Departamento de Engenharia Química e de Petróleo – UFF

Conceitos Básicos

Definições

Segurança ou prevenção de perdas: é a prevenção de acidentes pelo uso de tecnologias adequadas para identificar os perigos de uma planta química e eliminá-los antes de que ocorram acidentes. Prevenção de lesões às pessoas, danos à perda do ambiente, dos equipamentos, estoque ou produção.
Acidente: A ocorrência de uma seqüência de eventos que produzem a lesão não intencional, morte e danos materiais
Perigo: é qualquer coisa com o potencial para produzir um acidente
Risco: è a probabilidade de um perigo de converter em acidente.
.

Conceitos Básicos

No linguagem cotidiano, os termos "perigo" e "risco" se confundem. Não obstante, esses termos tem significados diferentes ….

Algumas abreviações

- AFAP – do ingles "tão baixo quanto razoavelmente praticável"
- Empregador - Empregador que tem o controle de gestão da instalação
- FTA: Fault Tree Analysis – Análise da Árvore de Falhas, é um modelo gráfico, onde a combinação das falhas é descrita (i.e., a ocorrência em série ou paralelo dos eventos irá resultar na ocorrência do evento indesejado pré-definido). As faltas podem ser do tipo falha de equipamento, erro humano, erro de software, ou qualquer outro evento
- HAZID – Identificação de perigo
- HAZOP - Análise de Perigos e Operacionalidade
- LOC - Perda de contenção ou vazamento de produto, derivado e gás
- LOPA: Layers of protection analysis – Análise de camadas de proteção
- PFD - Diagrama de Fluxo de Processo
- P & ID - Diagrama de Processo e Instrumentação
- PSV - válvula de segurança de pressão
- SMS - sistema de gestão de segurança

Conceitos Básicos

Perigo

É a característica de uma substância ou processos, que causa efeitos adversos nos organismos ou no ambiente, por suas propriedades inerentes e de acordo com o grau de exposição.

É uma fonte de dano.

Perigos identificados na atividade industrial ou laboratorial, que dão lugar a acidentes.

- Contato, inalação ou ingestão de substancias.
- Incêndios e explosões.
- Explosão de equipam. submetidos a pressão.
- Ambiente térmico inadequado.
- Iluminação inadequada.
- Eletricidade, radiações, ruído e vibrações.
- Quedas a nível ou entre níveis.
- Trabalho em espaço confinado.
- Manipulação inadequada de cargas.
- Transtornos do equipam.

Conceitos Básicos

Perigos tecnológicos (Harzard) associado a âmbito dos produtos químicos na industria e laboratório

- Incêndios.
- Explosões.
- Intoxicações e queimaduras por fugas de produtos tóxicos e corrosivos.

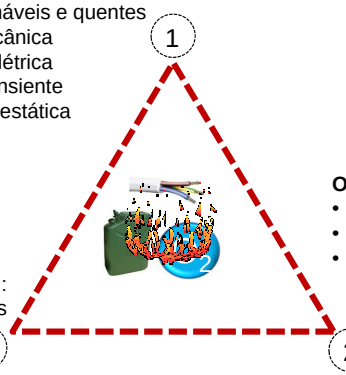
Perigo

- Uma característica inerente física ou química que tem o potencial de causar danos às pessoas, ao meio ambiente ou propriedade[1]
- Perigos são intrínsecos a um material, ou as suas condições de utilização
- Exemplos:
- Sulfeto de hidrogênio (H_2S) – tóxico por inalação
- Gasolina – inflamável
- Máquinas em movimento - energia cinética, pontos opressores perigosos

[1] *AICHE Center for Chemical Process Safety*

Conceitos Básicos : Triângulo de Segurança

Fonte de Ignição:
- superfície quente
- gases inflamáveis e quentes
- Faíscas mecânica
- Instalação elétrica
- Corrente transiente
- Eletricidade estática

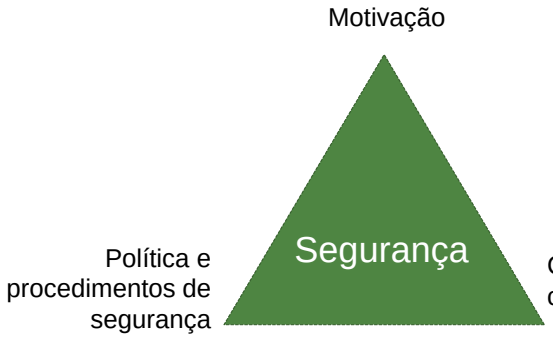


Oxidantes:
- ar (21% oxigênio)
- oxigênio puro
- oxigênio liberado de compostos (por ex. manganato de potássio))

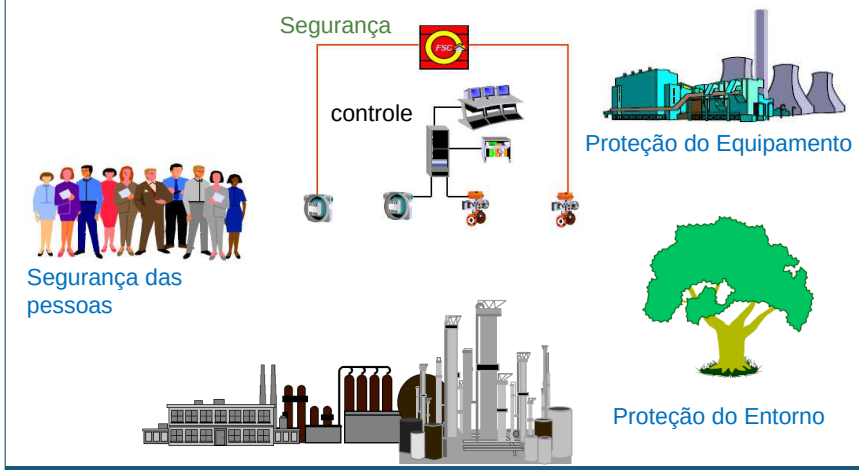
Combustível: substâncias inflamáveis

Conceitos Básicos : Triângulo de Segurança

Agentes químicos ⇨ perigosos em plantas químicas: inflamáveis, explosivos, reativos e tóxicos.



