的控制器故障触发控制器处理包含在项目的安全程序故障处理程序中的逻辑。安全程序故障处理程序为应用项目提供解决故障条件以及恢复操作的机会。



注意：您必须向认证机构证明可恢复故障的自动恢复可以保持 SIL 3 等级。

当不存在安全程序故障处理程序或无法由该程序恢复故障时，控制器处理控制器作用域故障处理程序中的逻辑，终止安全程序逻辑执行，将安全 I/O 连接保持在激活但空闲状态。

重要事项

当因安全程序故障处理程序未处理的一个可恢复故障而终止安全程序逻辑执行时，关闭安全 I/O 连接，然后重新打开以重新初始化安全连接。

如果因一个可恢复故障未得到恢复而终止用户逻辑，则将安全输出置于安全状态，且安全消费者标记的生产者命令消费者将它们置于安全状态。

提示

当对标准应用项目使用安全 I/O 时，如果因一个可恢复故障未得到恢复而终止用户逻辑，则命令安全 I/O 进入安全状态。

如果在控制器作用域故障处理程序中忽略可恢复的安全故障，则只有标准任务保持运行。如果故障没有被忽略，则也会关闭标准任务。



注意：忽略安全故障并不会清除该故障。如果忽略安全故障，您则有责任证明这样做可以保持 SIL 3 等级。

备注:

安全指令

如需了解最新信息，请参见

<http://www.rockwellautomation.com/products/certification/safety/> 上的安全认证。

表9和表10列出了经认证可在 SIL 3 应用项目中使用的安全应用项目指令。

表9- 常规安全应用项目指令

助记符	名称	目的	认证
CROUT	可配置的冗余输出	控制和监视冗余输出。	• BG • TÜV
DCA	双通道输入 — 模拟量 (整型)	监视两个模拟量值的偏差和范围容差。	TÜV
DCAF	双通道输入 — 模拟量 (浮点型)		
DCS	双通道输入 — 停止	监视主要用于提供停止功能的双输入安全设备，例如，急停、光幕或门开关。	• BG • TÜV
DCST	双通道输入 — 通过测试停止	监视主要用于提供停止功能的双输入安全设备，例如，急停、光幕或门开关。它包括启动停止设备功能测试的附加功能。	• BG • TÜV
DCSTL	双通道输入 — 通过测试和锁定停止	监视主要用于提供停止功能的双输入安全设备，例如，急停、光幕或门开关。它包括启动停止设备功能测试的附加功能。它可监控安全设备的反馈信号，向安全设备发出锁定请求。	• BG • TÜV
DCSTM	双通道输入 — 通过测试和静默停止	监视主要用于提供停止功能的双输入安全设备，例如，急停、光幕或门开关。它包括启动停止设备功能测试的附加功能以及使安全设备静默的功能。	TÜV
DCM	双通道输入 — 监视	监视双输入安全设备。	• BG • TÜV
DCSRT	双通道输入 — 启动	为主要用于安全启动机器的双输入安全设备通电，例如，带使能功能的悬吊式按钮盒。	• BG • TÜV
SMAT	安全垫	指示安全垫是否被占用。	TÜV
THRSe	双手运行站 — 增强型	监视两个不同的安全输入，一个输入来自右侧按钮，另一个输入来自左侧按钮，它们用于控制一个输出。具有可配置的通道间差异时间和旁路双手运行站的增强功能。	• BG • TÜV
TSAM	双传感器不对称静默	通过两个非对称排列的静默传感器自动临时禁用光幕的保护功能。	TÜV
TSSM	双传感器对称静默	通过两个对称排列的静默传感器自动临时禁用光幕的保护功能。	TÜV
FSBM	四传感器双向静默	通过在光幕检测场前后依次排列四个传感器，临时自动禁用光幕保护功能。	TÜV

表 10-金属体安全应用项目指令

助记符	名称	目的	认证
BCM	离合器闸连续模式	用于要求连续操作的冲压应用。	• BG • TÜV
CBIM	离合器闸缓动模式	用于要求执行小幅滑动调节的冲压应用，例如，冲压机设置。	• BG • TÜV
CBSSM	离合器闸单行程模式	用于单周期冲压应用。	• BG • TÜV
CPM	曲轴位置监视	用于确定冲压机的滑动位置。	• BG • TÜV
CSM	凸轮轴监视	监视凸轮轴启动、停止和运行操作的运动。	• BG • TÜV
EPMS	八位置模式选择器	监视 8 个安全输入来控制与活动输入对应的 8 个输入之一。	• BG • TÜV
AVC	辅助阀控制	控制与主阀一起使用的辅助阀。	TÜV
MVC	主阀控制	控制和监视主阀。	• BG • TÜV
MMVC	维护手动阀控制	用于在维护操作期间手动驱动阀。	• BG • TÜV

安全任务中的例程可以使用这些梯形图逻辑安全指令。

表 11-梯形图逻辑安全指令

类型	助记符	名称	目的
数组 (文件)	FAL ⁽¹⁾	文件算术和逻辑	对存储在数组中的数据执行复制、算术、逻辑和函数运算
	FLL ⁽¹⁾	文件填充	用源值填充数组元素，同时保留源值不变
	FSC ⁽¹⁾	文件搜索和比较	逐个元素地比较数组中的值
	SIZE ⁽¹⁾	元素大小	查找数组维度的大小
位	XIC	检查是否关闭	当位被置位时，启用输出
	XIO	检查是否打开	当位被清除时，启用输出
	OTE	输出通电	置位
	OTL	输出锁定	置位(保持性)
	OTU	输出解锁	清除位(保持性)
	ONS	一次扫描	触发某个事件发生一次
	OSR	一次扫描上升	在状态变化的假到真(上升)沿触发某个事件发生一次
	OSF	一次扫描下降	在状态变化的真到假(下降)沿触发某个事件发生一次
定时器	TON	定时器接通延时	确定定时器启用的时间
	TOF	定时器断开延时	确定定时器禁用的时间
	RTO	保持性定时器接通	累计时间
	CTU	递增计数	递增计数
	CTD	递减计数	递减计数
	RES	复位	复位定时器或计数器

表 11 - 梯形图逻辑安全指令

类型	助记符	名称	目的
比较	CMP ⁽¹⁾⁽²⁾	比较	对表达式中指定的算术运算进行比较
	EQU	等于	测试两个数值是否相等
	GEQ	大于或等于	测试一个数值是否大于或等于另一个数值
	GRT	大于	测试一个数值是否大于另一个数值
	LEQ	小于或等于	测试一个数值是否小于或等于另一个数值
	LES	小于	测试一个数值是否小于另一个数值
	MEQ	掩码比较是否相等	通过掩码传递源值和比较值，然后测试它们是否相等
	NEQ	不等于	测试一个数值是否不等于另一个数值
	LIM	界限测试	测试一个数值是否位于指定的范围内
移动	CLR	清除	清除数值
	COP ⁽³⁾	复制	复制数值
	MOV	移动	复制数值
	MVM	掩码移动	复制一个整数的某个特定部分
	SWPB ⁽¹⁾	字节交换	重新排列值的各字节
逻辑	AND	逐位逻辑与	执行逐位逻辑与运算
	NOT	逐位逻辑非	执行逐位逻辑非运算
	OR	逐位逻辑或	执行逐位逻辑或运算
	XOR	逐位异或	执行逐位异或运算
程序控制	JMP	跳转到标签	跳过一段不是始终需要执行的逻辑段 (跳转到引用标签指令)
	LBL	标签	标注一个指令，从而可以由 JMP 指令引用
	JSR	跳转到子例程	跳转到一个独立的例程
	RET	返回	返回子例程的结果
	SBR	子程序	将数据传递到子例程
	TND	临时终点	标记一个临时终点，暂停例程执行
	MCR	主控制复位	禁用逻辑段中的逻辑行
	AFI	始终为假指令	禁用逻辑行
	NOP	无操作	在逻辑中插入一个占位符
	EVENT	触发事件任务	触发事件任务的一次执行 ⁽⁵⁾
算术 / 计算	ADD	加	两个数值相加
	CPT ⁽¹⁾	计算	执行表达式中定义的算术运算
	SUB	减	两个数值相减
	MUL	乘	两个数值相乘
	DIV	除	两个数值相除
	MOD	模	确定一个数值除以另一个数值后的余数
	SQR	平方根	计算一个数值的平方根
	NEG	取反	取一个数值的相反符号
	ABS	绝对值	取一个数值的绝对值
I/O	GSV ⁽⁴⁾	获取系统值	获取控制器状态信息
	SSV ⁽⁴⁾	设置系统值	设置控制器状态信息

(1) 仅 1756-L7xS 和 1756-L7xSXT 控制器支持此操作。对于 REAL 数据类型，1756-L7xS 和 1756-L7xSXT 控制器支持对安全例程使用浮点格式。

(2) 安全例程中不支持诸如 SIN、COS 和 TAN 等高级运算符。

(3) 当在安全例程中使用 COP 指令时，长度操作数必须是一个常数。源地址和目标地址的长度必须相同。

(4) 如需了解使用 GSV 和 SSV 指令时的特殊注意事项，请参见 GuardLogix 5570 Controllers User Manual (GuardLogix 5570 控制器用户手册，出版号：[1756-UM022](#))。

(5) 事件指令将触发对标准任务的一次扫描。

重要事项 如果要在 Kinetix 5500 伺服驱动器上使用运动直接命令，请参见 Kinetix 5500 Servo Drives User Manual (Kinetix 5500 伺服驱动器用户手册，出版号：[2198-UM001](#))，以了解如何在安全应用项目中使用该功能。

有关详细信息，请参见以下出版物：

表 12 - 其他资源

资源	说明
GuardLogix Safety Application Instruction Set Reference Manual (GuardLogix 安全应用项目指令集参考手册，出版号： 1756-RM095)	提供关于安全应用项目指令的更多信息
Logix5000 Controllers General Instructions Reference Manual (Logix5000 控制器通用指令参考手册，出版号： 1756-RM003)	包含关于 Logix 指令集的详细信息

