

Setting the Standard for Automation™



Boas práticas para desenvolvimento de aplicações SCADA

Ana Cristina Rodrigues
acrodrigues29@hotmail.com
São Paulo, outubro de 2017

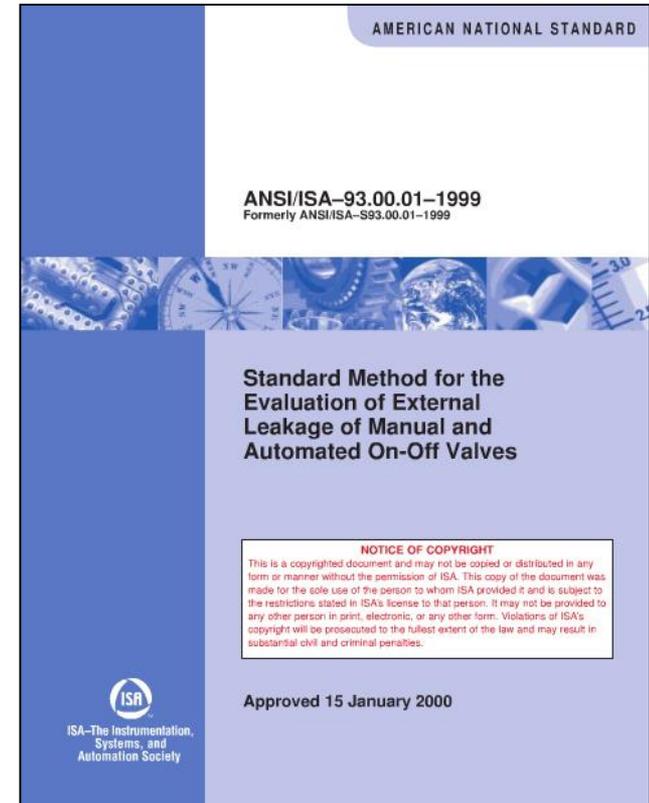
Standards
Certification
Education & Training
Publishing
Conferences & Exhibits

- Onde encontrar boas práticas?
- ISA 101 – Criação de IHMs
- ISA 99 – Segurança de Sistemas de Controle
- ISA 18.2 – Gestão de Alarmes
- ISA 106 – Automação de Procedimentos
- Próximos passos: ISA 112 – Sistemas SCADA
- Conclusão

O que é uma Norma?



- Um conjunto de características, quantidades ou procedimentos que descrevem um produto, um serviço, uma interface ou um material.
- As normas oferecem inúmeros benefícios em automação e produção.
- Um conjunto de normas normalmente inclui: Normas, Recomendações Práticas e/ou Relatórios Técnicos.



Como as Normas são desenvolvidas?

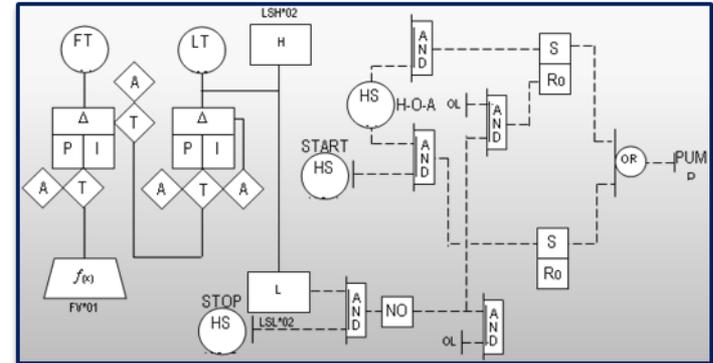


- Desenvolvidas por **Comitês de Normas**
 - Verifique os termos de referência do comitê
 - Verifique a que órgão está vinculado
 - Alguns comitês de normas são melhores que outros
- O que caracteriza um “bom” comitê de normas
 - Abertura
 - Domínio no assunto
 - Equilíbrio
 - Consenso
 - Direito de Apelação



- **Normas da ISA**

- Abertas e consensuais
- Mais de 4.000 profissionais participando ao redor do mundo



- **Benefícios da Padronização**

- Agilizar processos
- Aumentar a segurança, a confiabilidade
- Aumentar a eficiência, a produtividade

Credenciamento de Normas



- Normas credenciadas por institutos de normas nacionais ou internacionais é um bom sinal.
- Âmbito nacional:
 - EUA: American National Standards Institute (ANSI)
 - Brasil: Associação Brasileira de Normas Técnicas (ABNT)
- Âmbito internacional:
 - ISO: International Organization for Standardization
 - IEC: International Electrotechnical Commission



A ISA é credenciada no ANSI e associada à IEC

- São +160 documentos entre Normas (**ISA**), Recomendações Práticas (**ISA-RP**) e Relatórios Técnicos (**ISA-TR**) publicados pela ISA, que abrange **todos os aspectos** da automação e controle industrial:
 - ISA 5: Simbologia para Instrumentação
 - **ISA 18.2: Gerenciamento de Alarmes**
 - ISA 20: Formulários de Especificação de Instrumentação
 - ISA 75: Válvulas de Controle
 - ISA 84: Segurança Funcional
 - ISA 88: Sistemas de Controle de Bateladas
 - ISA 95: Integração de Sistemas de Controle-Corporativos
 - **ISA 99: Segurança de Sistemas de Controle e Automação Industrial**
 - ISA 100: Sistemas de Redes sem Fio para Automação
 - **ISA 101: Interfaces Homem-Máquina**
 - ISA 105: Comissionamento, Verificações de Loop, Testes FAT e SAT
 - **ISA 106: Automação de Procedimentos em Operações de Processo Contínuo**, etc.
- A lista completa de normas da ISA pode ser encontrada em:
 - <https://www.isa.org/standards-and-publications/isa-standards>

Normas da ISA credenciadas no ANSI e IEC

- **ANSI:** algumas normas desenvolvidas pela ISA foram registradas pela ANSI e são denominadas de **ANSI/ISA**, como por exemplo:

ISA 18.2	ANSI/ISA 18.2 - Management of Alarm Systems for the Process Industries
ISA 99	ANSI/ISA 62443 - Control Systems Security
ISA 101	ANSI/ISA-101.01 - Human Machine Interfaces for Process Automation Systems