Objetivos dos Sistemas de Controle e de Segurança

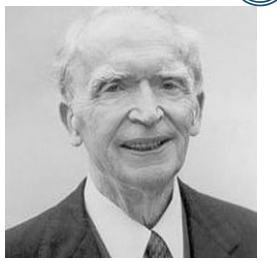


Principais Riscos de Processo

Porque devemos investir em segurança??

Sensores + Lógica + Elementos Finais

“A Lei de Murphy” !



Dr. Joseph Murphy

“Se algo puder dar errado, dará!”

Qualquer processo tem suas funções específicas, mas...

...devido à “Lei de Murphy”, temos que incluir funções adicionais, para reduzir o risco de que ocorra alguma falha no sistema que possa *Danificar ou Destruir bens, ou ainda, ferir / matar pessoas.*

Causas de Acidentes

- Os acidentes nas industrias não são uma fatalidade.
- Os acidentes não se dão porque o destino assim quer, mas porque alguém ou alguma coisa o provoca.
- Isto significa que um acidente é sempre a consequência de uma ou mais causas.
- A velha teoria da fatalidade há muito que foi substituída pela teoria da causalidade.
- A ideia-chave a fixar é a de que:

Todo acidente tem pelo menos uma causa.

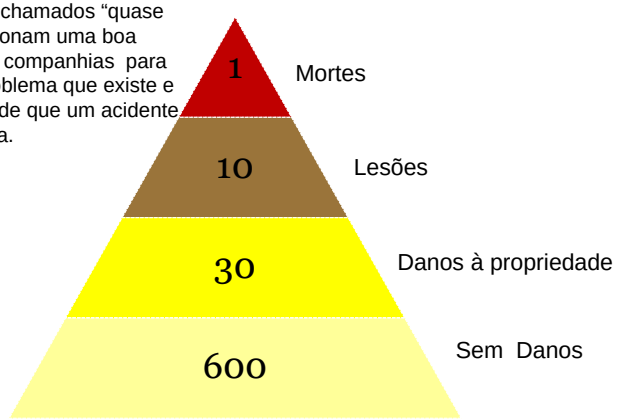
Causas de Acidentes

As causas dos acidentes podem classificar-se em:

- **Causas materiais:** dos acidentes, as mais comuns são:
  - Materiais defeituosos
  - Equipamentos em más condições
  - Ambiente físico ou químico não adequado
- **Causa humana** :
  - Maus hábitos de trabalho
  - Falta de experiência
  - Falta ou deficiente formação profissional
  - Cansaço
  - Stress

Causas de Acidentes

Os acidentes sem “nenhuma lesão ou dano” causados são freqüentemente chamados “quase falha” e proporcionam uma boa oportunidade às companhias para determinar o problema que existe e corrigir-lo antes de que um acidente mais sério ocorra.



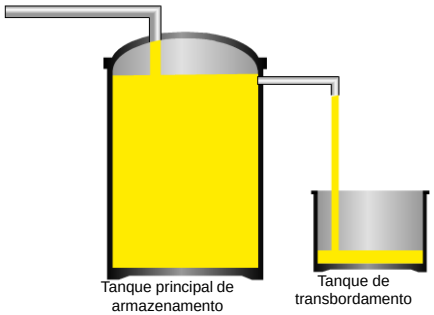
Pirâmide de acidentes

Trabalho sem segurança ainda é muito comum..

Trabalho sem segurança ainda é muito comum..

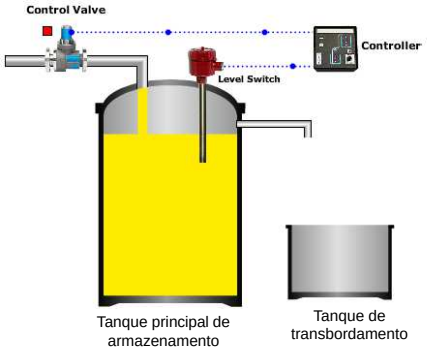
Segurança é definida como a liberdade de um **risco inaceitável** de danos às pessoas ou no ambiente. Segurança é o resultado de pessoas, processos e equipamentos, todos trabalhando juntos de uma forma destinada a garantir, que o risco às danos as pessoas ou ao ambiente, seja muito menor, ou inexistente. A parte da segurança que foi projetado para operar corretamente em resposta a suas entradas, é conhecida como **Segurança Funcional**.

Exemplo: Considere um tanque de armazenamento com uma linha de transbordamento conectado a um outro tanque de armazenamento, como mostrado na animação à sua direita. A linha de transbordamento é parte da segurança geral do tanque, mas não pode ser considerado como um "dispositivo de segurança funcional“.



Segurança Funcional
No exemplo anterior, se um interruptor de nível é montado no topo do tanque de armazenamento, o qual fecha automaticamente a válvula de entrada, para impedir o transbordamento, então, este dispositivo pode ser parte do sistema de **“Segurança funcional"**

Exemplo: Considere o exemplo anterior, agora com um sistema de controle de nível colocado no topo do tanque de armazenamento. Este dispositivo pode ser parte do sistema de “Segurança funcional"



Natureza de acidente

Os acidentes nas plantas químicas seguem padrão típico, cujo estudo é de particular importância para antecipar os tipos de acidentes que podem ocorrer são:

Tipo de acidente	Probabilidade de ocorrência	Potencial de fatalidade	Potencial de danos econômicos
Fogo	Alto	Baixo	Intermediário
Explosão	intermediário	Intermediário	Alto
Tóxicos liberados	Baixo	Alto	Baixo

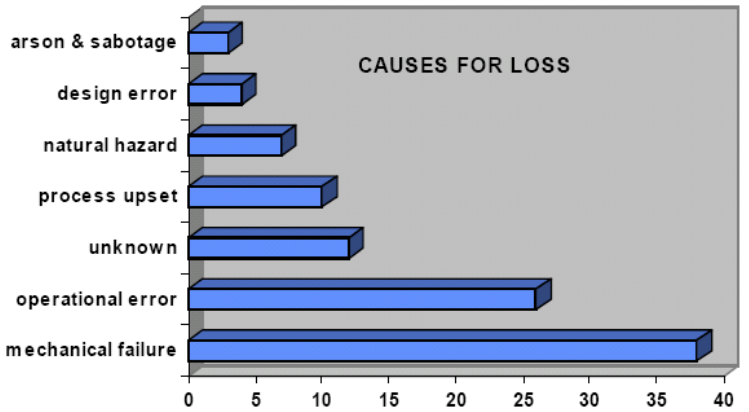
Como mostrado na tabela, fogo são os mais comuns, seguido por explosão e liberação de substancias tóxicas.