用户自定义安全指令

主题	页码
创建和使用用户 自定义安全指令	73
其他资源	78

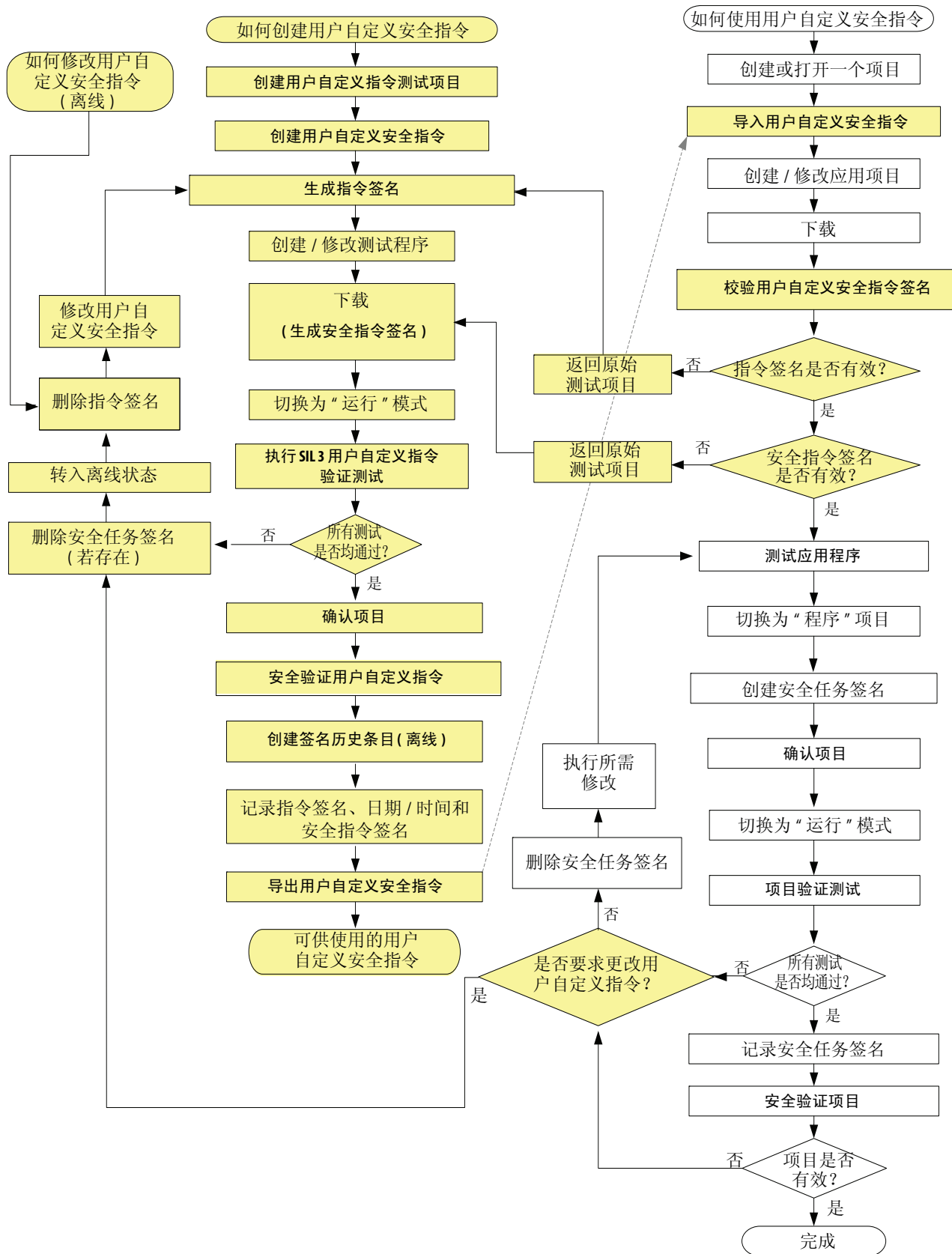
通过 Logix Designer 应用程序，可以创建用户自定义安全指令。用户自定义安全指令允许将通用的安全逻辑封装到一个指令中，使其模块化，更易于重复使用。

用户自定义安全指令使用高完整性的用户自定义指令的指令签名，以及在高达 (包括) SIL 3 的安全相关功能中使用 SIL 3 安全指令签名。

创建和使用用户自定义安全指令

第 74 页上的流程图显示了创建用户自定义安全指令以及在 SIL 3 安全应用程序中使用该指令所要求的步骤。阴影条目是只有用户自定义指令才有的步骤。以粗体文本显示的条目说明详见流程图后面的几页。

图 18- 用户自定义安全指令的创建和使用流程图



创建用户自定义指令测试项目

您必须创建一个唯一的测试项目，专门用于创建和测试用户自定义安全指令。它必须是一个独立专用项目，以将意外影响降至最小。

遵照[第 53 页的创建项目](#)中所述的项目指南。

创建用户自定义安全指令

如需了解创建用户自定义指令的指南，请参见 Logix5000 Controllers Add-On Instruction Programming Manual (Logix5000 控制器用户自定义指令编程手册，出版号：[1756-PM010](#))。

生成指令签名

指令签名允许您快速确定指令是否被修改。每个用户自定义指令都可以拥有自己的签名。当在安全相关的功能中使用用户自定义指令时，要求使用指令签名，此外，有时候，受管制行业也可能要求使用指令签名。当应用项目要求较高完整性等级时请使用指令签名。

指令签名由一个 ID 号和时间戳组成，用来识别给定时间点的用户自定义指令的内容。

用户自定义指令生成后，指令签名会立即将其封装，防止使用签名时对该指令进行编辑。该限制包括梯级注释、标签说明和所创建的所有指令文档。当指令被封装后，只能执行以下动作：

- 复制指令签名
- 创建或复制签名历史条目
- 创建用户自定义指令的实例
- 下载指令
- 移除指令签名
- 打印报表

当生成指令签名后，Logix Designer 应用程序显示带有封装图标的安全指令定义。



重要事项

如果计划通过 Logix Designer 应用程序中的源代码保护功能来保护用户自定义指令，则必须在生成指令签名之前启用源代码保护。

下载并生成安全指令签名

初次下载一个已封装的用户自定义安全指令时，会自动生成一个 SIL 3 安全指令签名。安全指令签名是一个 ID 号，用来识别用户自定义安全指令的执行特性。

SIL 3 用户自定义指令验证测试

必须在一个独立、专用的应用项目中执行用户自定义安全指令 SIL 3 测试，以确保将意外影响降至最低。您必须遵守合理设计的测试计划，执行用户自定义安全指令的单元测试（通过逻辑执行所有可能的路径），包括所有输入参数的有效和无效范围。

所有用户自定义安全指令的开发必须满足 IEC 61508 — “软件模块测试要求”，其中列出了单元测试的详细要求。

确认项目

必须打印或查看项目，并手动比较已上传的安全 I/O 和控制器配置、安全数据、用户自定义安全指令定义和安全任务程序逻辑，以确保在安全应用程序中下载、测试和保存正确的安全组件。

有关其中一种项目确认方法的描述，请参见[第 55 页的确认项目](#)。

安全验证用户自定义指令

在批准指令使用之前，需要由独立的第三方来审核用户自定义指令。IEC 61508 SIL 3 要求实施独立的第三方验证。

创建签名历史条目

签名历史为将来提供参考记录。签名历史条目包含用户名、指令签名、时间戳值和用户自定义描述。最多可存储 6 个历史条目。必须转入离线状态才能创建签名历史条目。

提示

Logix Designer 应用程序中的 **Signature Listing** (签名列表) 报告可打印指令签名、时间戳和安全指令签名。在控制器项目管理器中右击用户自定义指令，然后选择 **Print** (打印) > **Signature Listing** (签名列表) 即可打印报表。

导出和导入用户自定义安全指令

当导出用户自定义安全指令时，选择一个选项，以在同一个导出文件中包括所有被引用的用户自定义指令和用户自定义类型。通过包括被引用的用户自定义指令，可以更易于保留签名。

当导入用户自定义指令时，须遵守以下准则：

- 无法将用户自定义安全指令导入到标准项目中。
- 无法将用户自定义安全指令导入到已经安全锁定或具有安全任务签名的安全项目中。
- 无法在线导入用户自定义安全指令。
- 如果将带一个指令签名的用户自定义指令导入到被引用的用户自定义指令或用户自定义类型不可用的项目中，则需要删除该签名。

校验用户自定义安全指令签名

下载包含已导入的用户自定义安全指令的应用项目后，必须将指令签名值、日期和时间戳以及安全指令签名值与导出用户自定义安全指令之前记录的原始值进行比较。如果它们一致，则用户自定义安全指令有效，可以继续验证应用项目。

测试应用程序

该步骤包含正确运行应用项目所需的“运行”和“程序”模式、在线或离线程序编辑、上传和下载以及信息测试的任意组合。

项目验证测试

执行应用项目的工程测试，包括安全系统。

如需了解要求的更多信息，请参见[第 54 页的项目验证测试](#)。

安全验证项目

在批准系统运行之前，需要由独立的第三方来审核安全系统。
IEC 61508 SIL 3 要求实施独立的第三方验证。

其他资源

如需了解如何使用用户自定义指令的更多信息，请参见以下出版物。

资源	说明
Logix5000 Controllers Add-On Instructions Programming Manual (Logix5000 控制器用户自定义指令编程手册，出版号： 1756-PM010)	提供如何在 RSLogix 5000 应用程序中规划、创建、使用、导入和导出用户自定义指令的信息
Import/Export Project Components Programming Manual (导入 / 导出项目组件编程手册，出版号： 1756-PM019)	包含如何导入和导出项目组件的详细信息