- **IEC:** algumas normas desenvolvidas pela ISA serviram de base de normas internacionais **IEC ou ISA/IEC**, utilizadas mundialmente, como por exemplo:

ISA 18.2	IEC 62682 - Management of Alarm Systems for the Process Industries
ISA 99	ISA/IEC-62443: Control Systems Security

Como acessar uma Norma da ISA



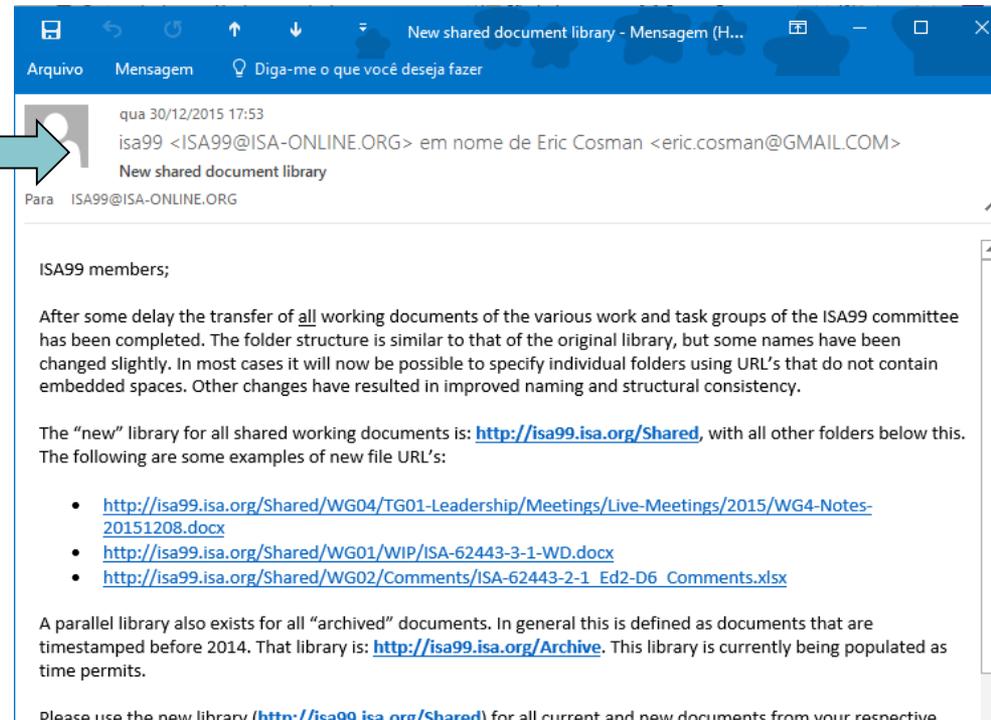
- Membros da ISA podem acessar online a maioria das normas técnicas (necessário login)
 - www.isa.org → Standards & Publications → View ISA Standards

The screenshot shows the ISA website interface. At the top left is the ISA logo with the tagline "Setting the Standard for Automation™". To the right are social media icons for Twitter, Facebook, LinkedIn, YouTube, and Instagram, followed by a "Join ISA" button, a "My ISA Account" button, and a "Renew Membership" button. Below these is a search bar and the phone number "Phone: (919) 549-8411". A navigation menu contains buttons for MEMBERSHIP, TRAINING & CERTIFICATIONS, STANDARDS & PUBLICATIONS, CONFERENCES & EVENTS, NEWS & PRESS RELEASES, RESOURCES, TECHNICAL TOPICS, PROFESSIONAL DEVELOPMENT, and STORE. The main content area is titled "ISA Standards" and lists several standards, including ISA-5.2-1976 (R1992), ISA-5.3-1983, ISA-5.4-1991, ISA-5.5-1985, ISA-7.0.01-1996, ISA12.10-1988, and ISA-18.1-1979 (R2004). On the right side of the standards list, there are buttons for "Share This Page", a printer icon, and font size controls (A A A). Below these are several buttons: "Find ISA Standards: Numerical Order", "View ISA Standards: A Member Benefit", "Ask a Question about ISA Standards", "Propose a New Standard", "Administratively Withdrawn Standards", and "Standards Committees: Numerical Order".

Como participar dos Comitês de Normas da ISA



- Qualquer voluntário pode participar de um comitê de normas técnicas
 - www.isa.org → Standards & Publications → Standards Committees: Numerical Order
- Os comitês organizam encontros de 1-2 vezes por ano ou conforme a necessidade.
- Muitos encontros são através de teleconferências e web meetings.
- Composto por:
 - Information Member
 - Voting Member (membros que participam ativamente são pontuados e recebem direito a voto)



ISA 101 – INTERFACE HOMEM- MÁQUINA

Documento da norma:

- ANSI/ISA-101.01-2015, Human Machine Interfaces for Process Automation Systems

Propósito da norma:

- Guia para **projetar, construir, operar e manter** uma IHM para se ter **sistemas de controle de processo mais seguros, efetivos e eficientes**, sob quaisquer condições de operação;
- Melhorar a habilidade de **detectar e responder** adequadamente a situações anormais.