Natureza de accidents (contin.)

- Em relação a fatalidades, a liberação de tóxicos tem mais alto potencial para causar fatalidades.
- Nos acidentes que envolvem explosões, as perdas econômicas são consideravelmente altas.
- O tipo de explosão que causa maiores danos é a explosão com nuvens de vapor não confinadas, onde uma grande nuvem volátil e inflamável é liberada e dispersa em toda a superfície da planta seguida pela ignição e explosão da nuvem.
- A liberação de tóxicos tipicamente causa pouco danos ao equipamento da planta, não obstante, as lesões do pessoal, perdas de empregados e responsabilidades legais são significativas.

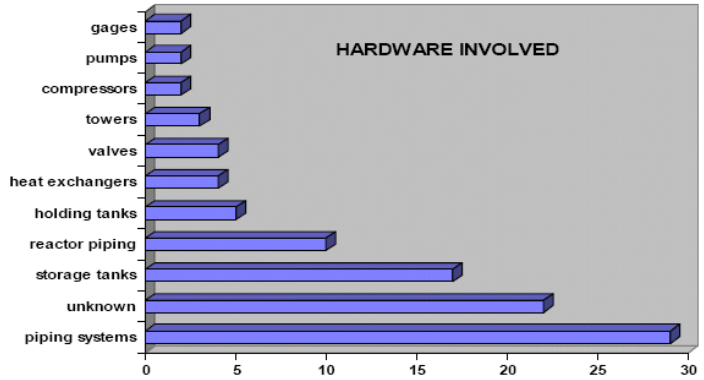
Natureza de acidente (contin.)

Natureza de acidente (contin.)



Causas de perdas em acidentes quimicos (A thirty of One of the hungred of the largest property damage losse in the hydrocarbon-chemical industries, 1997, M&M protection Consultants, Chicago).

Natureza de acidente (contin.)



Equipamentos associados em acidentes com perdas .(A thirty of One of the hungred of the largest property damage losse in the hydrocarbon-chemical industries, 1997, M&M protection Consultants, Chicago).

Análise de acidente

As maiorias dos acidentes seguem um processo de três etapas sucessivas:

- **Iniciação**: o evento que inicia o acidente.
- **Propagação**: o evento ou eventos que mantêm ou expandem o acidente
- **Finalização**: o evento ou eventos que detém o acidente ou diminuem seu tamanho.

Análise de acidente (contin.)

Flixborough, England, 1974	ruptura da tubulação bypass, inadequadamente apoiado, 155 º C, 7,9 atm 30 ton de nuvem de vapor de ciclohexano Explosão e inventários de fogo (10 dias), 28 mortes, 36 + 53 feridos, muitos danos
Bhopal, India, 1984 not operating scrubber & flare system	sistemas precários de alivio e dos depuradores e queimadores 25 toneladas de nuvem de vapor de MIC 2000 mortos, 20.000 feridos, nenhum dano
Explosão da **Plataforma P-36**, 2001	2 explosões nas colunas de sustentação mataram 11 integrantes da equipe de emergência que estava a bordo, além de fazer com que a estrutura tombasse 16 grau. Em poucas horas, a plataforma já estava inteiramente submersa.

MIC: isocianato de metila

Anatomia de um Acidente com algumas entradas típicas em cada coluna

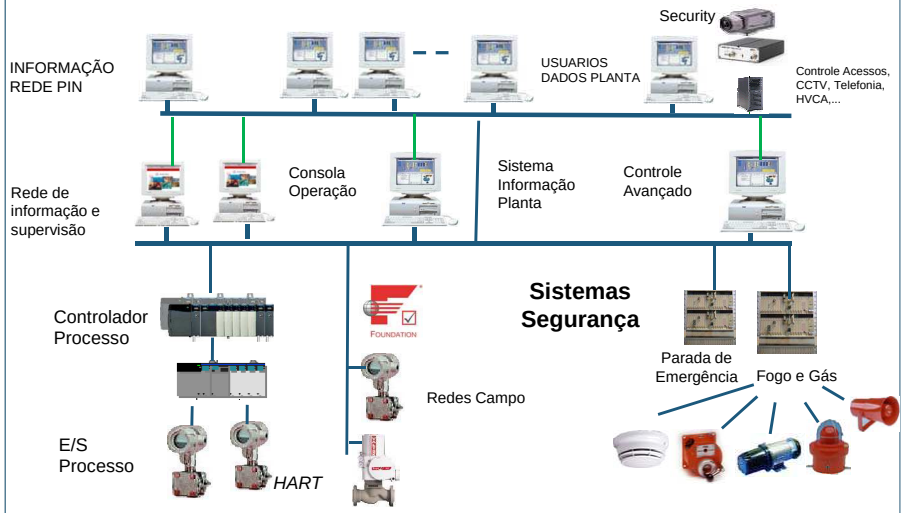
HAZARD → CAUSE → DEVIATION → ACCIDENT EVENT → CONSEQUENCE

Material and energy during operation	Initiating event or Root Cause	From design operating conditions*	Physical condition yielding harm	Severity of consequences
• Toxicity • Flammability • Reactivity • Elevated Pressure • Elevated temperature	• Action by person • Mechanical failure • Design flaw • Process change (e.g., fouling) • External change (force, fire, etc.)	• Flow variations (to zero or maximum) • Material compositions (or improper materials) • High/low pressure or temperatures • Improper mixture of materials	• Combustion/ explosion • Fire • Hazardous material released • Equipment damaged	• Injury • Death • Undesired releases to environment • Disease • Equipment damage • Recycle/scrap of materials in production • Loss of production

* We should also challenge the design conditions by asking, "Have they been properly selected for safety and profit?"