反应时间

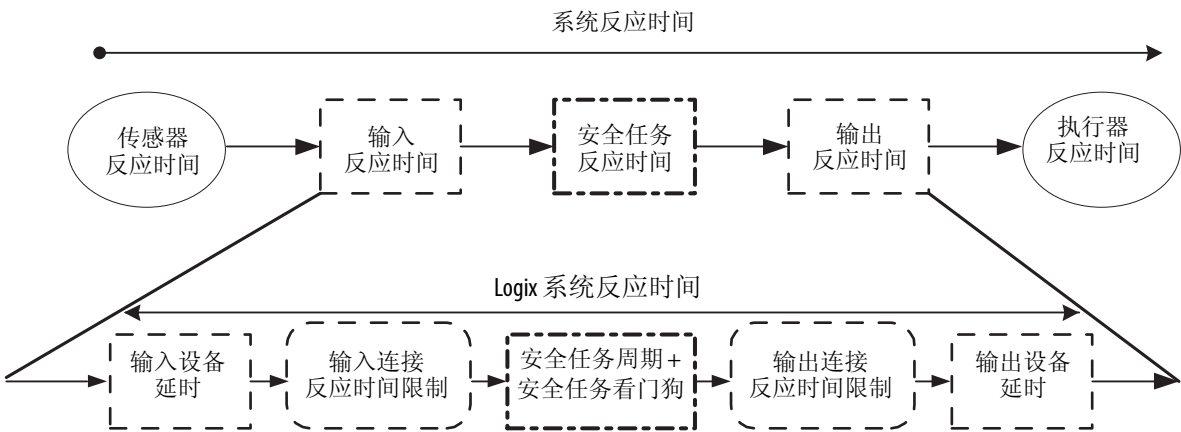
主题	页码
系统反应时间	79
Logix 系统反应时间	79

系统反应时间

如要确定任意一个控制链的系统反应时间，必须累加安全链中所有组件的反应时间。

系统反应时间 = 传感器反应时间 + Logix 系统反应时间 + 执行器反应时间

图 19- 系统反应时间

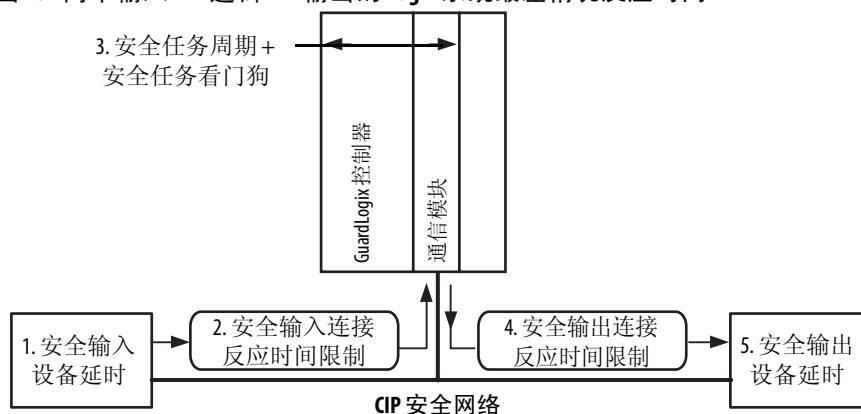


Logix 系统反应时间

下文提供了关于通过逻辑链中的生产者 / 消费者安全标签来计算简单输入 — 逻辑 — 输出链以及一个更为复杂应用项目的 Logix 系统反应时间的信息。

简单输入 — 逻辑 — 输出链

图 20 - 简单输入 — 逻辑 — 输出的 Logix 系统最差情况反应时间



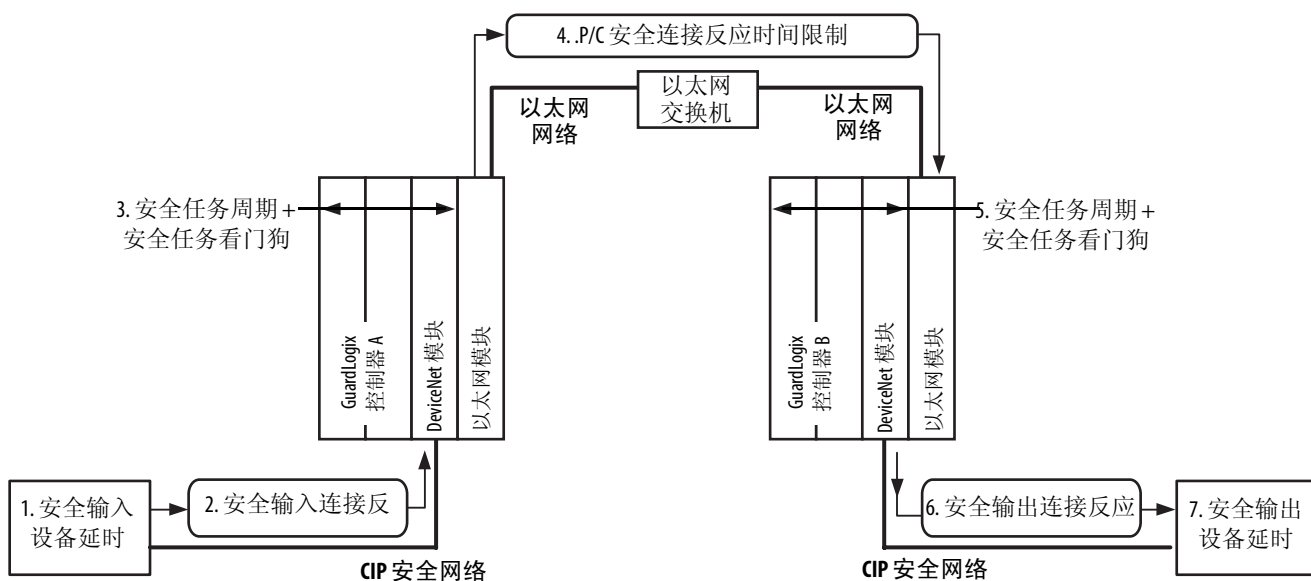
任何简单输入 — 逻辑 — 输出链的 Logix 系统反应时间都包含以下五个部分：

1. 安全输入设备反应时间 (+ 输入延迟时间，如果有的话)
2. 安全输入连接反应时间限制 (从 Logix Designer 应用程序的 Module Properties (设备属性) 对话框中读取，该值是安全输入设备连接 RPI 的倍数。)
3. 安全任务周期 + 安全任务看门狗时间
4. 安全输出连接反应时间限制 (从 Logix Designer 应用程序的 Module Properties (模块属性) 对话框中读取，该值是安全任务周期的倍数。)
5. 安全输出设备反应时间

为帮助您确定特定控制环的反应时间，在 Studio 5000 环境光盘的 Tools (工具) 文件夹下提供了一个 Microsoft Excel 电子数据表。

使用生产者 / 消费者安全标签的逻辑链

图 21- 输入 — 控制器 A 逻辑 — 控制器 B 逻辑 — 输出链的 Logix 系统反应时间



任何输入 — 控制器 A 逻辑 — 控制器 B 逻辑 — 输出链的 Logix 系统反应时间都包含以下七个部分：

1. 安全输入设备反应时间 (+ 输入延迟时间，如果有的话)
2. 安全输入连接反应时间限制
3. 控制器 A 的安全任务周期 + 安全任务看门狗时间
4. 生产者 / 消费者安全连接反应时间限制
5. 控制器 B 的安全任务周期 + 安全任务看门狗时间
6. 安全输出连接反应时间限制
7. 安全输出设备反应时间

为帮助您确定特定控制环的反应时间，在 Studio 5000 环境光盘的 Tools (工具) 文件夹下提供了一个 Microsoft Excel 电子数据表。

影响 Logix 反应时间分量的因素

上述的 Logix 反应时间分量受大量因素的影响。

表 13 - 影响 Logix 系统反应时间的因素

以下反应时间分量	受以下因素的影响
输入设备延时	输入设备反应时间
	每个输入通道的接通 — 关闭和关闭 — 接通延时设置 (适用的话)
安全输入连接反应时间限制	输入设备设置 • 请求数据包间隔 (RPI) • 超时乘数 • 延时乘数
	网络通信量
	系统的 EMC 环境
安全任务周期和安全任务看门狗	安全任务周期设置
	安全任务看门狗设置
	安全任务中的指令数量和执行时间
	可能优先于安全任务执行的任何高优先级任务
生产者 / 消费者安全连接反应时间限制	用于以下各项的消费者标记设置： • RPI • 超时乘数 • 延时乘数
	网络通信量
	系统的 EMC 环境
输出连接反应时间限制	安全任务周期设置
	用于以下各项的输出设备设置： • 超时乘数 • 延时乘数
	网络通信量
	系统的 EMC 环境
输出模块延时	输出模块反应时间

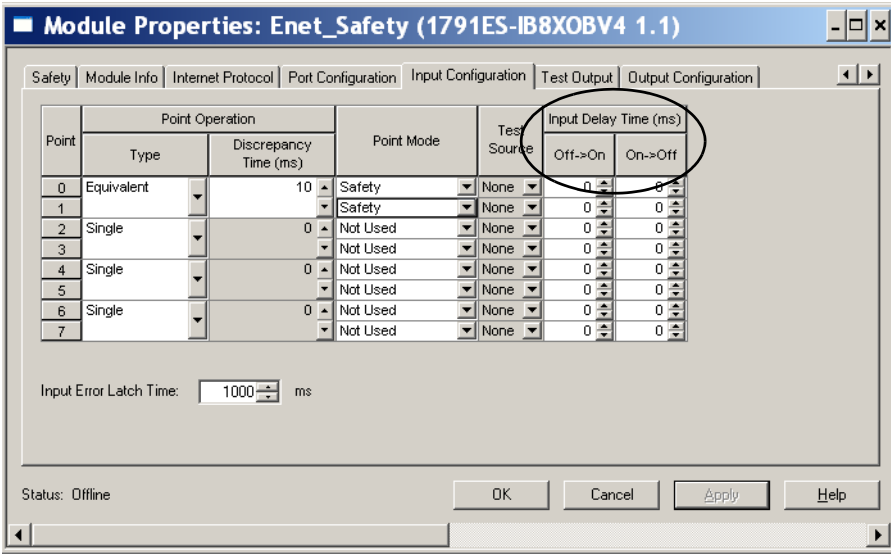
下文描述了如何访问这些因数的数据或设置。

访问 Guard I/O 输入模块延迟时间设置

请按以下步骤在 Logix Designer 应用程序中配置输入模块延迟时间。

1. 在配置树中右击 Guard I/O 模块，然后选择 Properties (属性)。
2. 单击 Input Configuration (输入配置) 选项卡。

3. 根据应用项目的要求调节输入延迟时间。



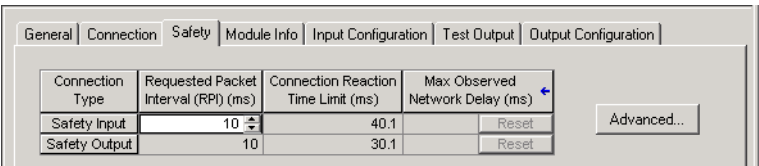
访问输入和输出安全连接反应时间限制

连接反应时间限制由以下三个值进行定义：

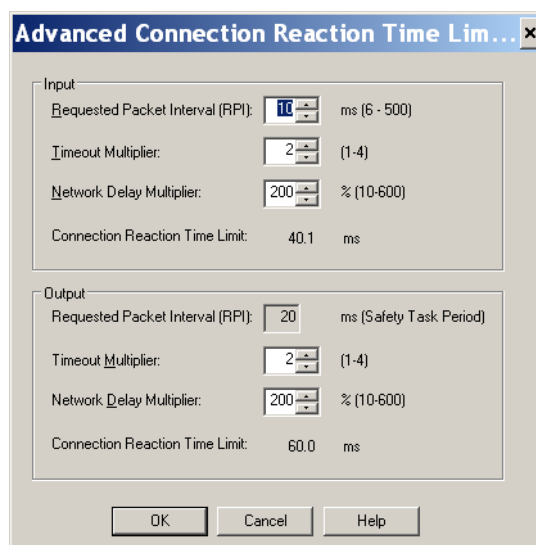
值	说明
请求数据包间隔 (RPI)	输入和输出数据包置入线路 (网络) 的频率。
超时乘数	超时乘数本质上是超时之前执行的重试次数。
网络延时乘数	网络延时乘数计算线路上已知的延时。当发生这些延时 时，可使用此参数避免超时。

通过调节这些值，可以调节连接反应时间限制。按以下步骤查看或配置这些设置。

- 1. 在配置树中右击安全 I/O 设备，然后选择 Properties (属性)。
- 2. 单击 Safety (安全) 选项卡。



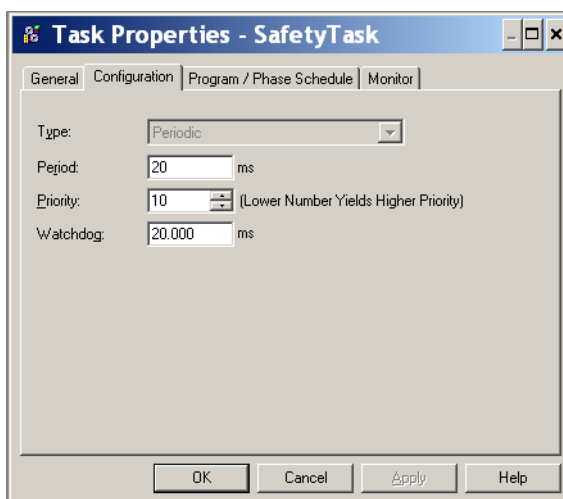
3. 单击 Advanced (高级), 打开 Advanced Connection Reaction Time Limit (高级连接反应时间限制) 对话框。



