ONE 系列

电子开关

安全手册

UNITED ELECTRIC CONTROLS

1XSW-SM_CH 01

本页特意留空。

ONE 系列电子开关
安全手册

目录

1 介绍

本安全手册内容为使用 One 系列电子开关（下称“本产品”）设计、安装、验证和维持安全仪表功能 (SIF) 的必要信息。以下简称“装置”。最终用户有责任遵循本手册中列出的必要要求，以保证满足 IEC 61508 或 IEC 61511 功能安全标准。

1.1 术语与缩写

安全	免受不可接受的伤害风险。
功能安全	系统执行达成或维持受其控制的设备/机械/产线/仪表的规定安全状态所需之必要操作的能力。
基本安全	设备在设计和制造方面必须保证能够针对导致人员触电伤害或其他伤害以及导致起火或爆炸的风险提供防护。此类防护措施必须在正常运行期间和单一故障时的所有条件下均保证有效。
安全评估	为判断安全相关系统能够达成的安全程度而根据相关证据对安全相关系统所做的调查。
故障安全状态	将相关输出置于不会导致危险工艺条件的用户定义安全状态。IAW 保持开启。
故障安全	在工艺未要求相关状态的时候导致相关输出进入用户规定故障安全状态的故障。
故障危险	导致无法对工艺要求做出响应（即无法进入用户定义故障安全状态）的故障。
故障危险 未检测到的	具有危险性、未在证明试验或仪器诊断的故障 测试或仪器诊断。
故障危险 检测到的	具有危险性、但通过验证或测试的故障 仪器诊断。
故障报警	不会造成误跳闸或妨碍安全功能、但会 导致自动诊断丧失且无法被另一次 诊断发现的故障。
故障报警	不会造成误跳闸或妨碍安全功能、但会 导致自动诊断丧失或误报 诊断指示 。
无影响故障	属于安全功能一部分的某个组件所发生的不会影响安全功能的故障。
低需模式	该模式下，需对安全相关系统进行操作的频率不超过证明试验频率两倍。

1.2 缩写

DTT	断电跳闸
DU	未检测到的危险
FMEDA	故障模式、影响和诊断分析
HFT	硬件容错
IAW	工作进行中 - 用于监测设备硬件和软件工作是否正常的自带诊断功能，用于提示操作员是否发生了会影响本产品安全性的问题。
MOC	变更管理 - 遵照政府监管部门要求执行任何工作活动时需遵循的具体程序。
PFD_{avg}	平均要求时故障概率
PLC	可编程逻辑控制器
SFF	安全故障率 - 导致安全故障或诊断的不安全故障的设备整体故障率的分数。
SIF	安全仪表功能 - 一套用于降低特定危害所带来风险的设备（一套安全回路）。
SIL	安全完整性等级 - 分配给 E/E/PE 安全相关系统的安全功能安全完整性要求的离散等级（四个等级之一），其中等级 4 为最高安全完整性等级，等级 1 则为最低。
SIS	安全仪表系统 - 包含一项或多项安全仪表功能的部署。一套 SIS 系统可包含传感器、逻辑运算器和最终元件的任意组合。

1.3 设备支持

United Electric Controls

180 Dexter Avenue

Watertown, MA 02472 USA

InsideSales@ueonline.com

电话： +1 617 923-6977

传真：+1 617 926-4354

如需美国国内市场或国际市场销售产品清单，请访问 www.ueonline.com/about-ue/sales-offices/。

产品支持（续）

丢失密码：

请发送邮件至 InsideSales@ueonline.com、电话拨打 +1 617 923-6977 或访问 www.ueonline.com/uuc 来获取唯一解锁代码。获取代码时需提供本产品铭牌上标出的 Kanban 编号（见图 1）。

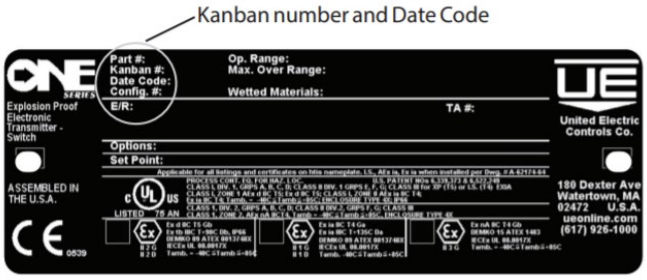

图 1

1.4 相关文档

硬件文档：

- One 系列电子开关安装和维护说明

  IM 1XSW-xx
- One 系列电子开关 FMEDA 报告 UE 21/01-054 R001
- One 系列电子开关产品手册 1X-B-xx
- 指导/参考资料：
  - 《实用 SIL 目标选择 - 基于 IEC 61511 安全寿命期的风险分析》，第二版，ISBN-13：978-1-934977-16-3，exida
  - 《控制系统安全评估和可靠性》，第三版，ISBN-13：978-1-934394-80-9，ISA
  - 《安全仪表系统验证：实用概率计算》，ations，ISBN-13：978-1556179099，ISA