Níveis de Automatização

Segurança e Controle na Industria de Processo

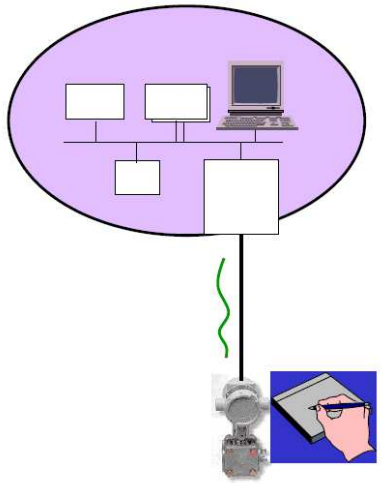


Evolução da Comunicação com Dispositivos de Campo

Analógico 4-20mA

Informação de Operação é 4-20 mA (1 variável de processo, sem estado do dispositivo)

Informação de Manutenção se recolhe a mão

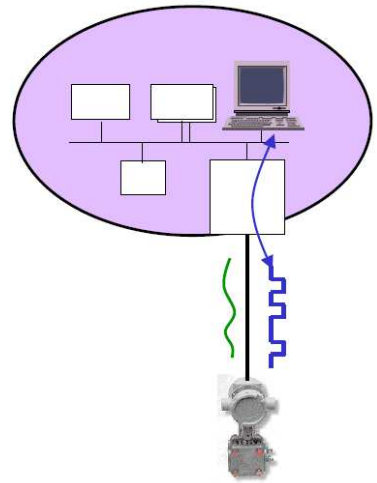


Evolução da Comunicação com Dispositivos de Campo

Protocolo HART

Informação de Operação é 4-20 mA (1 variável de processo, sem estado do dispositivo)

Informação de Manutenção é digital, se acesa via estações do sistema de controle ou estações específicas.



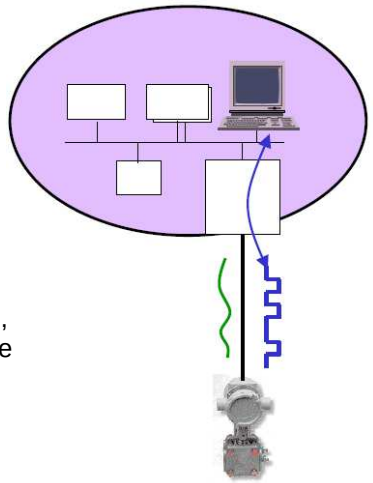
Evolução da Comunicação com Dispositivos de Campo

Integração Digital

Informação de Operação é digital (variáveis de processo + estado dos dispositivos)

- O estado do dispositivo se monitora/alarma
- Permite um controle de ativos

Informação de Manutenção é digital, se acesa via estações do sistema de controle com uma base de dados integrada.

