UNITED ELECTRIC CONTROLS

MANUAL DE SEGURANÇA DO TRANSMISSOR DE SEGURANÇA ONE SERIES

ONE AND DONE

UE

UNITED ELECTRIC CONTROLS

LEADERS IN SAFETY, ALARM & SHUTDOWN

OneST-SM-PTBR-01

1 INTRODUÇÃO

Este manual de segurança fornece as informações necessárias para projetar, instalar, verificar e manter uma Função Instrumentada de Segurança (Safety Instrumented Function, SIF) utilizando o *transmissor de segurança One Series*. Este manual fornece os requisitos para cumprir com os padrões de segurança funcional IEC 61508 ou IEC 61511.

1.1 Termos e abreviações

Segurança	Sem riscos inaceitáveis de danos
Segurança funcional	A habilidade de um sistema executar as ações necessárias para conseguir ou manter um estado de segurança definido para os equipamentos/maquinário/planta/aparatos sob controle do sistema
Segurança básica	O equipamento deve ser projetado e fabricado de tal modo que ele proteja pessoas contra riscos de danos por choque elétrico ou outros perigos e contra fogo e explosão resultantes. A proteção deve ser eficaz sob todas as condições de operação nominal e sob condições de falha única.
Avaliação de Segurança	A investigação para chegar a uma conclusão - baseada em evidências - sobre a segurança obtida pelos sistemas de segurança
Estados seguros contra falhas	Estado onde as saída são desenergizadas. Definido como:

Saída 4-20 mA	$\leq$3,6mA
Status de comutador	DESLIGADO
Saída do relé de segurança	DESLIGADO
IAW	DESLIGADO

Seguro contra falhas	Falhas que fazem com que a saída vá para o estado seguro contra falhas definido sem uma demanda do processo.
Perigoso contra falhas	Falha que não responda a uma demanda do processo (isto é, ser incapaz de ir para o estado seguro contra falhas).
Falha perigosa não detectada	Falha perigosa que não é diagnosticada por testes ou diagnósticos de instrumento.
Falha perigosa detectada	Falha perigosa que é detectada por testes ou diagnósticos de instrumento.

Anúncio de falha não detectada Falha que não causa uma ativação falsa ou impede a função de segurança, mas causa a perda de um diagnóstico automático e não é detectada por outro diagnóstico.

Anúncio de falha detectada Falha que não causa uma ativação falsa ou impede a função de segurança, mas causa a perda de um diagnóstico automático ou falsa indicação de diagnóstico.

Falha sem efeito Falha de um componente que faz parte da função de segurança, mas não possui efeito na função de segurança.

Modo de baixa demanda Modo onde a frequência de demandas para operações feitas em um sistema de segurança não é maior do que duas vezes a frequência de teste.

1.2 Acrônimos

DTT	Desenergizar para ativar
DU	Perigo não detectado
FMEDA	Análise dos modos de falha, efeitos e diagnóstico
HFT	Tolerância de falha de hardware
IAW	I Am Working (Estou trabalhando) - diagnósticos embutidos que monitoram o hardware do dispositivo e funções de software para alertar operador caso tenha ocorrido um problema que possa afetar a função de segurança do dispositivo.
MOC	Gerenciamento de mudança - são procedimentos específicos frequentemente feitos ao executar quaisquer atividades de trabalho com conformidade com as autoridades reguladoras governamentais.
PFD_{avg}	Probabilidade média de falha sob demanda
PLC	Controlador de lógica programável
SFF	Fração de falha segura - a fração da taxa de falha geral de um dispositivo que resulta ou em uma falha segura ou uma falha não segura diagnosticada.
SIF	Função instrumentada de segurança - um conjunto de equipamentos destinados a reduzir o risco devido a perigos específicos (um loop de segurança).
SIL	Nível de integridade de segurança - nível discreto (um de quatro possíveis) para especificar os requisitos de integridade de segurança das funções de segurança a serem alocadas aos sistemas E/E/PE de segurança onde o nível 4 de integridade de segurança possui o mais alto nível de integridade de segurança e onde o nível 1 de integridade de segurança possui o mais baixo.