1.5 参考标准

功能安全

- IEC 61508: 2010 电气/电子/可编程电子安全相关系统的功能安全
- ANSI/ISA 84.00.01-2004 (IEC 61511-1 Mod.) 功能安全：工艺行业领域用安全仪表系统

2 产品描述

本产品用于感应系统内温度或压力，提供控制输出以用于监测系统和出现不安全条件之前关闭系统。

开关输出是离散输出。IAW 输出是基于自诊断的一路离散输出，用于向用户指示本产品健康状况。IAW 输出工作于 DTT 中。诊断出的可导致 IAW 故障的任何失效均将强制所有输出进入故障安全状态。本产品的所有输出均在用户所选定的模式下运行，该模式可配置为断开进程的电源。

有关本产品的安装、编程和操作的详细信息以及系统环境图均请见《安装手册 IM_1XSW-xx》。

3 使用本产品设计 SIF

3.1 安全功能

已针对安全仪表系统用途对 IAW 和开关输出进行了评估。

设计人员必须验证所设计功能可以达到的 SIL 等级。

3.2 环境限制

SIF 设计人员必须核实本产品额定规格适用于预期环境限制条件。请查阅《产品手册 1X-B-xx》中的环境限制。

3.3 应用限制

本产品的制造材料详见《产品手册 1X-B-xx》。设计人员必须根据安装现场条件检查本产品的材料兼容性。如果将本产品用于应用限制之外或不兼容材料，所提供的可靠性数据将失效。

3.4 设计验证

详细的故障模式、影响和诊断分析 (FMEDA) 报告可从 United Electric Controls 获取，文档名为 UE 21/01-054 R001。该报告详述了所有故障率和故障模式以及预期寿命等方面信息。

整个安全仪表功能 (SIF) 设计可达到的安全完整性等级 (SIL) 需由设计人员利用对 PFD_{AVG} 的计算予以验证，验证时需考虑 SIF 中所含所有产品的架构、证明试验间隔、证明试验有效性、任何自动诊断、平均修复时间和具体故障率等。必须检查每个子系统以保证它们满足硬件容错 (HFT) 最低要求。建议采用 exida exSILentia® 工具进行这一检查，该工具内包含适用于本产品及其故障率的多个精准模型。

设计验证（续）

将本产品用于冗余配置时，应在安全完整性计算中纳入不小于 5% 的常见原因因素。

FMEDA 报告中给出的故障率数据仅针对本产品的使用寿命期有效。在此期限过后，故障率将有所升高。基于 FMEDA 报告中列出的数据针对寿命期限之后使用时间的可靠性计算得到的结果可能过于乐观，即实际上并无法达到计算得出的安全完整性等级。

3.5 SIL 能力

3.5.1 系统完整性

本产品满足制造商设计中的安全完整性等级 (SIL) 3 工艺要求。这是为了确保具有充分完整性以应对制造商设计中可能存在的系统误差。不得在最终用户未提供“之前使用”依据的情况下，或在设计中未准备多种技术冗余的情况下，将设计上采用本产品的安全仪表功能 (SIF) 用于高于所述的 SIL 等级。

3.5.2 随机完整性

本产品是一款 B 类产品。因此，基于 90% 到 99% 的 SFF，当本产品仅用作传感器元件子组件内的一个器件时，该设计可满足 SIL 2 @ HFT = 0。

当传感器元件组件包含多个器件时，必须利用所有器件的故障率验证整个组件的 SIL。验证分析时必须考虑到任何的硬件容错和架构限制条件。

3.5.3 安全参数

本产品的安全精度为工作范围的 3%。

详细的故障率信息请见本产品的 FMEDA 报告，
文档名为 UE 21/01-054 R001。

3.6 将本产品连接至 SIS 逻辑运算器

本产品可通过（最多）两路离散诊断状态输出连接至安全逻辑运算器。 逻辑运算器通过监测和解读本产品的输出信号来主动执行安全功能，设计上用于利用“工作进行中”(IAW) 诊断来发现设备中潜在的危险工艺条件和故障。