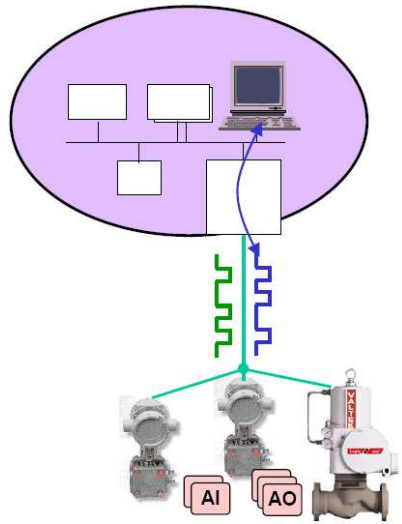


Evolução da Comunicação com Dispositivos de Campo

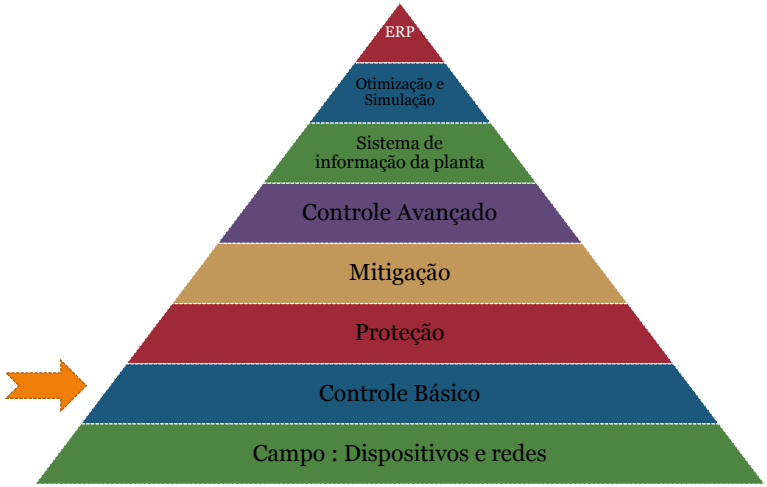
FOUNDATION Fieldbus

Integración Digital de Operação (valor + estado) e de Manutenção

- Mais dispositivos
- Function Blocks
- Interoperabilidade

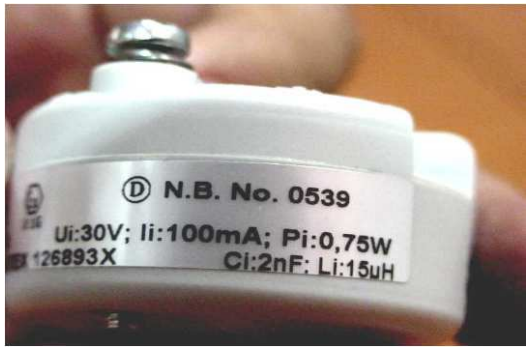


Níveis de Automatização



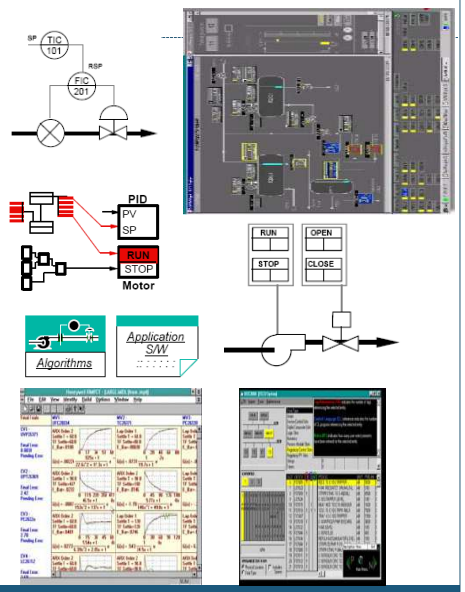
Monitoração e Controle de Processo

- Os sistemas de medição e controle regulam os processamentos e fluxos de materiais e de energia. O desempenho dinâmico correto destes sistemas torna as falhas internas raras.
- Quando acontece uma falha, sua ocorrência é facilmente evidenciada para o operador, através das indicadores e registradores.
- Quando o controle automático é insuficiente de fornecer o resultado desejado, (por falha da estação automática, má sintonia, carga diferente do processo), o operador transfere a operação de automática para manual. Isto não causa nenhum problema particular ao processo, que contínua operando com produtos dentro das especificações.



Controlador: Funções básicas

- Controle convencional
- Controle de Dispositivos Discretos
- Controle de sistemas de encravamento de segurança
- Lógica de encravamento
- Comunicações Peer-to-peer
  - Integração com outros equipamentos da rede de controladores
- Simulação de Entradas/Saídas
- Controle avançado



OPERAÇÃO E SUPERVISÃO DO PROCESSO

Supervision, Control and Protection Systems

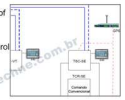
- HEPP Cana Brava
- HEPP Itapebi
- Small Hydroelectric Plant Mosquitão
- HEPP Palmucho
- HEPP Xacbal
- HEPP La Confluencia
- HEPP Boa Esperança
- HEPP São Salvador
- Hydroelectric Improvement Middle Kwanza

Intertechne implemented **Front end engineering designs, Pre-detailed engineering designs and detailed engineering designs of supervision and control** systems of several hydroelectric plants and substations as well as design electrical protection systems for these installations.

The engineering services consisted of:

- **Definition of the basic architecture** of the Supervision and Control Digital Systems (SDSC)
- Technical specification **preparation**.
- **Preparation of detailed functional diagrams** of panels of the Programmable Logic Controllers (PLC)
- **Preparation of** detailed Logic **Diagrams**
- **Preparation of** Functional **Diagrams** of conventional control panels and energy measurement panels for invoicing.
- **Preparation of** operational **manuals.**
- **Preparation of** Unifilar, Trifilar **Diagrams** and Protection System Functions.
- **Preparation of calculations and adjustments** of protection **relays** in generating units, substations and transmission lines.

Intertechne
www.intertechne.com.br



Sala do centro de controle do Tevatron, no Fermilab

Sala do centro de controle de usina nuclear

Causas de Incidentes

41

Um ACIDENTE acontece quando um agente ocorre na imperícia. exemplo: não sabe dirigir um carro,
imprudência (sabe dirigir mas não tomou cuidado) ou negligência (nem sabe dirigir nem toma cuidado).

Quando não acontece imperícia, imprudência ou negligência, e mesmo assim o fato ocorre, então é INCIDENTE, pois se originou de outros fatores (ex: uma pedra se soltou e rompeu a mangueira do óleo do freio, etc).

- os incidentes de planta na indústria petroquímica nos Estados Unidos oscilam entre 10 e 20 mil milhões /ano
- Entre o 3% e o 8% da perda de produção se devem a incidentes
- No mínimo um 40% é causada ou relacionada com as pessoas.

Alarme do processo

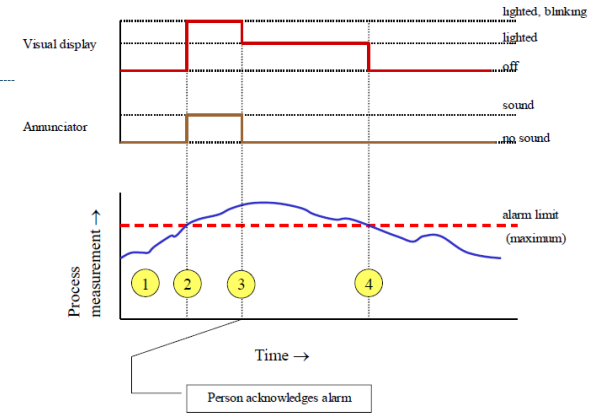
42

- O ideal é que a planta trabalhe em automático todo o tempo. Os distúrbios normais do processo são eliminados pelo controle automático.
- Quando houver uma anormalidade além da faixa de controle automático, o processo deve ser passado para a condição de manual. Para isso, deve haver sistema de alarme para chamar a atenção do operador, pois ele não está todo o tempo olhando os controladores e atualmente há tantas informações concentradas em tão pouco espaço que é impossível o operador perceber prontamente quando o controle automático é perdido.
- Na maioria dos casos, a atuação manual do operador no processo é suficiente para trazer o processo para as condições ideais. Porém, em uma minoria dos casos, a atuação manual não consegue retornar a variável de processo para o ponto de ajuste e o processo tende para condições de perda de produto ou inseguras.