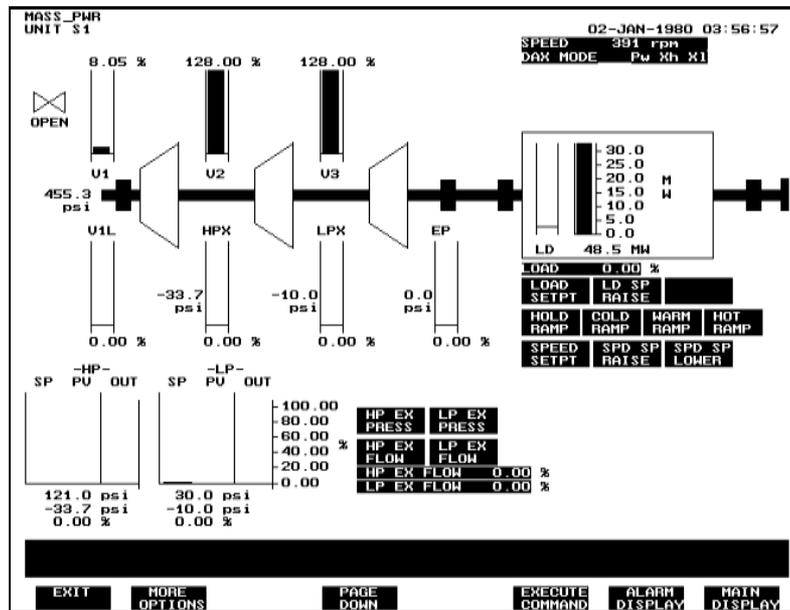
- Gerenciamento de Sistemas IHM
- Ergonomia e fatores humanos
- Estrutura da IHM e estilos de tela
- Interação com o usuário
- Performance
- Treinamento de usuário

- 7 -		ANSI/ISA-101.01-2015
Contents		
Introduction		9
Purpose		9
Organization		9
1 Scope		10
1.1 General Applicability		10
1.2 Exclusions		10
1.3 Intended Audience		10
2 Normative References		10
2.1 References		10
3 Definition of Terms and Acronyms		12
3.1 Definitions		12
3.2 Acronyms		18
4 HMI System Management		19
4.1 Introduction		19
4.2 System Standards		20
4.3 The Design Process		23
4.4 The Implementation Stage of the HMI Lifecycle		27
4.5 The Operate Stage of the HMI Lifecycle		30
4.6 Continuous Work Processes		32
5 Human Factors Engineering & Ergonomics		35
5.1 General Principles of HMI Design		35
5.2 User Sensory Limits		36
5.3 User Cognitive Limits		39
6 Display Styles and Overall HMI Structure		40
6.1 Introduction		40
6.2 Display Styles		40
6.3 Display Hierarchy		42
7 User Interaction		47
7.1 Introduction		47
7.2 Software Methods for User Interaction		47
7.3 Hardware Interfaces		57
8 Performance		59
8.1 Introduction		59
8.2 HMI Categories		59
8.3 HMI Duty Factors		60
9 Training		61
9.1 User Training		61

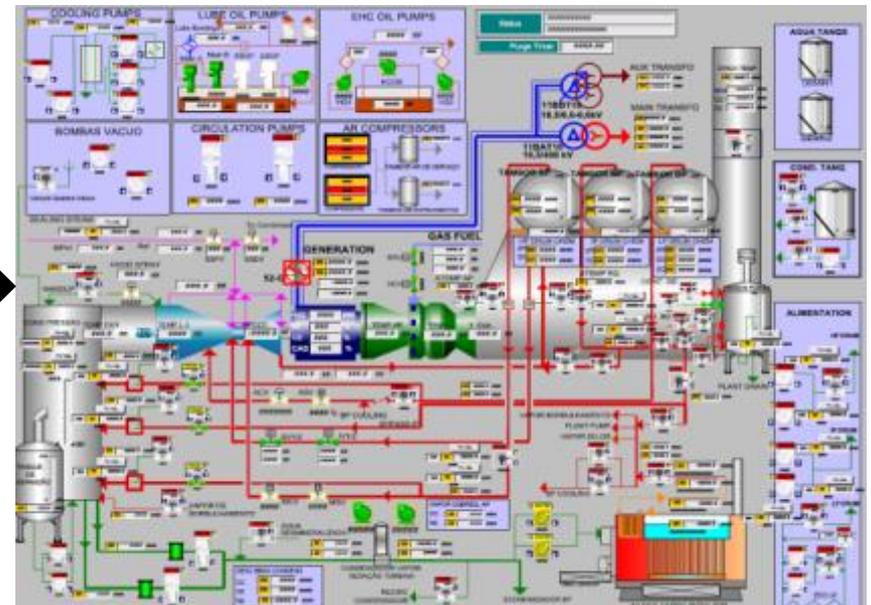
- **Etapas de projeto:** sala de operação (mobilierio, número de monitores, temperatura e luz ambiente), sistema IHM (seleção da plataforma, regras de segurança), requisitos funcional/usuário/tarefa e projeto gráfico. Atentar para a documentação do projeto.
- **Bibliotecas de objetos:** optar pelo uso de modelos prontos de telas, *pop-ups*, *faceplates*, objetos estáticos e dinâmicos: foram pensados para operações específicas com performance otimizada. Melhor ainda se tiver recurso de replicação global de mudanças
- **Fatores humanos/ergonomia:** densidade de informações, uso de cores, animação de objetos, alarmes sonoros etc.
- **Uso de script ou lógica embarcada:** reaproveitamento de códigos
- **Padronização de cores:** tons de cinza para objetos em geral, uso de cores como amarelo, vermelho, azul, verde somente para enfatizar situações.
- **Tamanhos das formas:** proporcionais às quantidades e/ou hierarquia do objeto.

- **Acessibilidade:** indicador muda de formato para destacar mudança no processo, com grande contraste de cores.
- **Hierarquia de telas:** nível 1 para visão geral e resumo de alarmes, nível 2 para detalhamento, nível 3 para tarefas não rotineiras (configuração de parâmetros, rotinas complexas), nível 4 para diagnósticos
- **Navegação de telas:** métodos por hierarquia, relacional ou sequencial
- **Indicadores numéricos:** adotar um padrão para a entrada de dados e apresentação de números
- **Animação de objetos:** poderoso atrativo para os olhos como recurso de entretenimento, deve ser usado com critério ou até mesmo eliminado de telas de operação
- **Posição:** utilizar objetos planos, evitando o uso de telas tridimensionais por trazer uma sobrecarga cognitiva, com excesso de cores e visibilidade prejudicada
- Etc.