将本产品连接至 SIS 逻辑运算器（续）

本产品还可配置为在不连接至安全额定逻辑运算器的情况下直接提供安全功能。请参阅《产品手册 IM_1XSW-xx》中的系统环境图中有关如何利用各逻辑输出的详细信息。

3.7 一般要求

系统的响应时间应小于工艺安全时间。本产品的开关输出和 IAW 输出在特定延迟滤波设定下将在 100 毫秒以内进入其安全状态。可用的设置以及延迟滤波运行描述相关内容请参阅《产品安装手册 IM_1XSW-xx》。诊断间隔时间为 600 秒。

所有 SIS 部件，包括本产品均需在工艺启动之前保证工作正常。启动时，可能需在短暂延时之后各输出才能达到稳定。最终用户在应用中必须考虑到这一点，保证在各输出达到稳定状态之前无需依赖本产品实现对安全仪表系统的控制。从通电到输出稳定的时间应短于 10 秒。

最终用户应通过确认铭牌所示规格的方式，核实本产品适用于安全应用。

负责对本产品进行维护和测试的人员应具备所需资质和能力。

证明试验的结果应记录并定期审核。

本产品使用寿命方面信息请见 FMEDA 报告，文档名为 UE 21/01-054 R001。

4 安装和调试

4.1 安装

必须按照《产品安装手册 IM_1XSW-xx》中给出的标准程序来安装阿本产品。

禁止对本产品进行改造。

必须检查所处环境，以验证实际环境条件未超过《产品手册 1X-B-xx》中给出的本产品额定规格。

本产品必须位于便于抵达处以便实地检查。

详细的编程和操作说明请见《产品安装手册 IM_1XSW-xx》。SIF 设计人员应负责通过测试或通过再次进入编程菜单并回读所有设定的方法验证本产品的所有设定。最终用户需负责保护密码免遭泄露。附录中的本产品设定工作表可用于记录所有设定以便将来查阅。处于编程菜单时，IAW 和开关输出应保持激活。

本产品出厂时，插拔端口检测功能已关闭。如需使用此功能，须通过编程菜单予以启用，相关说明请见《产品安装手册 IM_1XSW-xx》。

4.2 物理位置和布置

本产品应安装在便于抵达且空间充足处，以便完成连接以及进行人工证明试验。

到本产品的管路应尽量短且直，以避免流动受限或堵塞的情况。管路过长或有所扭曲也有可能导致响应时间增加。

本产品应安装在低振动环境中。如果预期会有过度振动，则应采取专门应对措施，保证连接器完整性，或使用有缓冲作用的底座来减少振动造成的影响。

4.3 连接

到本产品的连接需遵循《产品安装手册 IM_1XSW-xx》。

到本产品的压力接口的建议方法请见《产品安装手册 IM_1XSW-xx》。本产品和压力接口之间的管路长度应尽量短且不折弯。

5 操作和维护

5.1 证明试验（无自动测试）

证明试验的目标是检测出本产品内未在自动诊断中检出的故障。我们的关切重点是阻碍安全仪表功能发挥其预期作用的未检出故障。

证明试验的频率，或者证明试验间隔，需在对本产品将用于的安全仪表功能的可靠性计算中确定。证明试验频率必须至少达到计算中给出的频率，以维持安全仪表功能的要求安全完整性。

以下建议的验证试验方法包括模拟工艺扰动和注入产品故障，并观察 SIF 对此类扰动的反应。证明试验的结果应予以记录，检测到的任何会破坏功能安全的故障均应报告至 United Electric Controls。

1. 在证明试验之前，应对本产品执行一次断通电循环，以清除可能已经发生的任何软错误。
2. 需绕过 PLC 或采取其他适当操作以避免误跳闸。
3. 验证正常状况下的输出均是正确的。开关应处于未跳闸状态。IAW 输出应处于闭合状态。我们建议检查本产品之外的开关连接，以避免拆开本产品的盖子。
4. 更改工艺变量设定，以使开关变为跳闸状态。验证 IAW 输出应保持闭合状态。
5. 更改工艺变量设定（建议压力采用极端最大压力，即传感器量程的 150%，或温度采用量程的 110%），使 IAW 输出进入故障状态（断开）。验证屏幕显示报错时 IAW 输出断开。

   或者，如果您仅想要测试 IAW 接线的最终连接情况，则可以将 IAW 接线从最终元件中拔出来验证连接从闭合变为断开。这可避免在本产品上强行制造一次出错的需要。
6. 将工艺变量恢复正常，验证各输出已恢复为各自的非跳闸状态。
7. 将回路恢复为完整运行。
8. 将跳线从 PLC 上取下，或相应以其他方式恢复正常运行。