Alarme do processo

43

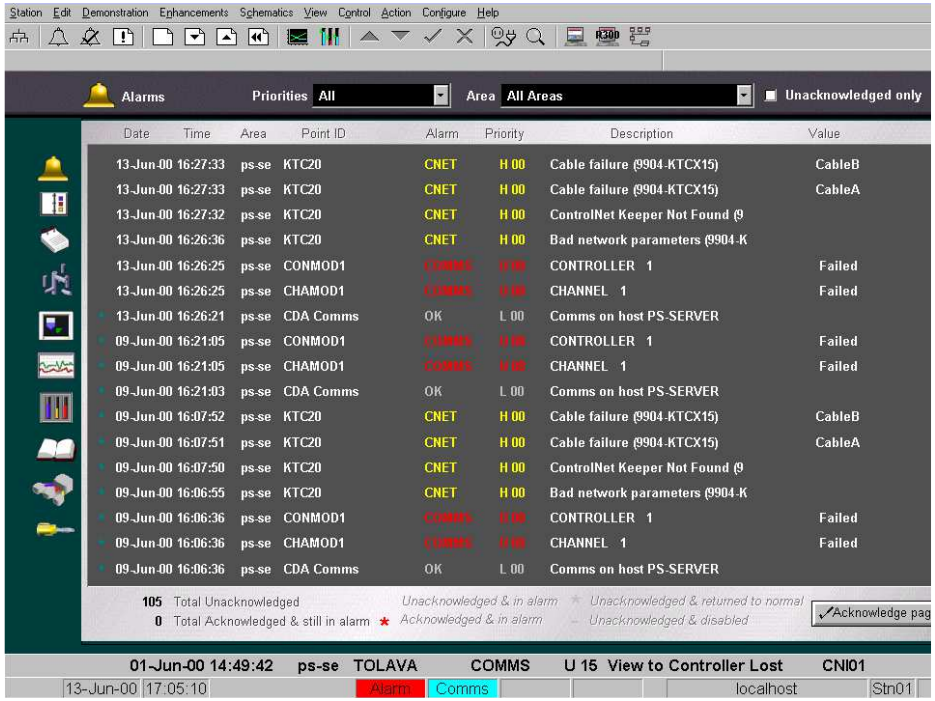
- Nesta camada na hierarquia de segurança são o alarmes, que são importantes porque uma pessoa pode ser responsável por uma seção de planta grande, complexa, com centenas de medições. Idealmente, esta pessoa monitora todas as variáveis simultaneamente, o que não é possível. Um alarme é projetado para alertar a pessoa para potenciais problemas de segurança associados a uma medição.
- Requeresse de um sensor de alarme e de um cálculo da medida, a que se compara a um valor limite pré-definido, e equipamentos para ganhar a atenção do pessoal da planta.

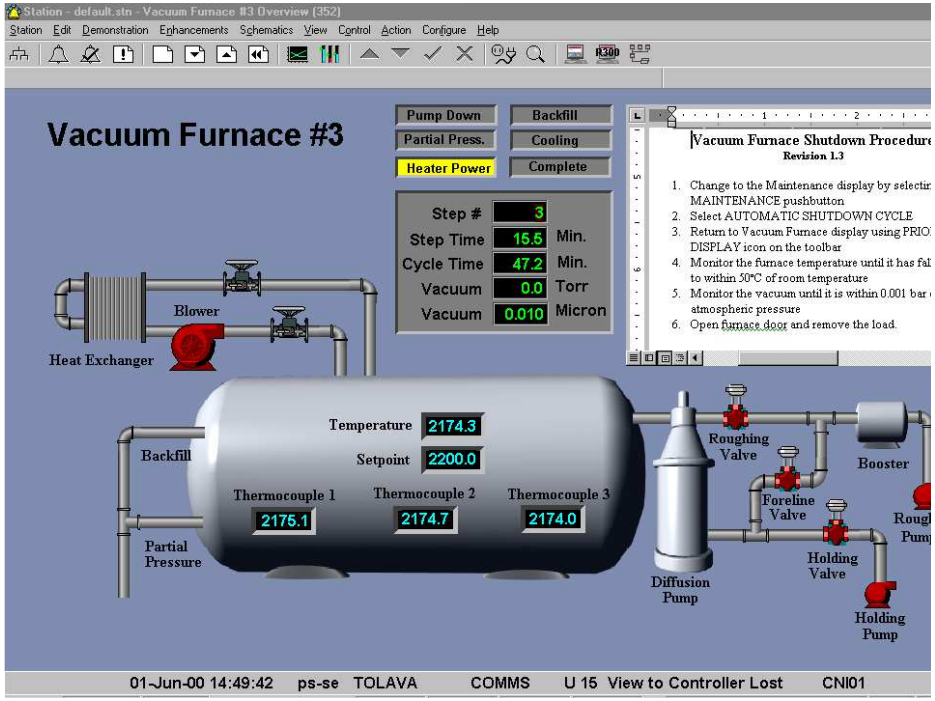


44

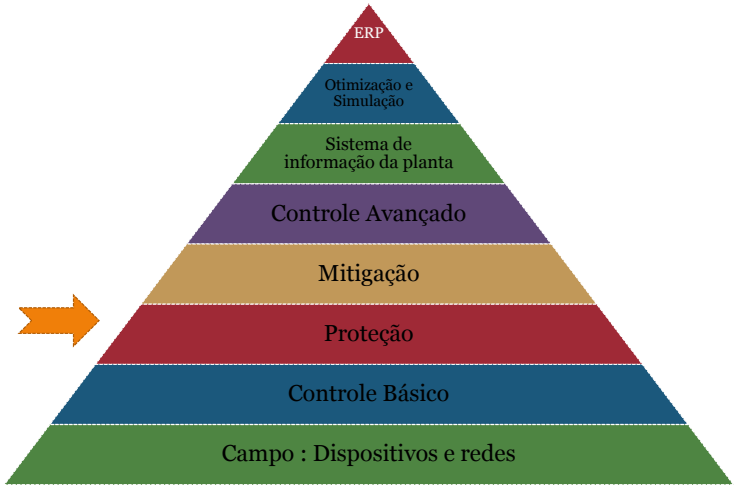
Uma sequência de alarme típica :

1. Começamos com a medição dentro do intervalo aceitável, ou seja, abaixo do limite superior. Sem sinal visual ou anunciador sonoro ativado.
2. Se a medição exceder o limite. O indicador de sons e pisca luz são ativados.
3. A pessoa reconhece o alarme. O indicador para, mas a o pisca luz já não fica aceso, indicando a necessidade de atuar nas variáveis para valor limitante.
4. A medição retorna dentro da região aceitável ; o pisca-luz é desligado.