SIS	Sistema instrumentado de segurança - implementação de uma ou mais funções instrumentadas de segurança. Um SIS é composto de qualquer combinação de sensor(es), resolvedor(es) lógico(s) e elemento(s) final(is).
SRO	Saída de relé de segurança - um comutador relé de estado sólido de alta capacidade

1.3 Suporte de produto

Suporte de produto pode ser obtido da:

United Electric Controls

180 Dexter Ave,

P.O. Box 9143

Watertown, MA 02471-9143

TechSupport@ueonline.com

Telefone: 617 923-6977

FAX: 617 926-2568

Senha perdida: acesse www.ueonline.com/uuc O número Kanban da placa de identificação é necessário.

1.4 Literatura relacionada

Documentos de hardware:

- Instruções de instalação e manutenção do *transmissor de segturança One Series*(IM_ONE_SAFETY-01)
- SR113028.D3.6 Relatório FMEDA UE 12-10-073 R001 V1 R2 TRANSMISSOR DE SEGURANÇA One Series
- Boletim de produto do transmissor de segurança One Series ST-B-01 da United Electric Controls
- Diretrizes/Referências:
  - Seleção prática de destino SIL – análise de riscos de acordo com ciclo de vida de segurança IEC 61511, ISBN 978-1-934977-03-3, exida
  - Avaliação de segurança e confiabilidade do sistema de controle, 3ª edição, ISBN, 978-1-934394-80-9, ISA
  - Verificação de sistemas instrumentados de segurança, cálculos probabilísticos práticos, ISBN 1-55617-909-9, ISA

1.5 Padrões de referência

Segurança funcional

- IEC 61508: 2010 Segurança funcional de sistemas de segurança elétricos/eletrônicos/programáveis
- ANSI/ISA 84.00.01-2004 (IEC 61511 Mod.) Segurança funcional - sistemas instrumentados de segurança para o setor da indústria de processo

2 DESCRIÇÃO DE DISPOSITIVO

O transmissor de Segurança One Series detecta a temperatura ou pressão de um sistema e fornece saídas de controle que são usadas para monitorar ou desligar esse sistema antes da ocorrência de uma condição não segura. Um 4-20mA externamente ativado fornece uma indicação analógica do processo para uso por um PLC de segurança. A saída do relé de estado sólido fornece um controle direto ou desligamento de um elemento final baseado em modos e limites de operação programados. A saída do status de comutação é uma saída discreta que imita a função da saída do relé de estado sólido. A saída IAW é uma saída discreta baseada em autodiagnósticos que fornece ao usuário uma indicação da integridade do dispositivo. Quaisquer falhas de diagnósticos que ocasionem uma falha de IAW forçarão todas as saídas para o estado seguro contra falhas. Todas as saídas do sensor de segurança One Series operam em modo DTT (Desenergizar para ativar).

Informações detalhadas sobre a instalação, programação e operação do transmissor de segurança One Series junto aos diagramas de contexto de sistema estão disponíveis no documento IM_ONE_SAFETY-01.

3 PROJETAR UM SIF USANDO O TRANSMISSOR DE SEGURANÇA ONE SERIES

3.1 Função de segurança

As saídas 4-20mA, I Am Working, do relé de segurança e do status de comutação foram avaliadas quanto ao uso de sistemas instrumentados de segurança.

O nível SIL obtido da função projetada deve ser verificado pelo designer.

3.2 Limites ambientais

O designer de um SIF deve verificar se o produto é classificado para uso dentro das restrições ambientais esperadas. Consulte o *boletim ST-B-01 One Series* da United Electric Controls para ver os limites ambientais.