配置安全任务周期和看门狗

安全任务是一种周期性定时任务。通过 Logix Designer 项目中的 Task Properties - Safety Task (任务属性 — 安全任务) 对话框选择任务优先级和看门狗时间。

为了访问安全任务周期和看门狗时间设置, 右击 Safety Task (安全任务), 然后选择 Properties (属性)。

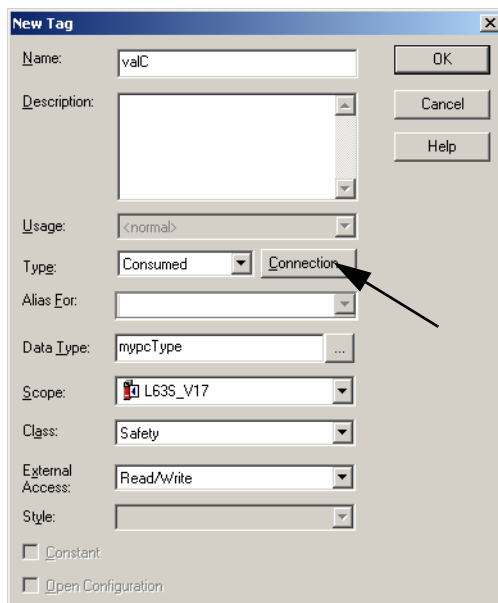


安全任务的优先级与安全无关, 因为安全任务看门狗监控该任务是否被更高优先级的任务中断。

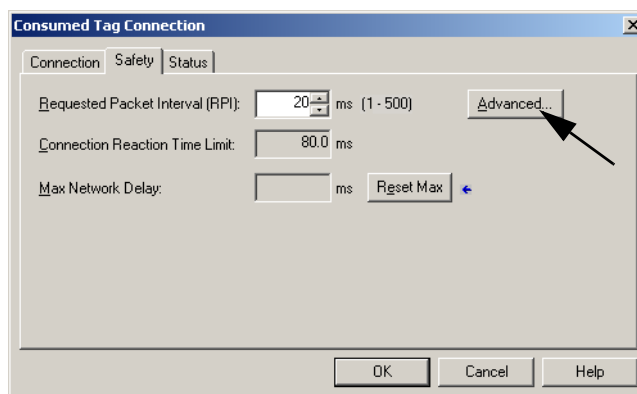
访问生产者 / 消费者标签数据

按以下步骤查看或配置安全标签连接数据。

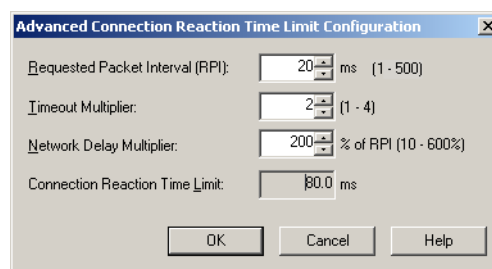
1. 在配置树中右击 **Controller Tags** (控制器标签), 然后选择 **Edit tags** (编辑标签)。
2. 在标签编辑器中, 右击标签名称, 然后选择 **Edit Properties** (编辑属性)。
3. 单击 **Connection** (连接)。



4. 单击 **Safety** (安全) 选项卡。



5. 单击 Advanced (高级), 查看或编辑当前设置。



如需了解更多信息，请参见 GuardLogix 5570 Controllers User Manual (GuardLogix 5570 控制器用户手册，出版号：[1756-UM022](#))。

GuardLogix 安全应用项目的检查表

主题	页码
GuardLogix 控制器系统的检查表	88
安全输入检查表	89
安全输出的检查表	90
开发安全应用程序的 检查表	91

当规划、编程和启动 SIL 3 认证 GuardLogix 应用项目时，要求使用本附录中的检查表。它们既可作为规划指南，也可在项目验证测试期间使用。如果用作规划指南，则可将检查表另存为计划记录。

下文的检查表提供了安全注意事项的一个示例，并非是包含所校验条目的完整列表。特定的安全应用项目可能还有附加安全要求，我们为此在检查表中留出了空间。

提示 复制检查表，并保存这些文件以备将来使用。

GuardLogix 控制器系统的检查表

GuardLogix 系统的检查表				
公司				
网站				
安全功能定义				
编号	系统要求	是否满足		备注
		是	否	
1	您是否仅使用 SIL 3 认证 GuardLogix 组件 on page 16 以及 http://www.rockwellautomation.com/products/certification/safety/ 网址中列出的具有相应固件版本的组件?	☐	☐	
2	您是否计算了每个安全链的系统安全响应时间?	☐	☐	
3	系统响应时间是否包括了用户自定义的安全任务程序看门狗(软件看门狗)时间和安全任务速率/周期?	☐	☐	
4	系统响应时间与过程容许时间之间的关系是否正确?	☐	☐	
5	是否根据系统配置计算了概率(PFD/PFH)值?	☐	☐	
6	是否执行了所有合适的项目验证测试?	☐	☐	
7	是否确定了系统处理故障的方式?	☐	☐	
8	安全系统中的每个网络是否都有一个唯一的 SNN?	☐	☐	
9	每个 CIP 安全设备是否都配置了正确的 SNN?	☐	☐	
10	是否已生成了安全任务签名?	☐	☐	
11	是否上传并记录了安全任务签名,以供将来比较?	☐	☐	
12	下载后,是否确认了控制器中的安全任务签名与所记录的安全任务签名一致?	☐	☐	
13	当在线编辑时,是否有另一种机制来保持系统的安全完整性?	☐	☐	
14	是否考虑了第 89 和 90 页列出的 SIL 输入和输出使用检查表?	☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	

安全输入检查表

当编程或启动时，可以为系统中的每个 SIL 输入通道填写单独的检查表。这是确保完全并明确实现要求的唯一方法。该检查表还可作为将外部接线连接到应用程序的指导文档使用。

GuardLogix 系统的输入检查表

公司				
网站				
安全功能定义				
SIL 输入通道				
编号	输入设备要求	是否满足		备注
		是	否	
1	您是否遵守了安装说明和预防措施，从而满足适用的安全标准？	☐	☐	
2	您是否在系统和设备上执行了项目验证测试？	☐	☐	
3	是否在应用项目逻辑中按顺序执行了控制、诊断和报警功能？	☐	☐	
4	是否上传了每个设备的配置，并将每个设备的配置与配置工具发送的配置进行了比较？	☐	☐	
5	是否根据 ISO 13849-1 的 PLe/Cat 4 要求连接了设备？ ⁽¹⁾	☐	☐	
6	是否确认了传感器和输入的电气技术规范兼容？	☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	

(1) 如需了解关于连接 CIP 安全 I/O 设备的信息，请参见特定设备的产品文档。

安全输出的检查表

当编程或启动时，必须为系统中的每个 SIL 输出通道填写单独的要求检查表。这是确保完全并明确实现要求的唯一方法。该检查表还可作为将外部接线连接到应用程序的指导文档使用。

GuardLogix 系统的输出检查表				
公司				
网站				
安全功能定义				
SIL 输出通道				
编号	输出设备要求	是否满足		备注
		是	否	
1	您是否遵守了安装说明和预防措施，从而满足适用的安全标准？	☐	☐	
2	您是否在设备上执行了项目验证测试？	☐	☐	
3	是否上传了每个设备的配置，并将每个设备的配置与配置工具发送的配置进行了比较？	☐	☐	
4	是否确认了测试输出没有用作为安全输出？	☐	☐	
5	是否根据 ISO 13849-1 的 PLe/Cat 4 要求连接了设备？ ⁽¹⁾	☐	☐	
6	是否确认了输出和执行器的电气技术规范兼容？	☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	

(1) 如需了解关于连接安全 I/O 设备的信息，请参见特定设备的产品文档。

开发安全应用程序的 检查表

当创建或修改安全应用程序时，使用以下检查表来帮助保持安全性。

GuardLogix 应用程序开发的检查表				
公司				
网站				
项目定义				
编号	应用程序要求	是否满足		备注
		是	否	
1	是否将版本 21 或更高版本的 Logix Designer 应用程序用作 GuardLogix 系统编程工具？	☐	☐	
2	在创建安全应用程序期间是否遵守了 章节 6 给出的编程指南？	☐	☐	
3	安全应用程序是否只包含继电器梯形图逻辑？	☐	☐	
4	安全应用程序是否只包含 附录 A 中列出的适合安全应用项目编程的指令？	☐	☐	
5	安全应用程序是否明确区别安全标签和标准标签？	☐	☐	
6	是否只将安全标签用于安全例程？	☐	☐	
7	是否已经确认安全例程没有尝试读写标准标签？	☐	☐	
8	是否已经确认没有将安全标签作为标准标签的别名使用，并且没有将标准标签作为安全标签的别名？	☐	☐	
9	每个安全输出标签是否正确配置并连接至物理输出通道？	☐	☐	
10	是否已经确认在安全应用逻辑中已经调节了所有已映射标签？	☐	☐	
11	是否定义了由故障例程监视的过程参数？	☐	☐	
12	是否用一个指令签名封装了所有用户自定义安全指令并记录了该安全指令签名？	☐	☐	
13	是否由独立的安全审查方审核了程序(如必要)？	☐	☐	
14	审核过程是否已归档并已签名？	☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	
		☐	☐	

备注:

GuardLogix 系统安全数据

主题	页码
PFD 值	93
PFH 值	94

以下示例显示了使用 Guard I/O 模块的 GuardLogix 1002 SIL 3 系统的要求故障概率 (PFD) 和每小时故障概率 (PFH) 值。

GuardLogix 控制器和 Guard I/O 模块的使用寿命为 20 年。

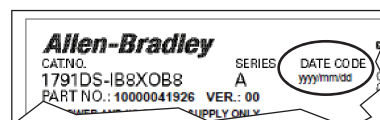
PFD 值

表 14 - 由验证测试时间间隔得出的 PFD

目录号	说明	得出的 PFD			
		2 年 (17,520 小时)	5 年 (43,800 小时)	10 年 (87,600 小时)	20 年 (175,200 小时)
1756-L7xS 和 1756-L7SP	GuardLogix 控制器	5.7E-06	1.5E-05	3.5E-05	8.9E-05
1756-L73SXT 和 1756-L7SPXT	GuardLogix-XT 控制器	5.7E-06	1.5E-05	3.5E-05	8.9E-05
1791DS-IB12	CIP 安全 12 点输入模块	4.73E-07	1.18E-06	2.35E-06	4.71E-06 ⁽²⁾
1791DS-IB16	CIP 安全 16 点输入模块	4.11E-06	1.03E-05	2.06E-05	4.11E-05
1791DS-IB8XOB8	CIP 安全 8 点输入 /8 点输出模块	4.73E-07	1.18E-06	2.35E-06	4.71E-06 ⁽²⁾
1791DS-IB4XOW4	CIP 安全 4 点输入 /4 点继电器输出模块	2.21E-05	7.05E-05	1.92E-04	5.88E-04 ⁽²⁾
1791DS-IB8XOBV4	CIP 安全 8 点输入 /4 双极性输出模块	4.16E-06	1.04E-05	2.08E-05	4.16E-05
1732DS-IB8XOBV4					
1732DS-IB8	CIP 安全 8 点输入模块	4.11E-06	1.03E-05	2.06E-05	4.11E-05
1791ES-IB16	CIP 安全 16 点输入模块	4.13E-06	1.03E-05	2.06E-05	—
1791ES-IB8XOBV4	CIP 安全 8 点输入 /4 双极性输出模块	4.17E-06	1.04E-05	2.09E-05	—
1734-IB8S, 系列 A	CIP 安全 8 点输入模块	4.23E-06	1.06E-05	2.11E-05	4.23E-05
1734-IB8S, 系列 B ⁽¹⁾	CIP 安全 8 点输入模块	4.36E-06	1.09E-05	2.18E-05	4.36E-05
1734-OB8S, 系列 A	CIP 安全 8 点输出模块	4.27E-06	1.07E-05	2.13E-05	4.27E-05
1734-OB8S, 系列 B	CIP 安全 8 点输出模块	4.32E-06	1.08E-05	2.16E-05	4.32E-05
1734-IE4S	CIP 安全 4 点模拟量输入模块, 单通道操作	4.7E-07	1.2E-06	2.4E-06	4.8E-06
1734-IE4S	CIP 安全 4 点模拟量输入模块, 双通道操作	3.2E-07	8.1E-07	1.6E-06	3.3E-06