请参阅 FMEDA 报告，文档名为 UE 21/01-054 R001 中的第 B.2 节中的证明试验覆盖范围。

负责进行本产品的证明试验的人员应已接收有关 SIS 操作的培训，包括如何绕过、维护和公司的变更管理程序等。拆下盖子需用到一把 2mm 内六角扳手。遵照《产品安装手册 IM_1XSW-xx》中的软件流程图来修改编程设定。

5.2 故障排除、维修和更换

如果发生故障，可参阅《产品安装手册 IM_1XSW-xx》中的完整故障代码列表和故障排除步骤说明。

本产品的维修和更换程序可联系 United Electric Controls 技术支持获取，您可电话拨打 617-923-6977 或发送邮件至 InsideSales@ueonline.com。

5.3 硬件和软件配置

本产品的型号请见铭牌的 PART# 一栏（图 1，页6）。 硬件和软件版本请见显示模块背面标签。

5.4 使用寿命

本产品的使用寿命为 50 年。

最终用户需负责正确停用本产品。停用后应遵照当地相关法律法规处置本产品。

5.5 厂家提示

发现的任何会破坏功能安全的故障均应告知 United Electric Controls。请联系 United Electric Controls 技术支持，您可电话拨打 617-923-6977 或发送邮件至 InsideSales@ueonline.com。

附录

附录包含两份文档，用于指导如何在 SIS 中部署本产品。这些文档应成为任何安全管理计划的一部分。

1. 《启动检查表》用于提供本产品部署指导。
2. 《产品设定工作表》用于记录各项设定。

本页特意留空。

启动检查表

应采用以下检查表来指导本产品在符合 IEC61508 的安全关键 SIF 中的部署。

#	活动	结果	验证	
			验证人	日期
	设计			
	确定目标安全完整性等级和 PFD_{avg}			
	选择正确模式（升时开、降时开、升时闭、降时闭，或窗口开、窗口闭）			
	选择正确的设定点和死区			
	记录设计决策			
	验证流体兼容性和稳定性			
	制定并记录自动测试的 SIS 逻辑运算器要求			
	确定流体连接管路的路径			
	正式审核设计，正式评估适用性			
	部署			
	确定适当物理位置			
	完成适当流体连接，保证符合相关规范			
	实施 SIS 逻辑运算器自动测试			
	发布用于证明试验的维护说明			
	发布验证和测试计划			
	正式审核部署，正式评估适用性			

启动检查表（续）

#	活动	结果	验证	
			验证人	日期
	验证和测试			
	验证和测试电气连接			
	验证和测试流体连接			
	验证 SIS 逻辑运算器自动测试			
	验证安全回路功能			
	测定安全回路正时			
	测试绕过功能			
	正式审核验证和测试结果，正式评估适用性			
	维护			
	测试管路堵塞/部分堵塞			
	测试安全回路功能			

产品设定工作表：

记录所有产品设定以便于参考查阅。有关本产品功能的详细解释，请参阅《产品安装手册 IM_1XSW-xx》。

产品 ID：_____

量程：_____

Kanban#：_____

密码：_____

测量单位：☐ psi（默认） ☐ bar/mbar ☐ KPa/MPa ☐ Kg/cm² ☐ “wc
☐ ° F（默认） ☐ ° C

开关模式：
☐ 升时开 ☐ 升时闭
☐ 降时开 ☐ 降时闭
设定点：_____
死区：_____

☐ 窗口开 ☐ 窗口闭
设定点（上限）：_____
死区（上限）：_____
设定点（下限）：_____
死区（下限）：_____

显示补偿：_____（标称 0.0）

量程跨度：_____（标称为产品的量程上限）

锁定模式：☐ 关闭（默认） ☐ 开启

插拔端口：☐ 关闭（默认） ☐ 开启 / 设置： ☐ 1Min ☐ 1HR ☐ 24HR

过滤器：

压力 ☐ 关闭（默认） ☐ 开启 / 设置： ☐ ¼Sec ☐ ½Sec ☐ 1Sec ☐ 2Sec

温度 ☐ 开启（默认）/ 设置： ☐ ½Sec（默认） ☐ 1Sec ☐ 2Sec

跳闸延迟：☐ 关闭（默认） ☐ 开启 / 设置：_____（0 到 999.9 sec）

如需我司国际和国内销售办事处完整列表，请访问 www.ueonline.com

UNITED ELECTRIC CONTROLS
180 Dexter Avenue
Watertown, MA 02472 USA
电话：+1 617 926-1000
传真：+1 617 926-2568
http://www.ueonline.com