3.3 Limites de aplicação

Os materiais da construção do *transmissor de segurança One Series* são especificados no boletim United Electric Controls *One Series ST-B-01*. É especialmente importante que o designer verifique a compatibilidade de materiais, considerando as condições do local. Se o *transmissor de segurança One Series* for usado fora dos limites de aplicação ou com materiais incompletos, os dados de confiabilidade fornecidos se tornam inválidos.

3.4 Verificação de projeto

Um relatório detalhado sobre a análise dos modos de falha, efeitos e diagnóstico (FMEDA) está disponível da *United Electric Controls*. Este relatório detalha todas as taxas de falha e modos de falha, além da vida útil esperada.

O nível de integridade de segurança (SIL) obtido de um design inteiro de função instrumentada de segurança (SIF) deve ser verificado pelo designer por meio de um cálculo de PFD_{AVG} considerando arquitetura, intervalo de teste, efetividade de teste, quaisquer diagnósticos automáticos, tempo médio de conserto e as taxas específicas de falha de todos os produtos inclusos na SIF. Cada subsistema deve ser verificado para assegurar a observância dos requisitos mínimos de tolerância de falha de hardware (HFT) A ferramenta exida exSILentia® é recomendada para esta finalidade, pois contém modelos precisos do *transmissor de segurança One Series* e suas taxas de falha.

Ao usar o *transmissor de segurança One Series* em uma configuração redundante, um fator de causa comum de pelo menos 5% deve ser incluído em cálculos de integridade de segurança.

Os dados de taxas de falhas listados no relatório FMEDA somente são válidos para a vida útil do *transmissor de segurança One Series*. As taxas de falha aumentarão algum tempo após este período. Cálculos de confiabilidade baseados nos dados listados no relatório FMEDA para tempos de missão além da vida útil podem fornecer resultados excessivamente otimistas, isto é, o nível de integridade de segurança calculado não será obtido.

3.5 Capacidade SIL

3.5.1 Integridade sistemática

O produto atendeu os requisitos do processo de design do fabricante do nível de integridade de segurança (SIL) 3. Eles são destinados a obter integridade suficiente contra erros sistêmicos de design pelo fabricante. Uma função instrumentada de segurança (SIF) projetada com este produto não deve ser usada em um nível SIL mais alto do que declarado sem justificativa de "uso prévio" pelo usuário final ou redundância de tecnologia diversa no design.

3.5.2 Integridade aleatória

O *transmissor de segurança One Series* é um dispositivo tipo B. Portanto, baseado no SFF entre 90% e 99%, quando o *transmissor de segurança One Series* for usado como o único componente em uma subunidade de um elemento sensor, um design pode atender SIL 2 a HFT = 0.

Quando a unidade do elemento sensor consistir de múltiplos componentes, o SIL deve ser verificado para a unidade inteira, usando taxas de falha de todos os componentes. Esta análise deve levar em conta quaisquer tolerâncias de falha de hardware e constrições arquitetônicas.

3.5.3 Parâmetros de segurança

A precisão de segurança do dispositivo é 3% do alcance de operação.

Para obter informações detalhadas sobre taxas de segurança, consulte a análise dos modos de falha, efeitos e diagnóstico para o *transmissor de segurança One Series*.

3.6 Conexão do *transmissor de segurança One Series* ao solucionador lógico SIS.

O *transmissor de segurança One Series* é conectado ao solucionado lógico de classificação de segurança através de uma NAMUR NE 43 4-20mA analógica e até duas saídas discretas de status de diagnóstico. O solucionador lógico está ativamente desempenhando a função de segurança monitorando e interpretando as saídas do transmissor de segurança One Series, projetado para diagnosticar condições de processo potencialmente perigosas e falhas no *transmissor de segurança One Series* por meio do diagnóstico Estou Trabalhando (IAW).

O transmissor de segurança One Series também pode ser configurado para fornecer a função de segurança diretamente sem conexões a um solucionador lógico com classificação de segurança.Consulte os diagramas de contexto de sistema no documento

IM_ONE_SAFETY-01 para obter detalhes sobre o uso de diversas saídas lógicas no transmissor de segurança One Series.