(1) 该数据适用于单通道和双通道操作。

(2) 该产品的 20 年 PFD 数据仅适用于制造日期代码为 2009/01/01 (2009 年 1 月 1 日) 或之后的产品。有关日期代码, 请参见产品标签。



PFH 值

以下数据适用于达到 (包括) 20 年的验证测试时间间隔。

表 15 - PFH 计算

目录号	说明	PFH (1/ 小时)
1756-L7xS 和 1756-L7SP	GuardLogix 控制器	1.2E-09
1756-L7xSXT 和 1756-L7SPXT	GuardLogix-XT 控制器	1.2E-09
1791DS-IB12	CIP 安全 12 点输入模块	5.77E-11 ⁽¹⁾
1791DS-IB16	CIP 安全 16 点输入模块	4.96E-10
1791DS-IB8XOB8	CIP 安全 8 点输入 /8 点输出模块	5.77E-11 ⁽¹⁾
1791DS-IB4XOW4	CIP 安全 4 点输入 /4 点继电器输出模块	9.03E-09 ⁽¹⁾
1791DS-IB8XOBV4	CIP 安全 8 点输入 /4 双极性输出模块	5.02E-10
1732DS-IB8XOBV4		
1732DS-IB8	CIP 安全 8 点输入模块	4.96E-10
1791ES-IB16	CIP 安全 16 点输入模块	4.98E-10
1791ES-IB8XOBV4	CIP 安全 8 点输入 /4 双极性输出模块	5.04E-10
1734-IB8S, 系列 A	CIP 安全 8 点输入模块	5.10E-10
1734-IB8S, 系列 B	CIP 安全 8 点输入模块	5.27E-10
1734-OB8S, 系列 A	CIP 安全 8 点输出模块	5.14E-10
1734-OB8S, 系列 B	CIP 安全 8 点输出模块	5.20E-10
1734-IE4S	CIP 安全 4 点模拟量输入模块, 单通道操作	5.6E-11
	CIP 安全 4 点模拟量输入模块, 双通道操作	3.9E-11

(1) 该产品的 PFH 数据仅适用于制造日期代码为 2009/01/01 (2009 年 1 月 1 日) 或之后的产品。有关日期代码, 请参见产品标签。

RSLogix 5000 软件版本 14 及更高版本的安全应用项目指令

主题	页码
断电跳闸系统	95
使用连接状态数据以程序方式启动故障	95

断电跳闸系统

当使用 RSLogix 5000 软件版本 14 的安全应用项目指令时，所有输入和输出会在检测到故障后设为零。因此，由不同输入指令之一（不同输入或双路运行站）监视的任一输入应具有由逻辑调节的常闭输入，该逻辑与第 98 页和第 99 页的“[梯形图逻辑示例 2](#)”和“[梯形图逻辑示例 3](#)”中逻辑行 4 的逻辑类似。所要求的实际逻辑取决于应用项目和输入设备。但是，逻辑必须为不同输入指令的常闭输入创建安全状态 1。

使用连接状态数据以程序方式启动故障

以下各图提供了锁定和复位 I/O 故障所要求的应用逻辑示例。这些示例显示了仅输入模块以及输入和输出组合模块所需的逻辑。这些示例使用 I/O 模块的“组合状态”功能，它在一个布尔变量中表示所有输入通道的状态。另一个布尔变量表示所有输出通道的状态。该方法可减少所要求的 I/O 调节逻辑的数目，并强制逻辑关闭受影响模块上的所有输入和输出通道。

使用第 96 页的“[输入故障锁定和复位流程图](#)”来确定不同应用情况所要求的逻辑行。[梯形图逻辑示例 1](#) 显示了在存在故障情况时负责改写实际输入标签变量的逻辑。如果在输入故障锁定时要求使用实际输入状态进行故障诊断，则使用“[梯形图逻辑示例 2](#)”中显示的逻辑。该逻辑使用内部标签，这些标签表示要在应用项目逻辑中使用的输入。当锁定输入故障时，将内部标签设为它们的安全状态。当输入故障未锁定时，将实际输入值复制到内部标签。