1990

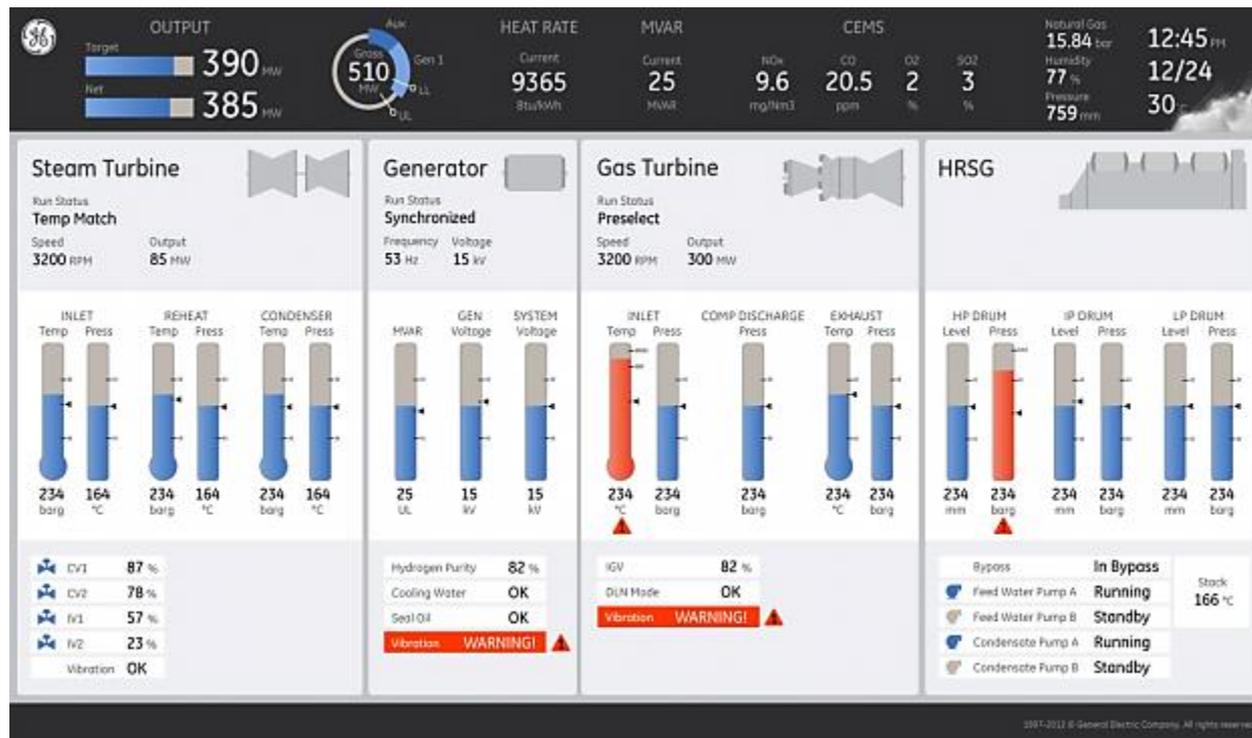


Hoje



Simplificação = Segurança

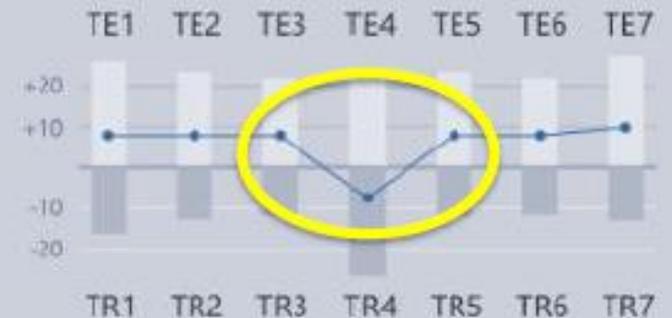
Hoje e futuro



ISA 101 – Apresentação de dados

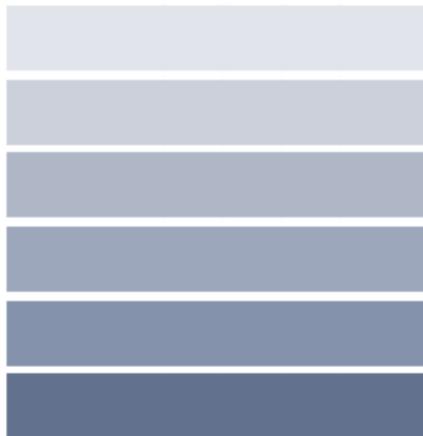
TE1	25.1 °C	TR1	16.0 °C	GD1	9.1 °C
TE2	22.3 °C	TR2	13.2 °C	GD2	9.1 °C
TE3	21.6 °C	TR3	12.6 °C	GD3	9.0 °C
TE4	22.4 °C	TR4	30.9 °C	GD4	-8.5 °C
TE5	22.3 °C	TR5	13,4 °C	GD5	8.9 °C
TE6	21.5 °C	TR6	12.5 °C	GD6	9.0 °C
TE7	26.9 °C	TR7	16.8 °C	GD7	10.1 °C

Temperature gradient



Representação analógica permite uma compreensão mais rápida.

- Dados mais importantes devem se destacar dos demais.