3.7 Requisitos Gerais

O tempo de resposta do sistema deve ser menor do que o tempo de segurança de processo. O *transmissor de segurança One Series* e as saídas do status de comutação e do relé de segurança se moverão até seu estado de segurança em menos de 100 milissegundos sob configurações de filtro de atraso específicas. A saída de 4-20mA estabilizará a 90% de uma reposta em 250 ms sob configurações específicas de filtro de atraso. Para obter as configurações disponíveis e uma descrição do documento da operação do filtro de atraso, consulte a instalação de produto e o manual de manutenção IM_ONE_SAFETY-01.

O intervalo de diagnóstico do transmissor de segurança One Series é de menos de 10 segundos.

Todos os componentes SIS incluindo o *transmissor de segurança One Series* devem estar operacionais antes do início de processo. Na hora de ligar, pode haver um breve atraso antes de as saídas se tornarem estáveis. O usuário deve considerar isto na aplicação e não depender do *transmissor de segurança One Series* para o controle do sistema instrumentado de segurança até que as saídas tenham se estabilizado. O intervalo entre a hora de ligar e a hora em que as saídas se estabilizarem deve ser menor do que 10 segundos.

O usuário deverá verificar se o *transmissor de segurança One Series* é adequado para uso em aplicações de segurança confirmando se a placa de identificação do *transmissor de segurança One Series* está adequadamente marcada.

O pessoal efetuando a manutenção e testagem do *transmissor de segurança One Series* deve ser capacitado para tal.

Os resultados dos testes devem ser registrados e revisados periodicamente.

A vida útil do *transmissor de segurança One Series* é discutida em análise dos modos de falha, efeitos e diagnóstico do *transmissor de segurança One Series*.

4 INSTALAÇÃO E COMISSIONAMENTO

4.1 Instalação

O *transmissor de segurança One Series* deve ser instalado de acordo com as práticas padrão descritas no manual de instalação.

O transmissor de segurança One Series não deve ser modificado.

O ambiente deve ser verificado para certificar-se de que as condições ambientais não excedem as classificações.

O *transmissor de segurança One Series* deve ser acessível a inspeções físicas.

Instruções detalhadas de programação e operação estão disponíveis no manual de instruções de instalação e manutenção do*transmissor de segurança One Series* (IM_ONE_SAFETY-01). É de responsabilidade do designer SIF validar todas as configurações do dispositivo, através de testes ou acessando novamente o menu de programação e lendo todas as configurações novamente. A lista de verificação no Apêndice A fornece um lugar onde registrar todas as configurações de dispositivo, à medida que elas forem lidas novamente. Enquanto no menu de programação, todas as saídas são forçadas para o estado seguro contra falhas:

Saída 4-20mA	≤3,6mA
Status de comutador	Desligado
Saída do relé de segurança	Desligado
IAW	Desligado

A detecção de porta plugada e o monitor de falhas do relé de segurança vêm desligados de fábrica. Se estes recursos forem desejados, eles devem ser habilitados usando o menu de programação. Utilize o manual de instruções de instalação e manutenção do transmissor de segurança One Series (IM_ONE_SAFETY-01) como referência para obter detalhes.

4.2 Local físico e posicionamento

O *transmissor de segurança One Series* deve estar acessível com espaço suficiente para conexões e deverá permitir testagem manual.

O encanamento conectando ao *transmissor de segurança One Series* deve ser mantido curto e tão reto quanto possível de modo a minimizar restrições e possíveis entupimentos. Tubos longos ou amassados também podem aumentar o tempo de resposta.

O *transmissor de segurança One Series* deverá ser montado em um ambiente de baixa vibração. Se vibrações excessivas forem esperadas, adote precauções especiais de modo a assegurar a integridade dos conectores ou reduza a vibração utilizando as montagens de amortecimento adequadas.

4.3 Conexões

As conexões ao *transmissor de segurança One Series* deverão ser feitas de acordo com as instruções de instalação e manutenção (IM_ONE_SAFETY-01).