使用“[输出故障锁定和复位流程图](#)”来确定在第 99 页的“[梯形图逻辑示例 3](#)”中要求使用哪些应用逻辑行。

图 22- 输入故障锁定和复位流程图

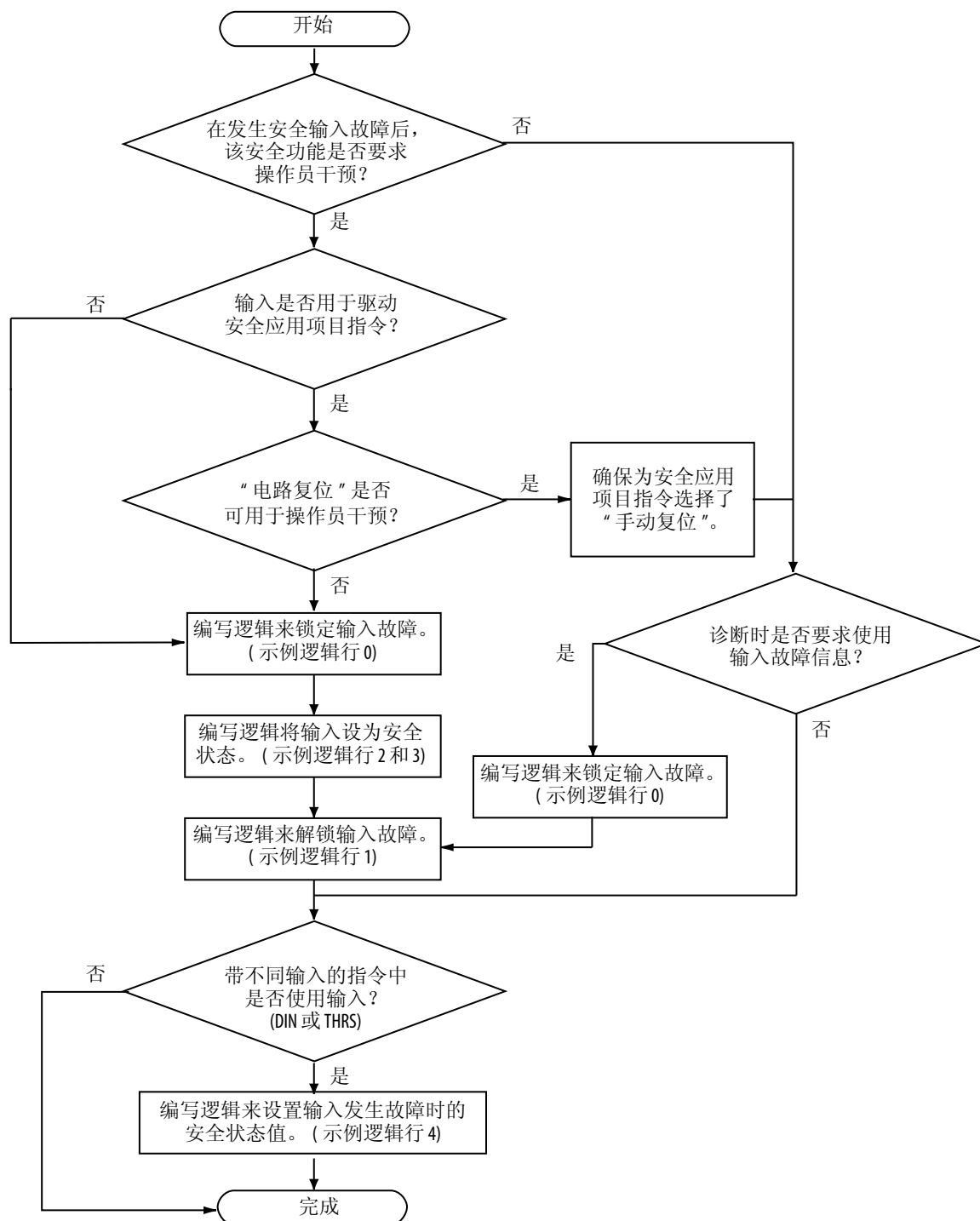


图 23 - 梯形图逻辑示例 1

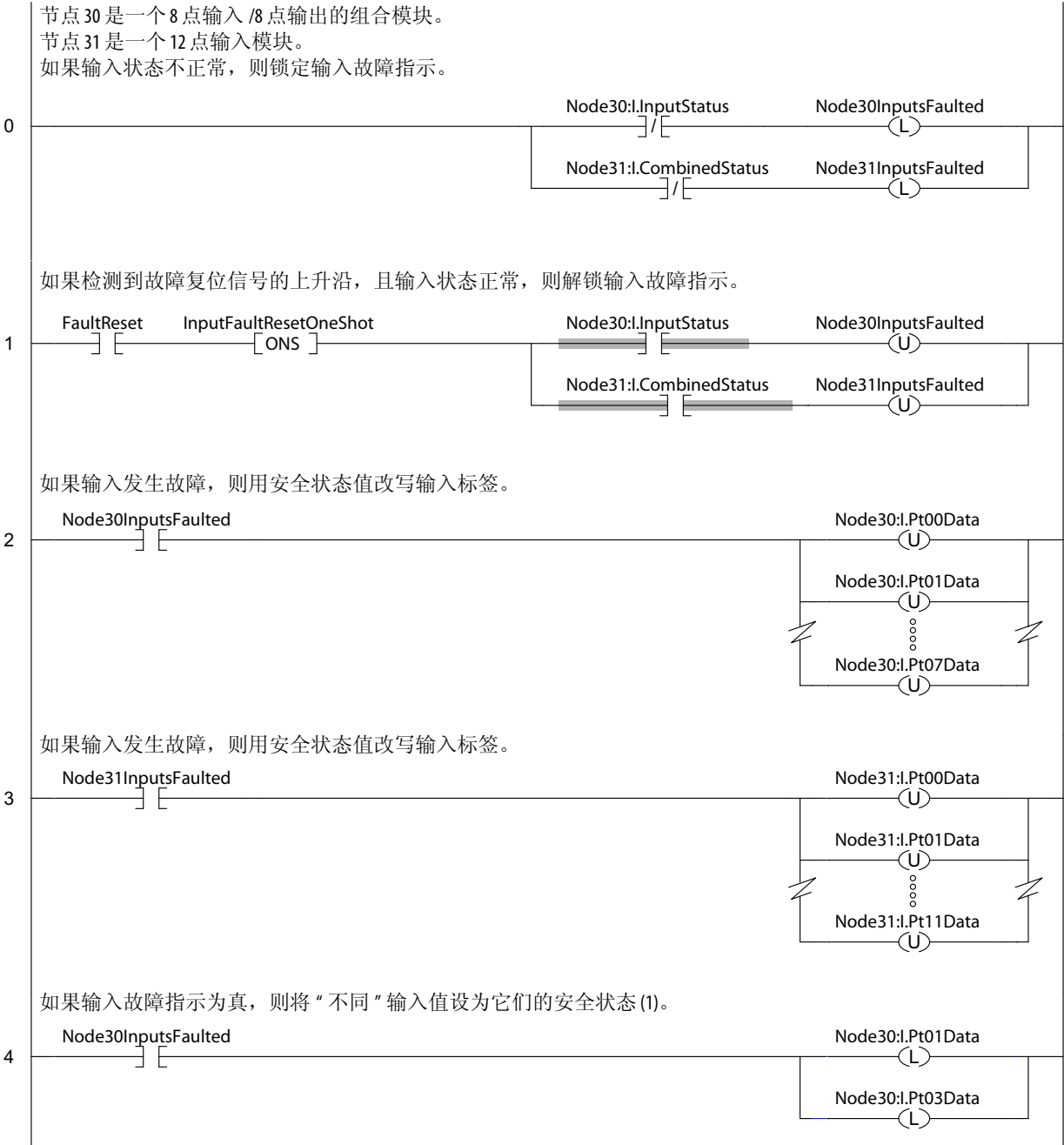


图 24- 梯形图逻辑示例 2

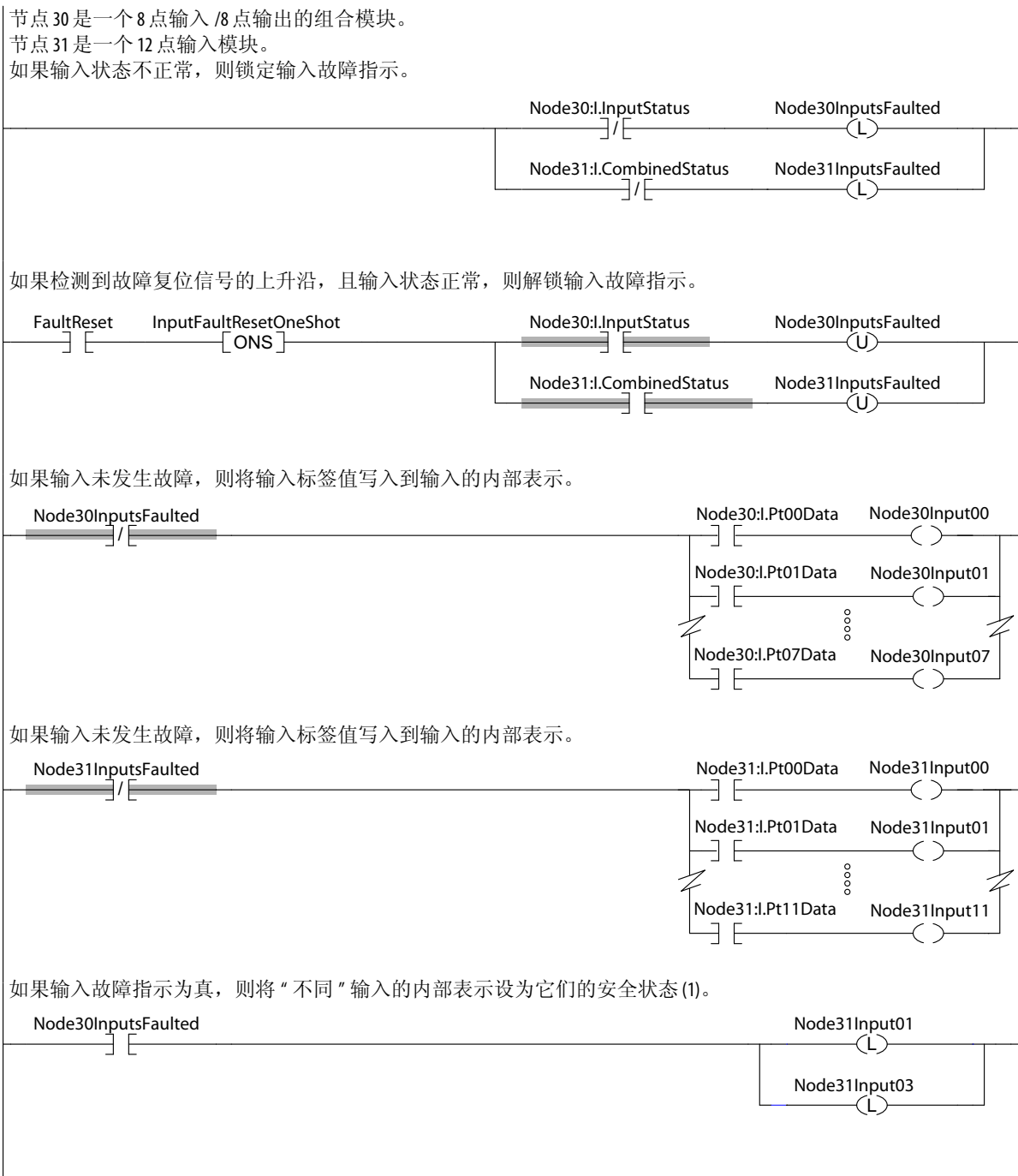


图 25 - 输出故障锁定和复位流程图

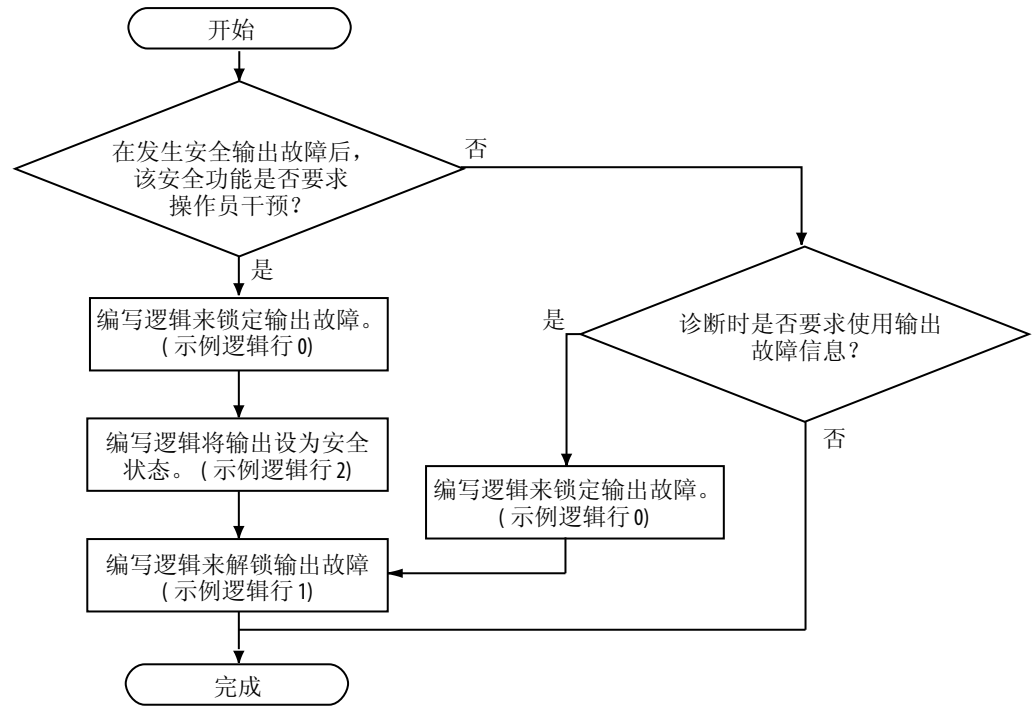
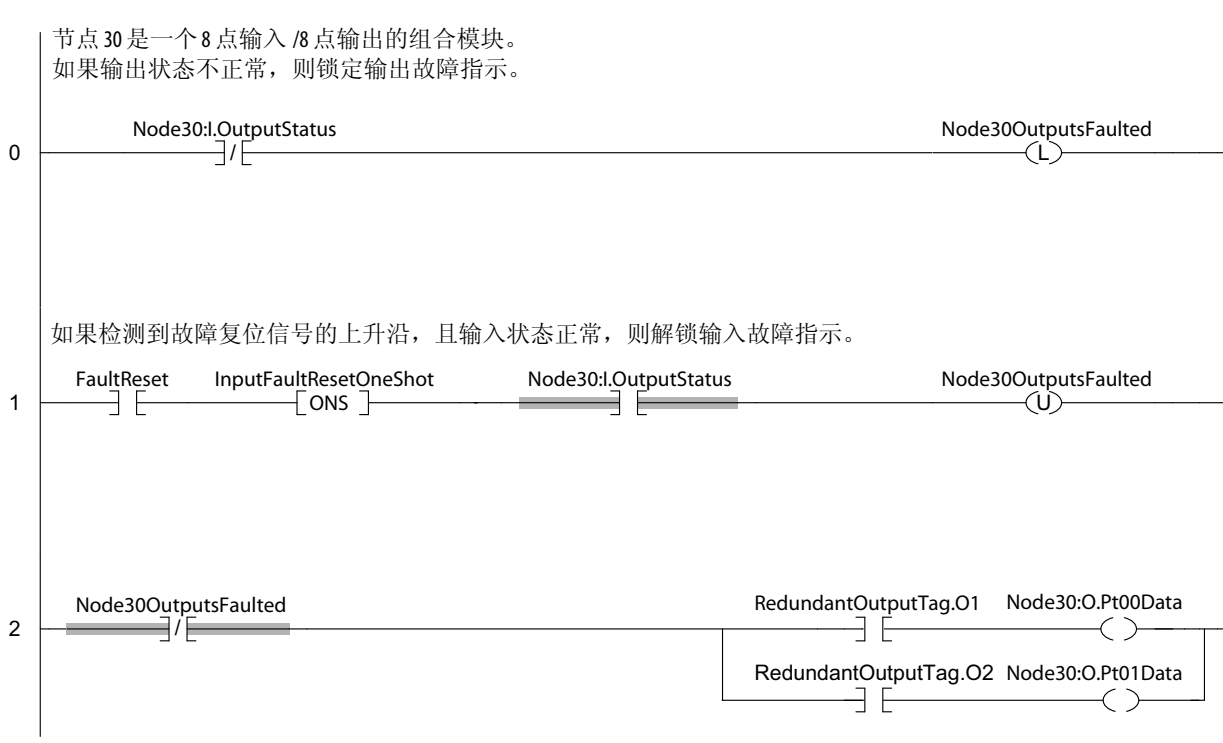