Cores para Uso Normal

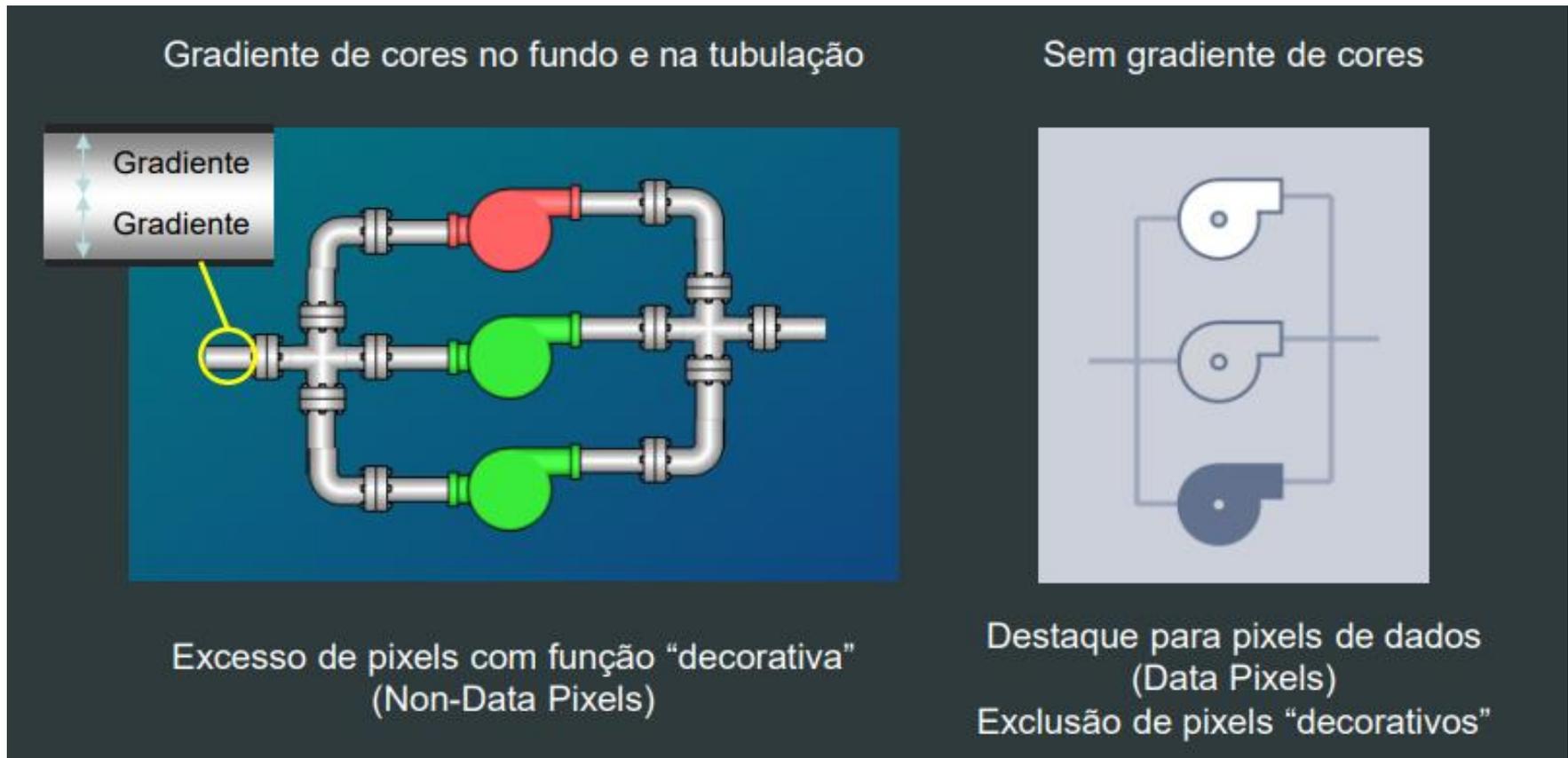
Representação de objetos em geral e status.



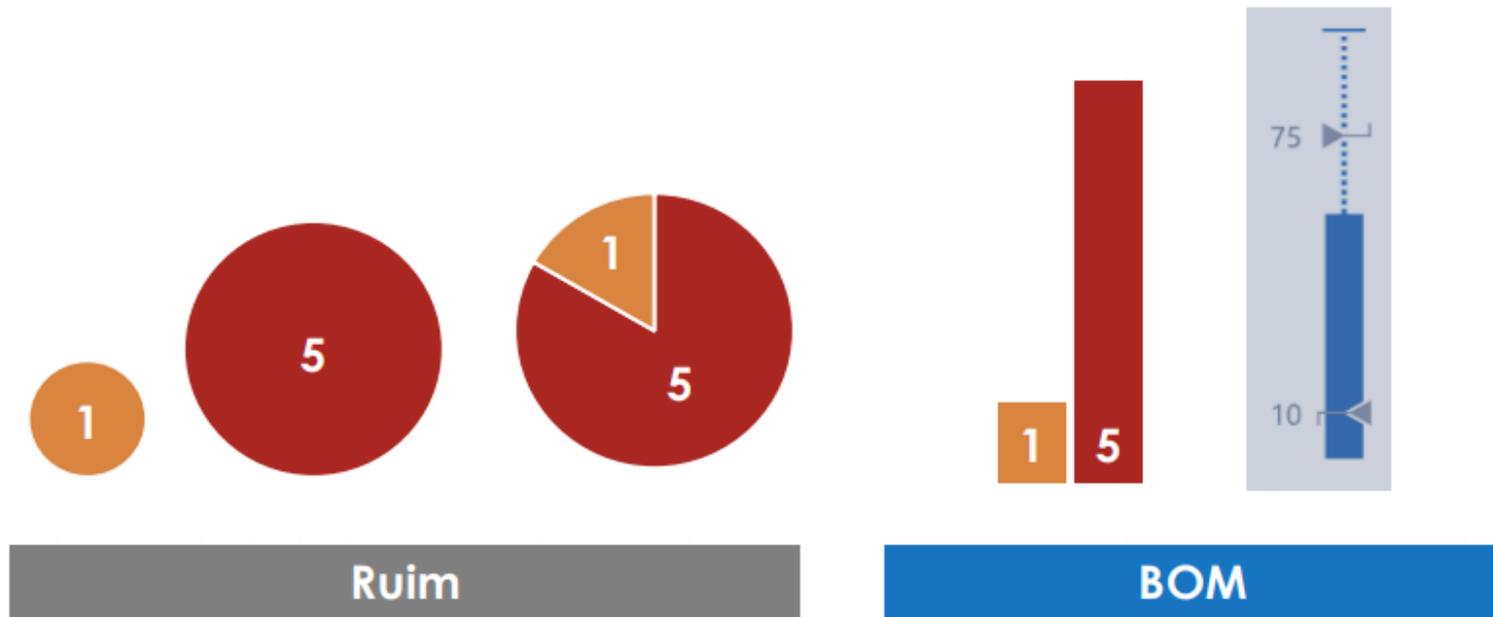
Cores para Ênfase

Indicação de Alarmes, Falhas, Bloqueios, Inibições, SetPoints, Intertravamentos

Cuidado com Gradientes de Cores!