Os métodos recomendados para conexões de processo ao *transmissor de segurança One Series* estão disponíveis no manual de instalação e manutenção IM_ONE_SAFETY-01. O comprimento do tubo entre o *transmissor de segurança One Series* e a conexão de processo deverá ser mantido tão curto quanto possível e sem curvas.

5 OPERAÇÃO E MANUTENÇÃO

5.1 Testagem não automática

O objetivo da testagem é detectar falhas dentro do *transmissor de segurança One Series daUnited Electric Controls* que não sejam detectadas por quaisquer outros diagnósticos automáticos do instrumento. De importância essencial são as falhas não detectadas que previnem a função instrumentada de segurança de desempenhar sua função pretendida.

A frequência da testagem, ou o intervalo entre testagens, deve ser determinada em cálculos de confiabilidade para as funções instrumentadas de segurança para a qual um *transmissor de segurança One Seriesa United Electric* for aplicado. Os testes devem ser feitos pelo menos tão frequentemente quanto especificado no cálculo de modo a manter a integridade de sistema necessária da função instrumentada de segurança.

O seguinte teste é recomendado. Os resultados do teste devem ser registrados e quaisquer falhas detectadas que comprometam a segurança funcional devem ser informadas à *United Electric Controls*. O teste de prova sugerido consiste em simular um distúrbio de processo e injetar uma falha do *transmissor de segurança One Series* e observar a reação do SIF a estes distúrbios.

Tabela 1: Teste recomendado

Passo	Ação
1.	Desative o PLC de segurança ou adote outra ação adequada para prevenir um acionamento falso.
2.	Verifique se a saída correta está sob as condições normais. A saídas do relé de segurança, do status SRO e do IAW estarão no estado fechado. A saída 4-20 mA fornecerá um sinal proporcional à variável de processo.
3.	Mude a variável de processo ou a programação do instrumento de modo que a saída do relé de segurança mude para o estado ativado (aberto). Verifique se as saídas relé de segurança e do status SRO se abrem e se a do IAW permanece fechada. A saída 4-20 mA fornecerá um sinal proporcional à variável de processo.
4.	Mude a variável de processo de modo que a saída IAW vá para o estado de falha (aberto). (Sugere-se uma ultrapassagem extrema do limite de 150% do alcance do sensor.) Verifique se a saída IAW se abre e se a saída 4-20mA fornece ≤3,6 mA.
5.	Restaure os valores normais de entrada ou programação. Verifique se as saídas retornaram para seus estados não ativos (fechados). Verifique se a saída 4-20mA é proporcional à variável de processo.
6.	Restaure o loop de volta à operação completa.
7.	Reative o PLC de segurança ou, de algum modo, restaure a operação normal.

Este teste detectará >99% de possíveis falhas DU no *transmissor de segurança One Series*.

A pessoa efetuando a testagem do *transmissor de segurança One Series* deve ser treinada em operações SIS, incluindo procedimentos de desativação de segurança, manutenção e procedimentos de gerenciamento de mudanças da empresa. Uma chave hexagonal de 2 mm é necessária para remover a tampa. O fluxograma de software do manual de instalação e manutenção do transmissor de segurança One Series IM_ONE_SAFETY-01 é necessário para alterar a programação.

5.2 Conserto e substituição

Procedimentos de conserto e substituição para o *transmissor de segurança One Series* são obtidos ao entrar em contato com o suporte técnico da United Electric Controls no telefone 617-923-6977 ou e-mail techsupport@ueonline.com.

Uma lista completa de códigos de falha para o transmissor de segurança One Series está disponível no manual de instalação e manutenção IM_ONE_SAFETY-01.

5.3 Configuração de hardware e software

O número de modelo do dispositivo está disponível campo PART# da placa de identificação do dispositivo. As revisões de hardware e software são anotadas na etiqueta localizada na parte traseira do módulo do visor.