图 26 - 梯形图逻辑示例 3



备注:

将 1794 FLEX I/O 模块、 1756 SIL 2 输入和输出与 1756 GuardLogix 控制器组合使用，以符合 EN 50156 标准要求

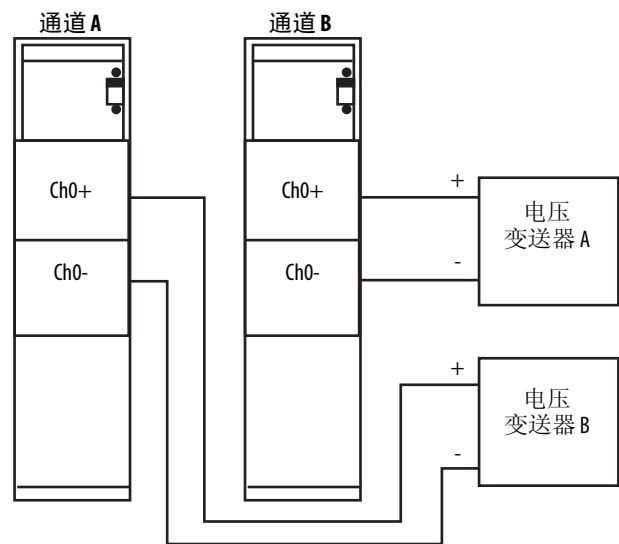
主题	页码
SIL 2 双通道输入 (GuardLogix 控制器的标准侧)	101
使用 SIL 3 Guard I/O 输出模块的 SIL 2 输出	103
使用 1756 或 1794 SIL 2 输出模块的 SIL 2 输出	103
1756 GuardLogix 安全任务内的安全功能	104

为符合某些安全相关应用项目 (包括燃烧炉相关安全功能) 的要求，需要使用双通道配置。这些示例提供旨在满足 EN50156 SIL 2 双通道要求 (1 年和 2 年验证测试间隔) 的指南信息。

SIL 2 双通道输入
(GuardLogix 控制器的
标准侧)

必须在两个输入通道之间实现清晰、易识别的隔离，并遵照 Using ControlLogix in SIL 2 Applications (在 SIL 2 应用项目中使用 ControlLogix，出版号：[1756-RM001](#)) 中规定的所有现有的 SIL 2 要求。

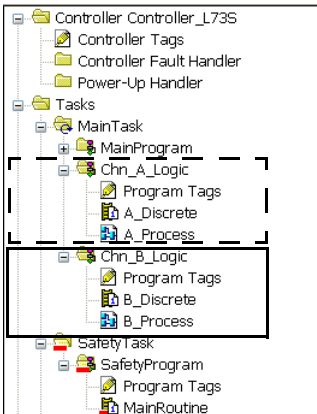
图 27 - SIL 2 双通道输入示例 F



SIL 2 输入数据

在任何时候，应始终隔离通道 A 和通道 B 输入数据。该示例阐述了一种在应用项目中隔离通道 A 和通道 B 数据的方法。

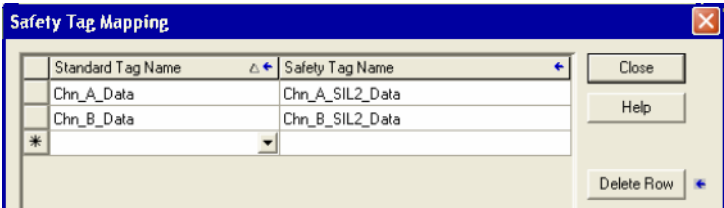
应遵照 Using ControlLogix in SIL 2 Applications Safety Reference Manual (SIL 2 应用安全等级下使用 ControlLogix 参考手册，出版号：[1756-RM001](#)) 中规定的 1756 I/O 模块和 1794 FLEX™ I/O 模块的所有规则。



重要事项 不得在这些例程内执行安全相关功能。必须在 1756 GuardLogix 安全任务中处理安全评估。

将 SIL 2 数据传送到安全任务中

若要将通道 A 和通道 B 的 SIL 2 安全数据传送到 GuardLogix 安全任务，可使用 Logix Designer 应用程序中的安全标签映射功能。此处使用的标签名称仅用于举例。执行并遵守适用于应用项目的命名规定。



提示 若要使用安全标签映射功能，从 Logix Designer 应用程序的 Logic (逻辑) 菜单中选择 Map Safety Tags (映射安全标签)。

使用 SIL 3 Guard I/O 输出模块的 SIL 2 输出

- 对于 SIL 2 输出，应符合以下准则：
- 必须将用于 SIL 2 安全输出的 Guard I/O 输出模块配置成双通道工作模式。
 - 所有 Guard I/O 输出模块已获准用于 SIL 2 应用项目。
 - 1732DS-IB8XOBV4
 - 1791ES-IB8XOBV4
 - 1791DS-IB8XOBV4、1791ES-IB8XOBV4
 - 1791DS-IB4XOW4
 - 1791DS-IB8XOB8
 - 1734-OB8S

使用 1756 或 1794 SIL 2 输出模块的 SIL 2 输出

当使用这些 SIL 2 等级输出模块时，要求您将 SIL 2 安全输出配置为 GuardLogix 生产者安全标签，以符合 EN 50156 中的双通道要求。

创建带有应用项目所要求的 SIL 2 输出的生产者安全标签。GuardLogix 生产者 / 消费者安全标签要求将第一个成员分配给诊断。生产者 / 消费者安全连接的第一个成员的数据类型必须为 CONNECTION_STATUS。该示例显示了一个带有 2 个 INT 成员和 2 个 BOOL 成员的 SIL 2 标签。使用这些 SIL 2 安全标签来直接控制 1756 或 1794 SIL 2 输出。

Name	Alias For	Base Tag	Data Type	Class	Description	External Access	Constant	Style
SIL2_Outputs			SIL_2_Produced	Safety		Read/Write	☐	
SIL2_Outputs.Connection_Status			CONNECTION_STA	Safety		Read/Write		
SIL2_Outputs.SIL2_TempA			INT	Safety		Read/Write		Decimal
SIL2_Outputs.SIL2_TempB			INT	Safety		Read/Write		Decimal
SIL2_Outputs.SIL2_Valve1			BOOL	Safety		Read/Write		Binary
SIL2_Outputs.SIL2_Valve2			BOOL	Safety		Read/Write		Binary

提示 在本例中，未显示生产者标签对应的消费者。如果没有配置消费者，则连接状态将显示故障。但是，在该配置类型中，不要求对生产者标签的连接状态进行监视，因此是否发生故障并不重要。

应遵照 Using ControlLogix in SIL 2 Applications Safety Reference Manual (SIL 2 应用安全等级下使用 ControlLogix 参考手册，出版号：[1756-RM001](#)) 中规定的 1756 I/O 模块和 1794 FLEX I/O 模块的所有规则。

1756 GuardLogix 安全任务内的安全功能

在安全任务内使用 SIL 2 和 SIL 3 安全功能时应遵照下列指南：

- 可使用所有可用的安全应用项目指令。
- SIL CL3 安全输入模块 (即 Guard I/O 模块) 可对 SIL 2 安全功能使用单通道配置。
- 建议使用安全任务签名和安全锁定应用项目。

重要事项	不得使用 SIL 2 数据来直接控制 SIL 3 输出。
-------------	------------------------------

本手册使用以下术语和缩略词。对于此处未列出的术语定义，请参见 Allen-Bradley Industrial Automation Glossary (Allen-Bradley 工业自动化术语表，出版号：[AG-7.1](#))。

CIP 安全协议	一种网络通信方法，设计用于传输高完整性数据，并已通过认证。
安全 I/O	除了通过 SIL 3 认证的数据完整性机制，安全 I/O 的大部分属性与标准 I/O 相同。
安全标签	除 GuardLogix 控制器提供 SIL 3 认证机制来确保相关数据的完整性外，安全标签具有标准标签的所有属性。它们可以属于程序作用域或控制器作用域。
安全程序	安全程序具备标准程序的所有属性，但它只能在安全任务中调度。安全程序由零个或多个安全例程组成。它不能包含标准例程或标准标签。
安全伙伴	双处理器控制器中的处理器，它与主控制器共同执行安全相关的功能。
安全例程	安全例程具有标准例程的所有属性，但它仅在安全程序内有效，并包含一个或多个适用于安全应用项目的指令。（有关可在安全例程逻辑中使用的安全应用项目指令和标准 Logix 指令的列表，请参见 附录 A 。）
安全任务	安全任务具有标准任务的所有属性，但它只在 GuardLogix 控制器中有效，且只能由安全程序调度。一个 GuardLogix 控制器中只有一个安全任务。安全任务必须是周期性 / 定时任务。
安全任务反应时间	安全任务周期与安全任务看门狗时间之和。该时间是从给 GuardLogix 控制器提供任何输入更改到已处理的输出可供生产连接使用之间的最大延时。
安全任务看门狗	从安全任务执行开始到安全任务执行结束所允许的最大时间。超出安全任务看门狗会触发不可恢复的安全故障。
安全任务签名	一个由固件计算的数值，该数值是表示安全系统的逻辑与配置的唯一途径。其作用是在下载到控制器过程中校验安全应用程序的完整性。
安全任务周期	安全任务执行的周期。

安全网络编号 (SNN)	识别安全系统中所有网络中的某个网络的唯一标识。最终用户负责为系统内的每个安全网络或安全子网分配一个唯一编号。安全网络编号构成唯一节点标识符 (UNID) 的一部分。
安全应用项目指令	提供安全相关功能的安全指令。这些指令经过 SIL 3 认证，可在安全例程中使用。
安全指令签名	安全指令签名是一个 ID 号，用来识别用户自定义安全指令的执行特性。它用于在下载至控制器的过程中校验用户自定义安全指令的完整性。
安全组件	标记为安全相关条目的任意对象、任务、程序、例程、标签或模块。
标准控制器	在本文档中，标准控制器通常指 ControlLogix 控制器。
标准组件	不标记为安全相关条目的任意对象、任务、标签、程序等。
不可恢复的安全故障	即使在由安全控制器提供且由用户实现的故障处理机制正确处理时，此类故障也会终止所有安全任务处理，并要求采取外部用户动作来重新启动安全任务。
不可恢复的控制器故障	一种会强制所有处理终止，并要求控制器电源断开后重新接通的故障。此时用户程序不会被保留，必须重新下载。
超时乘数	该数值确定在声明连接错误之前可能丢失的报文数目。
重叠	指任务 (周期性或事件性) 经过上次触发还在执行时又被触发的情况。
待定编辑	在 Logix Designer 应用程序中更改了某个例程，但尚未通过接受编辑将所作的更改传送到控制器。
符号寻址	一种寻址方法，旨在提供标签名的 ASCII 解释。
伙伴关系	必须同时存在主控制器和安全伙伴，且硬件和固件必须兼容，才能建立伙伴关系。
可恢复的故障	当通过实施由控制器提供的故障处理机制进行正确处理时，该故障不会强制终止用户逻辑执行。