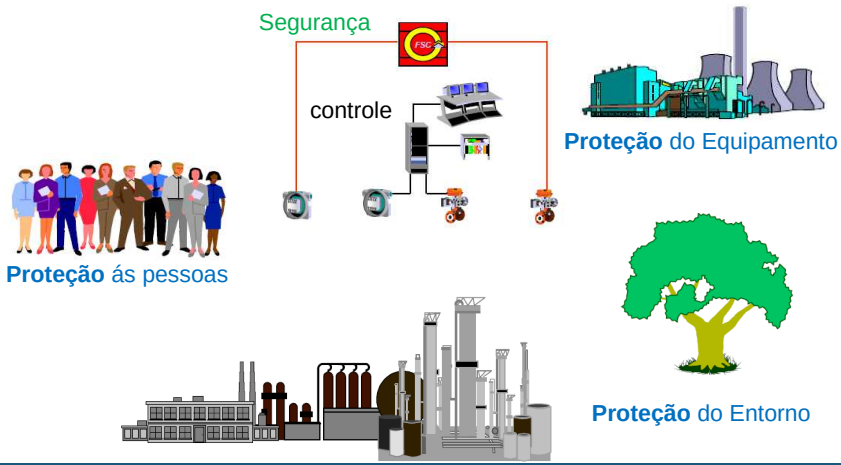


Níveis de Automatização



Camada de Proteção

- **Objetivos dos Sistemas de Controle e de Segurança**



Camada de Proteção: Sistemas de Controle e de Segurança

Os sistemas de segurança devem ser selecionados e instalados de modo a atender aos seguintes requisitos:

a) ter categoria de segurança conforme prévia análise de riscos prevista as normas técnicas oficiais vigentes;

b) estar sob a responsabilidade técnica de profissional legalmente habilitado;

c) possuir conformidade técnica com o sistema de comando a que são integrados;

d) instalação de modo que não possam ser neutralizados ou burlados;

e) manterem-se sob vigilância automática, ou seja, monitoramento, de acordo com a categoria de segurança requerida, exceto para dispositivos de segurança exclusivamente mecânicos; e

f) paralisação dos movimentos perigosos e demais riscos quando ocorrerem falhas ou situações anormais de trabalho.

Camada de Proteção

As proteções, dispositivos e sistemas de segurança **devem integrar as máquinas e equipamentos,** e **não** podem ser considerados **itens opcionais** para qualquer fim.

Análise de camadas de proteção (LOPA)

Camada de Proteção

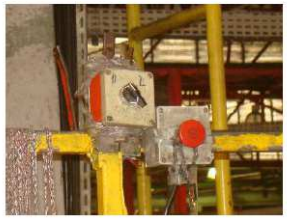
Dispositivos de Parada de Emergência

Camada de Proteção

Os dispositivos de parada de emergência devem ser posicionados em locais de fácil acesso e visualização pelos operadores em seus postos de trabalho e por outras pessoas, e mantidos permanentemente desobstruídos.

Camada de Proteção

Parada de emergência



Camada de Proteção

Parada de emergência

Segurança da Planta

Projeto da planta

- Toda planta deve ser projetada usando-se princípios de segurança baseados em praticas de engenharia estabelecidas.
- Procedimentos como:
  - Perigo e Operabilidade - Hazard and Operability (HAZOP),
  - Análise de Perigo - Hazard Analysis (HAZAN) e
  - Análise de Arvore de Falha – Fault Tree Analysis (FTA)

podem revelar problemas potenciais de segurança e operação relacionados com o projeto.

Projeto da planta

Depois de projetada, instalada e dada a partida (*start up*) a planta entra em operação de regime. Há vários sistemas automáticos associados à planta, para garantir sua operação correta e eficiente e a segurança dos equipamentos envolvidos e dos operadores presentes.

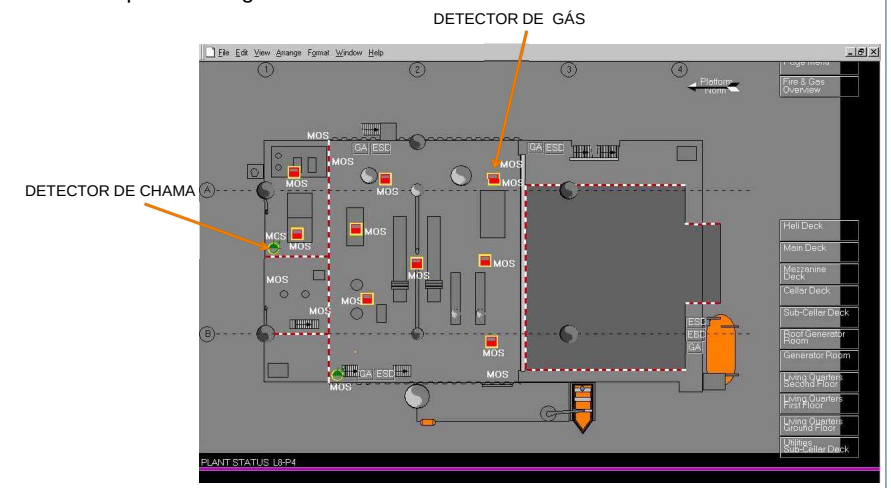
Pode-se perceber quatro níveis distintos de atividade da planta:

1. Medição e controle regulatório do processo,
2. Alarme do processo,
3. Desligamento de emergência,
4. Monitoramento e controle do fogo

- o sistema procura eliminar o julgamento humano das funções críticas de segurança. O sistema atua automaticamente no processo, desligando-o ordenadamente.
- A proteção da planta independente da ação humana é implementada pelo sistema de desligamento, com suas entradas e saídas dedicadas e completamente separadas do sistema de controle do processo.
- Este sistema monitora as operações em uma condição estática, até ser ativado ou disparado por uma condição anormal prevista.
- O sistema requer um alto nível de diagnose, geralmente não existente nos equipamentos de controle do processo, para detectar falhas internas que podem não ser facilmente evidente.