5.4 Vida útil

A vida útil do *transmissor de segurança One Series* é de 50 anos.

5.5 Notificação do FABRICANTE

Quaisquer falhas detectadas que comprometam a segurança funcional devem ser informadas à *United Electric Controls*. Entre em contato com o suporte técnico da *United Electric Controls* pelo número 617-923-6977 ou techsupport@ueonline.com.

Appendix A Exemplo de lista de verificação de inicialização

Este apêndice fornece uma Sample Start-up Checklist para um *transmissor de segurança One Series*.Uma lista de verificação de inicialização fornecerá diretrizes durante a implementação do *transmissor de segurança One Series*.

1 LISTA DE VERIFICAÇÃO DE INICIALIZAÇÃO

A seguinte lista de verificação pode ser usada como um guia para implementar o *transmissor de segurança One Series* em um SIF de segurança crítica em conformidade com o IEC61508.

Nº	Atividade	Resultado	Verificado	
			Por	Data
	Design			
	Nível desejado de integridade de segurança e PFD_{avg} determinados			
	Modo correto selecionado (aberto em elevação, aberto em queda ou modo janela)			
	Corrija o ponto de ajuste e a faixa inativa escolhidos			
	Decisão de design documentada			
	Compatibilidade de líquido e adequabilidade verificada			
	Requisitos de solucionador lógico SIS para testes automáticos definidos e documentados			
	Roteamento de conexões de líquido determinado			
	Design formalmente revisado e adequabilidade formalmente avaliada			
	Implementação			
	Local físico apropriado			
	Conexões de líquido adequadas e de acordo com os códigos aplicáveis			
	Teste automático de solucionador lógico SIS implementado			
	Instruções de manutenção para testagem publicadas			
	Plano de verificação e testagem publicado			
	Implementação formalmente revisada e adequabilidade formalmente avaliada			

Nº	Atividade	Resultado	Verificado	
			Por	Data
	Verificação e testagem			
	Conexões elétricas verificadas e testadas			
	Conexões de líquido verificadas e testadas			
	Teste automático de solucionador lógico SIS verificado			
	Função de loop de segurança verificada			
	Temporização do loop de segurança medida			
	Função de desativação testada			
	Resultados de verificação e testagem formalmente revisados e adequabilidade formalmente avaliada			
	Manutenção			
	Bloqueio de tubulação/bloqueio parcial testado			
	Função de loop de segurança testada			

Registre todas as configurações de dispositivo na planilha fornecida abaixo:

Para obter uma explicação detalhada de cada recurso, consulte o manual e instalação e manutenção do transmissor de segurança One Series IM_ONE_SAFETY-01 d.

ID do dispositivo: _____
Alcance: _____
Nº de Kanban: _____
Senha: _____

Unidades de medida: ☐ psi ☐ bar/mbar ☐ KPa/MPa ☐ Kg/cm^2 ☐ "wc (Padrão psi)
☐ °F ☐ °C (Padrão °F)

Modo de comutação: ☐ Aberto em elevação ☐ Aberto em queda
Ponto de ajuste:_____
Faixa inativa:_____

☐ Janela
Ponto de ajuste (Superior):_____
Faixa inativa (Superior):_____
Ponto de ajuste (Inferior):_____
Faixa inativa (Inferior):_____

Offset (compensação): _____ (Nominalmente 0,0)
Span (intervalo): _____ (Nominalmente o limite superior do transmissor)

Modo trava: ☐ Ligado ☐ Desligado

Porta plugada: ☐ Desligado ☐ 1 min. ☐ 1HR ☐ 24HR (Padrão desligado)

Monitor de falha SSR: ☐ Ligado ☐ Desligado (Padrão desligado)

Atraso: ☐ Desligado ☐ ¼ s ☐ ½ s ☐ 1 s ☐ 2 s (Padrão desligado)

Configuração 4mA: _____ (Nominalmente o limite inferior do dispositivo)
Configuração 20mA: _____ (Nominalmente o limite superior do dispositivo)