Representar “Quantidade” por comprimento de linha



Representar “Agrupamento” por contornos e preenchimentos ao redor dos objetos de um mesmo grupo



ISA 99 – SEGURANÇA CIBERNÉTICA

ISA 99 Security for Industrial Automation and Control Systems



Propósito da norma:

- Guia de **segurança cibernética** para sistemas industriais de automação e controle (IACS).
- **IACS** incluem sistemas usados em plantas de manufatura e processamento, utilidades, sistemas de distribuição, etc que utilizam dispositivos automáticos ou controlados remotamente.
- **Segurança** definida como meio para prevenir o acesso ilegal e não desejado à operação de um processo, a interferência intencional ou não intencional à operação, ou o acesso à informações confidenciais em IACS.

ISA 99 ou ISA/IEC 62443?



- Como essas normas se relacionam?
 - ISA/IEC 62443 é uma série de normas
 - Desenvolvida por 3 grupos:
 - ISA99 → ANSI/ISA 62443
 - IEC TC65 WG10 → Comitê Técnico 65, Grupo de Trabalho 10 (TC65 WG10): Security for industrial process measurement and control – network and system security
 - ISO/IEC JTC1/SC27 → ISO/IEC 2700x



ISA/IEC 62443 – Estrutura



* IACS: Industrial Automation and Control Systems

General

ISA-62443-1-1

Terminologia,
conceitos e modelos

ISA-TR62443-1-2

Glossário de termos
e abreviações

ISA-62443-1-3

Métricas de
conformidade de
segurança do sistema

ISA-TR62443-1-4

Ciclo de vida e caso
de uso de segurança
IACS*

Policies & procedures

ISA-62443-2-1

Requisitos para um
sistema de gestão de
segurança para IACS*

ISA-TR62443-2-2

Guia de
implementação de
sistema de gestão de
segurança para IACS*

ISA-TR62443-2-3

Gerenciamento de
patches no ambiente
IACS*

ISA-62443-2-4

Requisitos de
instalação e
manutenção para
fornecedores IACS*

System

ISA-TR62443-3-1

Topologias de
segurança para IACS*

ISA-62443-3-2

Níveis de segurança
para zonas e
conduites

ISA-62443-3-3

Requisitos de
sistemas e níveis de
segurança

Component

ISA-62443-4-1

Requisitos para
desenvolvimento de
produtos

ISA-62443-4-2

Requisitos para
segurança técnica de
componentes IACS*

- Realizar uma análise de riscos de todo o sistema
- **Confidencialidade (TI) \neq Disponibilidade (TA/TO)**
- Controle de acesso em sistemas SCADA
 - Roubo de identidades digitais: crackers de senhas, sniffers, malwares, permanência de dados
 - Engenharia social: por e-mail, por help desk
 - Antivírus e políticas de atualização de patches

- Políticas de controle de acesso:
 - Segurança do SCADA integrada à segurança do sistema operacional
 - Política de senhas e perguntas randômicas
 - Duplo fator de autenticação: *smartcards*, *tokens*, biometria etc
 - Desconexão automática de usuários inativos
 - Auditoria de eventos através de trilhas de auditoria
 - Verificação do usuário em operações críticas (assinatura eletrônica)
 - Bloqueio de acesso do usuário ao sistema operacional
 - Etc

ISA 18.2 – GESTÃO DE ALARMES

ISA 18.2 ou IEC 61512

Documentos da norma:

- ANSI/ISA-18.2-2016, Management of Alarm Systems for the Process Industries
- ISA-TR18.2.2-2016, Alarm Identification and Rationalization
- ISA-TR18.2.3-2015, Basic Alarm Design
- ISA-TR18.2.4-2012, Enhanced and Advanced Alarm Methods
- ISA-TR18.2.5-2012, Alarm System Monitoring, Assessment, and Auditing
- ISA-TR18.2.6-2012 - Alarm Systems for Batch and Discrete Processes
- ISA-TR18.2.7-2017, Alarm Management When Utilizing Packaged Systems

Propósito da norma:

- **Desenvolvimento, projeto, instalação e gerenciamento** de sistemas de alarme para indústrias de processo. Gerenciamento de alarmes inclui múltiplos processos de trabalho dentro do **ciclo de gerenciamento de alarmes**.

- Modelos de sistemas de alarmes
- Filosofia de alarme
- Requisitos de um sistema de alarmes
- Identificação
- Racionalização
- Projeto detalhado de alarme básico
- Interface de IHM com sistemas de gestão de alarmes
- Métodos avançados de alarme
- Implementação, Operação, Manutenção, Monitoramento
- Controle de versão e auditoria

CONTENTS	
Introduction	11
1 Scope	13
1.1 General applicability	13
1.2 Exclusions and inclusions	14
2 Normative references	15
3 Terms, definitions, and acronyms	15
3.1 Terms and definitions	15
3.2 Abbreviations	25
4 Conformance to this standard	25
4.1 Conformance guidance	25
4.2 Existing systems	25
4.3 Use of required functionalities	26
4.4 Responsibility	26
5 Alarm system models	26
5.1 Alarm systems	26
5.2 Alarm management lifecycle	26
5.3 Alarm states	31
5.4 Alarm response timeline	35
5.5 Feedback model of operator – process interaction	37
6 Alarm philosophy	38
6.1 Purpose	38
6.2 Alarm philosophy contents	38
6.3 Alarm philosophy development and maintenance	44
7 Alarm system requirements specification	45
7.1 Purpose	45
7.2 Recommendations	45
7.3 Development	45
7.4 Systems evaluation	46
7.5 Packaged systems	46
7.6 Customization	46
7.7 Alarm system requirements testing	46
8 Identification	46
8.1 Purpose	46
8.2 Alarm identification methods	46
8.3 Identification training	47
8.4 Identification documentation	47
9 Rationalization	47
9.1 Purpose	47
9.2 Rationalization documentation	47
9.3 Alarm justification	48
9.4 Alarm setpoint determination	49
9.5 Prioritization	49