- 例程** 以一种编程语言表示的一组逻辑指令，例如，梯形图。例程为控制器中的项目提供可执行代码。每个程序都有一个主例程。此外，还可指定可选例程。
- 配置签名** 用于标识设备配置的唯一编号。配置签名由 ID 号、日期和时间组成。
- 请求数据包间隔 (RPI)** 当通过网络通信时，该值是连续生产输入数据之间的最大时间。
- 取消编辑** 为拒绝任何未组合的在线编辑更改所采取的措施。
- 任务** 一种用于执行程序的调度机制。任务为根据某些标准执行的一组程序 (一个或多个) 提供调度和优先级信息。一旦任务被触发 (激活)，所有的分配 (预定) 到该任务的程序将按照它们在控制器项目管理器中显示的顺序执行。
- 系统反应时间** 从作为系统输入或作为系统故障的安全相关事件发生到系统处于安全状态之间的最大时间。系统反应时间包括传感器和激励器反应时间以及控制器反应时间。
- 用户自定义安全指令** 一种可使用安全应用项目指令的用户自定义指令。除用于高完整性的用户自定义指令的指令签名外，用户自定义安全指令还提供在安全相关功能中使用的 SIL 3 安全指令签名。
- 用户自定义指令** 用户创建的作为 Logix 指令集组成部分的指令。一旦定义，用户自定义指令就可以与其他任何 Logix 指令一样使用，并可跨项目使用。用户自定义指令由参数、本地标签、逻辑例程和可选的扫描模式例程组成。
- 有效连接** 安全连接是开放、活动且没有错误的连接。
- 在线** 监视 / 修改控制器中程序的一种状态。
- 指令签名** 指令签名由 ID 号、日期 / 时间戳组成，用于标识给定时间点的用户自定义指令定义的内容。

- 周期性任务** 一种由操作系统以重复的周期触发的任务。当时间到时后，触发该任务并执行其程序。由任务中的程序建立的数据和输出保持其数值不变，直到下一次执行任务或由另一个任务操作这些数据和输出。周期性任务始终中断连续任务。
- 主控制器** 双处理器控制器中的一种处理器，它执行标准控制器功能，并与安全伙伴通信，以执行安全相关的功能。
- 组合编辑** 由于可以测试、取消测试或取消编辑，当对控制器程序完成了在线编辑修改，且希望所作修改成为永久性修改时，可以组合编辑。

数字

1734-AENT 17, 23
1756-A10 17
1756-A13 17
1756-A17 17
1756-A4 17
1756-A5XT 17
1756-A7 17
1756-A7XT 17
1756-CN2 17, 23
1756-CN2R 17, 23
1756-CN2RXT 17, 23
1756-DNB 17, 23
1756-EN2F 17, 23
1756-EN2T 17, 23
1756-EN2TR 23
1756-EN2TXT 17, 23
1756-EN3TR 23
1756-ENBT 17, 23
1756-PB72 17
1756-PB75 17
1768-CNB 23
1768-CNBR 23
1768-ENBT 23
1784-CF128 17
1784-SD1 17
1784-SD2 17

字母

CIP 安全协议
 定义 105
 概述 22
 可路由系统 33
CONNECTION_STATUS
 数据类型 63
ControlNet 网桥模块
 硬件概述 23
DeviceNet 安全
 通信概述 24
DeviceNet 扫描器接口模块
 硬件概述 23
EN50156 101
EN954-1
 CAT 4 9, 13
EtherNet/IP
 通信概述 23
EtherNet/IP 通信接口模块
 硬件概述 23
GSV 指令 65
Guard I/O 模块
 SIL 2 应用项目 103
I/O 模块
 替换 29-31
IEC 61508
 安全完整性等级 3 (SIL 3) 认证 9, 13, 76
ISO 13849-1 9, 13

Logix 系统反应时间

 计算 80

Logix 组件

 SIL 3 认证 16

PLe 9, 13

RSLogix 5000 软件 17

SIL 2

 EN50156 101

Studio 5000 环境 17

XT 组件 17

A

安全标签 46
 定义 105
 有效数据类型 46
安全程序 45
 定义 105
安全功能
 CIP 安全 I/O 27
 安全输出 28
安全伙伴
 定义 105
 位置 22
 硬件概述 22
安全例程 45
 定义 105
安全认证与合规性 18
安全任务
 定义 105
 反应时间 20, 105
 概述 41
 看门狗时间 84
 优先级 84
 执行 42
安全任务看门狗 20
 超时 41
 定义 105
 概述 20
 设置 20
 修改 20
安全任务签名
 定义 105
 删除 54
 生成 53
 受限操作 54
安全任务周期 20
 定义 105
 概述 20
 限制条件 41
安全数字 (SD) 卡 17
安全锁定 56
 密码 56
 缺省值 56
 受限操作 56
安全完整性等级 (SIL)
 策略 13-20
 符合性分配与权重 19
 功能示例 16

安全完整性等级 (SIL) 3 认证

- Logix 组件 16
- TÜV Rheinland 14
- 用户责任 14

安全完整性等级 3 (SIL 3) 认证 9, 13, 76**安全网络编号 34**

- 安全消费者标签 35
- 出厂模块 36
- 定义 106
- 手动分配 34

安全消费者标签

- 安全网络编号 35

安全应用项目指令

- 定义 106

安全原理

- 假设 49

安全指令签名 76

- 定义 106

安装控制器 21**B****标签**

- 安全 I/O 46
- 另请参见安全标签
- 生产者 / 消费者安全数据 46
- 不可恢复的安全故障 66, 106
- 重新启动安全任务 66
- 不可恢复的控制器故障 66, 106

C**超时乘数 82**

- 定义 106

程序

- 编辑生命周期 61
- 检查表 91
- 离线编辑 60
- 上传 57
- 识别 53
- 下载 56
- 验证 54
- 在线编辑 60

重叠

- 定义 106

存储卡 17**D****待定编辑 57****电源 17**

- 硬件概述 22

对等通信 23**F****反应时间**

- 安全任务 20
- 系统 19, 107
- 系统计算 79

G**更改应用程序 59****固件版本 17****故障**

- 不可恢复的安全故障 66
- 不可恢复的控制器故障 66
- 忽略 66
- 可恢复 67, 106

H**伙伴关系**

- 定义 106

获取系统值 (GSV)

- 定义 10

机构认证 18**机架**

- 产品目录号 17
- 硬件概述 22

J**检查表**

- GuardLogix 控制器系统 25, 88
- SIL 3 输出 90
- SIL 3 输入 89
- 程序开发 91
- 鉴定标准数据 47
- 界面
- HMI 用法和应用 43-45
- 禁止模块 58

K**看门狗时间 84****可恢复的故障 67, 106****可靠性负担 19****控制功能**

- 技术规范 52
- 控制和信息协议
- 定义 10

L**离线编辑 60****连接状态 64****M****每小时故障概率 (PFH) 18-19**

- 定义 10

O**欧洲标准**

- 定义 10

P

配置签名 29

Q

签名历史 77

强制赋值 58

请求数据包间隔

定义 107

范围 42

R

燃烧炉相关安全功能 101

人机界面

用法和应用 43-45

认证 18

软件

更改应用程序 59

S

设置系统变量 (SSV) 指令 65

输出延时 28

术语 10

所属关系 29

T

梯形图逻辑安全指令 70

调试生命周期 51

通信模块

产品目录号 17

硬件概述 23

W

唯一节点参考

已定义 34

X

系统反应时间 19

计算 79

项目

确认 55

项目验证测试 54, 78

性能等级

定义 10

Y

验证测试 14

要求故障概率 (PFD) 18-19

定义 10

应用程序

参见程序

更改 59

应用程序开发基础 50

映射标签 47

硬件故障

恢复 66

用户自定义指令

安全指令签名 76

认证 73

指令签名 75

在线

定义 107

在线编辑 57, 60

Z

章节 49

诊断覆盖率

定义 10

指令签名 75

定义 107

周期性任务

定义 108

主控制器

定义 108

硬件概述 22

罗克韦尔自动化公司支持

罗克韦尔自动化在网站上提供可帮助您使用其产品的技术信息。您可访问 <http://www.rockwellautomation.com/support>，获取技术和应用说明、示例代码和软件补丁包的链接。您也可以访问我们的支持中心 (<https://rockwellautomation.custhelp.com/>)，获取软件更新，寻求支持对话，浏览论坛，查询技术信息及常见问题，还可以在此注册，接收产品更新通知。

另外，我们还提供多种安装、配置和故障处理支持计划。更多信息，请联系您当地的分销商或罗克韦尔自动化代表处，也可以访问 <http://www.rockwellautomation.com/services/online-phone>。

安装帮助

如果您在安装后的 24 小时内遇到问题，请查看本手册中包含的信息。您可以联系客户支持，获取使产品功能正常运行的初步帮助。

美国或加拿大	1.440.646.3434
美国或加拿大以外的其它地区	使用 http://www.rockwellautomation.com/rockwellautomation/support/overview.page 上的 Worldwide Locator ，或联系您当地的罗克韦尔自动化代表处。

新产品退货

在所有产品出厂前，罗克韦尔自动化公司都会进行测试，以确保产品完全可用。但是，如果您的产品因不能正常工作而需要退货，请遵照下列步骤。

美国	联系当地经销商。必须向经销商提供一个客户支持案例号 (拨打上述电话获取)，以完成退货过程。
美国以外地区	有关退货手续，请联系您当地的罗克韦尔自动化代表。

文档反馈

您的意见将有助于我们改进文档，更好地满足您的要求。如有任何关于如何改进本文档的建议，请填写 <http://www.rockwellautomation.com/literature/> 上提供的表单 (出版号: [RA-DU002](#))。

罗克韦尔自动化在其网站上保留了最新的产品环境信息：
<http://www.rockwellautomation.com/rockwellautomation/about-us/sustainability-ethics/product-environmental-compliance.page>。

中文网址 www.rockwellautomation.com.cn

新浪微博 www.weibo.com/rockwellchina

动力、控制与信息解决方案总部

美洲地区：罗克韦尔自动化，南二大街1201号，密尔沃基市，WI 53204-2496 美国，电话：(1) 414.382.2000，传真：(1) 414.382.4444

欧洲/中东/非洲：罗克韦尔自动化，NV, Pegasus Park, De Kleetlaan 12a, 1831布鲁塞尔，比利时，电话：(32) 2 663 0600，传真：(32) 2 663 0640

亚太地区：罗克韦尔自动化，香港数码港道100号数码港3座F区14楼1401-1403 电话：(852)2887 4788 传真：(852)2508 1486

中国总部：上海市徐汇区虹梅路1801号宏业大厦 邮编：200233 电话：(86 21)6128 8888 传真：(86 21)6128 8899

客户服务电话：400 620 6620 (中国地区) +852 2887 4666 (香港地区)

出版物 1756-RM099B-ZH-P - 2014 年 11 月

Supersedes Publication 1756-RM099A-EN-P - December 2012

©2014 年罗克韦尔自动化有限公司版权所有。保留所有权利。美国印刷。