ISA 18.2 – O Ciclo de Vida do Gerenciamento de Alarmes



Métricas da Norma ISA 18.2

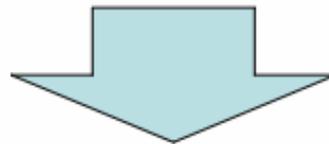


Alarm performance metrics based upon at least 30 days of data		
Metric	Target value	
Annunciated alarms per time	Target value: Very likely to be acceptable	Target value: Maximum manageable
Annunciated alarms per day per operating position	~150 alarms per day	~300 alarms per day
Annunciated alarms per hour per operating position	~6 (average)	~12 (average)
Annunciated alarms per 10 minutes per operating position	~1 (average)	~2 (average)
Metric	Target value	
Percentage of hours containing more than 30 alarms	~<1%	
Percentage of 10-minute periods containing more than 10 alarms	~1<5%	
Maximum number of alarms in a 10 minute period	≤10	
Percentage of time the alarm system is in a flood condition	~<1%	
Percentage contribution of the top 10 most frequent alarms to the overall alarm load	~<1% to 5% maximum, with action plans to address deficiencies.	
Quantity of chattering and fleeting alarms	Zero, with action plans to correct any that occur.	
Stale alarms	Less than 5 present on any day, with action plans to address	

Taxas de Alarmes e Classificação



Quantidade de Alarmes/10 minutos	Classificação
Até 1	Muito provavelmente aceitável
Até 2	Gerenciável
De 2 a 5	Possivelmente sobre-demanda
De 5 a 10	Provável sobre-demanda
Acima de 10	Muito provavelmente inaceitável



O gráfico das taxas de Alarmes (**Alarm Rates**) na forma horária ou diária ajuda na visualização do desempenho.

- Análise dos alarmes mais frequentes
- Resolução de alarmes problemáticos
- Distribuição por prioridade
- Alarmes de diagnóstico com prioridade mínima
 - Devem ser eliminados em situação de enxurrada de alarmes
- Racionalização de alarmes
 - Diversas técnicas nos relatórios TR2, TR3 e TR4

ISA 106 – AUTOMAÇÃO DE PROCEDIMENTOS

ISA 106 – Automação de Procedimentos



Documentos da norma:

- ISA-TR106.00.01-2013, Procedure Automation for Continuous Process Operations - Models and Terminology
- ISA-TR106.00.02-2017, Procedure Automation for Continuous Process Operations - Work Processes

Propósito da norma:

- Oferecer um conjunto de **boas práticas com relação à automação de procedimentos** e estratégias para incorporar procedimentos automáticos nos sistemas de automação.

ISA 106 – Automação de Procedimentos



Garantir que sejam efetuadas as ações corretas no momento certo

- Modelos e terminologia
- Modularização de etapas de procedimentos
- Resolução de situações anormais
- Modelagem física, de procedimentos e de aplicações
- Implantação de lógicas para partidas, desligamentos, transições operacionais e outras situações críticas
- Recomendação de interface entre diferentes sistemas para cada procedimento
- Treinamento e certificação

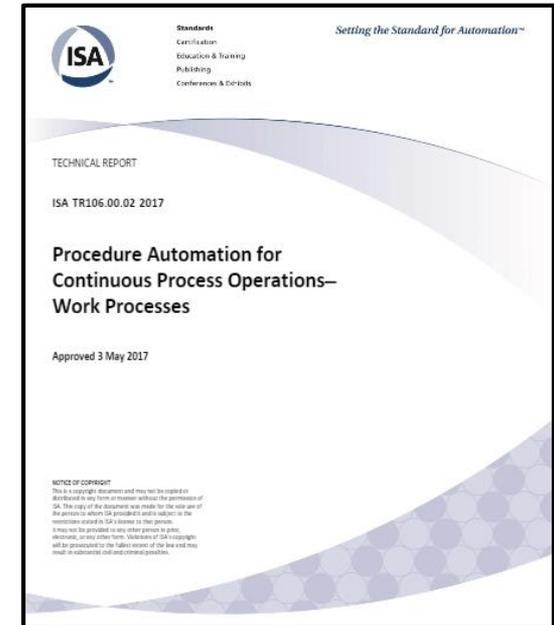
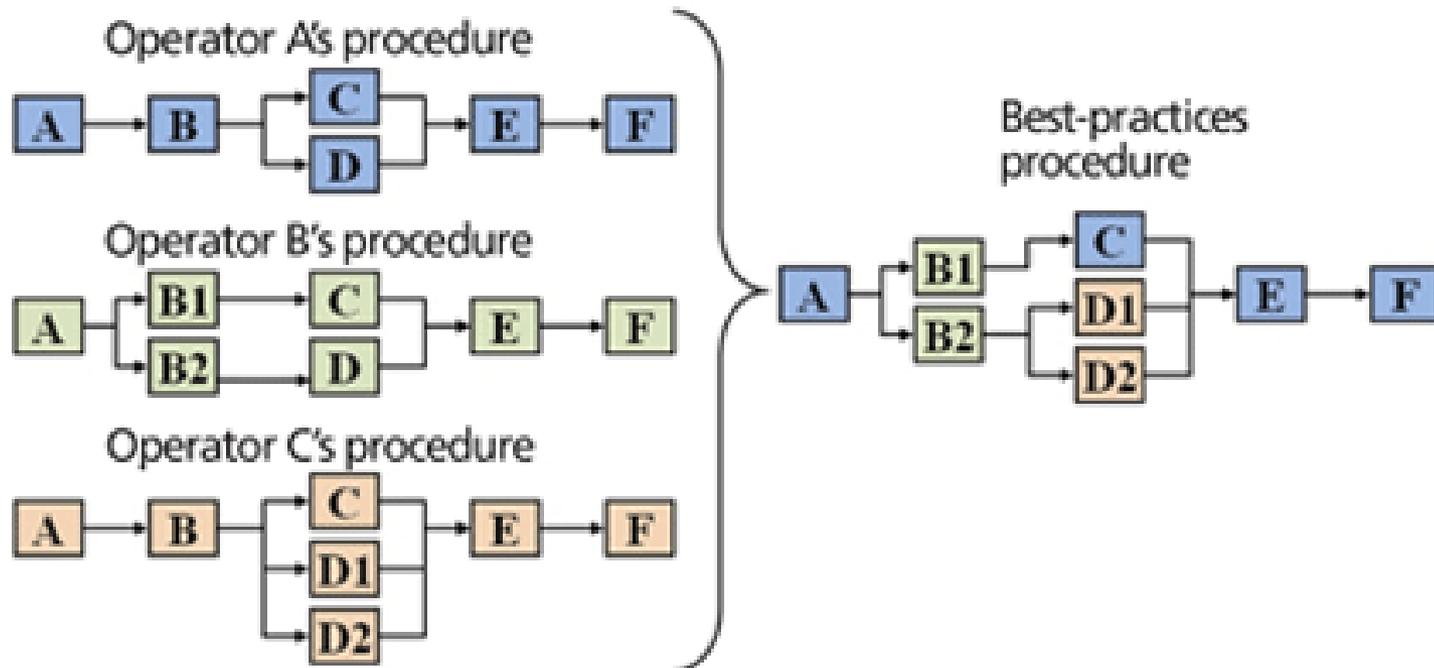


TABLE OF CONTENTS	
1	Scope 11
2	References 11
2.1	Cited References 11
2.2	Relevant References 12
2.3	References of Interest 12
3	Definitions of Terms and Abbreviations 14
3.1	Definitions of Terms 14
3.2	Abbreviations 18
4	Historical Perspective 19
5	Value Proposition 20
6	Models 23
6.1	Procedure Automation Models 23
6.2	Physical Model 24
6.3	Procedure Requirements Model 26
6.4	Procedure Implementation Model 29
6.5	Model Summary 32
6.6	Collapsibility 33
6.7	Mapping Procedure Requirements to Implementation Modules 37
6.8	Implementation Modules 39
6.9	State-Based Control 46
6.10	Mapping Implementation Modules to BPCS Components 52
6.11	Alignment with Other Standards 54
6.12	Model Level Names Used in Various Industries 58

Desafios e Oportunidades

Procedimentos não documentados podem ser executados de maneira diferente por diferentes pessoas. A automação dos procedimentos visa identificar as melhores práticas e padronizá-las para trazer consistência à operação

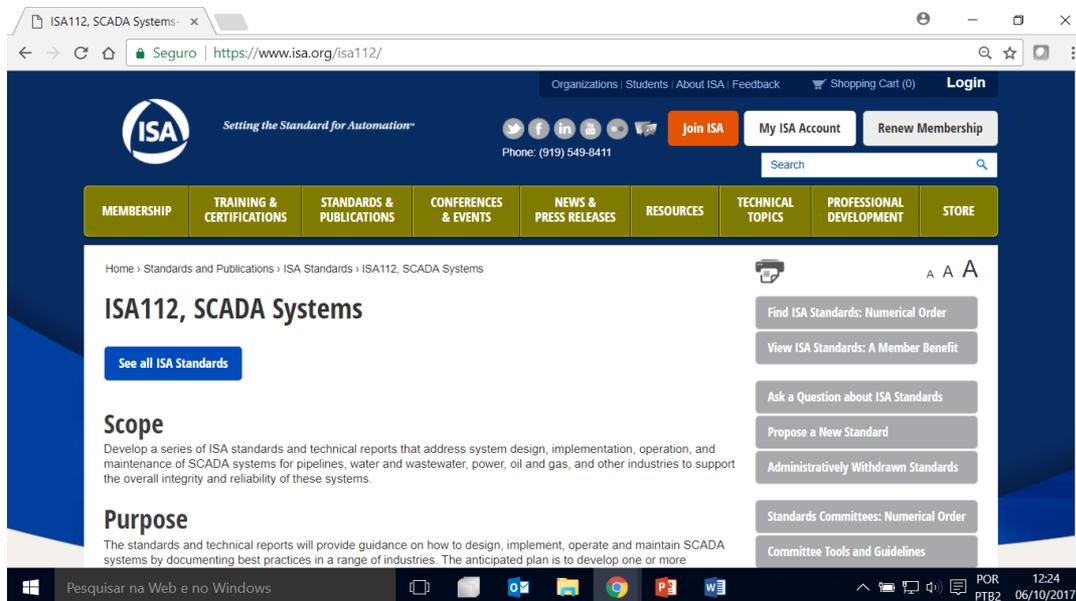


PRÓXIMOS PASSOS

ISA 112 – SISTEMAS SCADA

Propósito da norma:

- Guia de como projetar, implementar, operar e manter um sistema SCADA através de documentação das melhores práticas encontradas nas indústrias.
- O plano é desenvolver uma ou mais normas complementadas por relatórios técnicos específicos para alguns tipos de indústrias.



The screenshot shows the ISA website interface for the ISA 112, SCADA Systems page. The page features a navigation menu with categories like MEMBERSHIP, TRAINING & CERTIFICATIONS, STANDARDS & PUBLICATIONS, CONFERENCES & EVENTS, NEWS & PRESS RELEASES, RESOURCES, TECHNICAL TOPICS, PROFESSIONAL DEVELOPMENT, and STORE. The main content area displays the title 'ISA112, SCADA Systems' and a 'See all ISA Standards' button. Below this, there is a 'Scope' section and a 'Purpose' section. On the right side, there is a list of actions: 'Find ISA Standards: Numerical Order', 'View ISA Standards: A Member Benefit', 'Ask a Question about ISA Standards', 'Propose a New Standard', 'Administratively Withdrawn Standards', 'Standards Committees: Numerical Order', and 'Committee Tools and Guidelines'. The page is viewed in a browser window with the URL 'https://www.isa.org/isa112/' and a search bar.

Faça parte do Comitê de desenvolvimento da Norma ISA 112!

- ✓ O uso das normas ISA101, ISA99, ISA18.2 e ISA 106 em projeto IHM/SCADA aproveita as boas práticas e a experiência de usuários e desenvolvedores de todo o mundo.
- ✓ Exija que seu desenvolvedor/integrador conheça e utilize as normas da ISA em seu próximo projeto!

Ana Cristina Rodrigues

Professora e Consultora de Automação
acrodrigues29@hotmail.com
São Paulo, outubro de 2017