- Mesmo com o sistema de regulação, alarme e desligamento, ainda é possível haver fogo ou explosão no processo. Pode haver falhas no sistema de alarme e desligamento, que deixa de atuar em condição de perigo ou pode haver fogo provocados por outras fontes diferentes.
- Os perigos devidos a gases combustíveis e tóxicos são manipulados por outro sistema.
- Este sistema além de detectar a presença de gases no local também pode ter condição de desligar equipamento do processo, ou seja, o sistema de detecção de gases pode inicializar o sistema de desligamento. Em plantas grandes e complexas, hoje a tendência é de integrar o projeto e suprimento do gás e fogo com o sistema de desligamento, ambos agrupados em um mesmo sistema de segurança.

Gráfico sinóptico de Fogo e Gás no Sistema de Controle



Sistemas instrumentados de segurança – SIS

A grande expansão do uso de Controladores Programáveis ou simplesmente CLPs (como são mais conhecidos na indústria) popularizou e barateou seu uso. Os CLPs são equipamentos extremamente confiáveis, com alta disponibilidade, fáceis de programar e bastante flexíveis, podendo ser aplicados a praticamente todos os tipos de controle industriais.

No entanto, para aplicações em sistemas instrumentados de segurança em processos de alto risco, os CLPs convencionais não devem ser utilizados. Para estas aplicações devem ser usados CLPs especialmente projetados para atuar em áreas de segurança, denominados CLPs de segurança ou Safe PLCs. Estes equipamentos trabalham com o conceito de falha segura e alta integridade.

Sistemas instrumentados de segurança – SIS

Nenhum sistema é completamente imune a falhas, mas na maioria dos casos, esta falha pode ser controlada colocando o sistema em um estado seguro.

É o que chama-se de falha segura (*Fail Safe)*.

Sistemas instrumentados de segurança – SIS

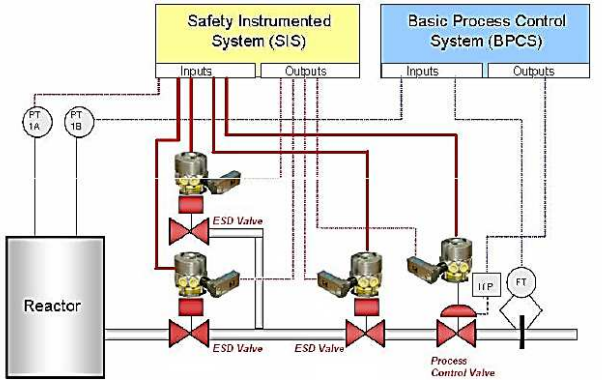
O primeiro passo da identificação do perigo, assumir que não existem proteções:

Sistemas instrumentados de segurança – SIS

- Sistemas instrumentados destinados a proteger sistemas industriais diferem significativamente daqueles projetados para controlar processos gerais.
- Sistemas instrumentados de segurança monitoram continuamente variáveis selecionadas, mas permanecem inativos até que uma condição anormal e possivelmente perigosa ocorra.
- Para funcionar satisfatoriamente, um SIS requer um nível superior de performance e diagnóstico do que o normalmente solicitado para um equipamento genérico de controle de processo. É necessária, nos processos industriais, a separação de sistemas de segurança dos sistemas de controle gerais.

Sistemas instrumentados de segurança – SIS

Sistemas Instrumentados de Segurança (SIS) e Sistema Básico de Controle de Processos



Segurança Totalmente baseada no PLC de segurança + Transmissor SIL + Atuador SIL (não está ligado numa malha de BPCS comum e vulnerável a falhas)

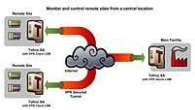
Sistemas instrumentados de segurança – SIS

Um sistema instrumentado de segurança SIS é composta de sensores, processadores e elementos atuadores projetados com a finalidade de:

- Levar automaticamente um processo industrial para um estado seguro quando condições específicas forem violadas;
- Permitir que o processo seja executado normalmente quando condições específicas permitirem (funções que dão permissão); ou
- Executar ações que reduzam as consequências de um acidente industrial.

Norma

- Os CLPs de segurança são empregados em sistema de:
  - shutdown de plataformas de petróleo,
  - sistemas de fogo e gás,
  - bombeamento de petróleo,
  - caldeiras,
  - queimadores,
  - enfim, sistemas que podem provocar riscos de vida a pessoas, riscos de grandes prejuízos econômicos e ao meio ambiente.



- A Norma IEC61508 dá um tratamento sistemático para todas atividades do Ciclo de Vida de um SIS, possibilitando que os desenvolvimentos tecnológicos dos produtos se realizem em um ambiente sistemático de Segurança Funcional. A norma busca potencializar as melhorias dos PES (Programmable Electronic Safety), nome dado aos controladores de segurança nos aspectos de desempenho e de viabilidade econômica, uniformizando conceitos e servindo de base para elaboração de normas setoriais.

Hazop

- HAZOP (HAZARD AND OPERABILITY STUDIES) é uma técnica de análise qualitativa desenvolvida com o intuito de examinar as linhas de processo, identificando perigos e prevenindo problemas.
- Esta metodologia é baseada em um procedimento que gera perguntas de maneira estruturada e sistemática através do uso apropriado de um conjunto de palavras guias aplicadas a pontos críticos do sistema em estudo.
- As palavras-chaves/palavras-guias são aplicadas às variáveis identificadas no processo (pressão, temperatura, fluxo, composição, nível, etc.) gerando os desvios, que nada mais são do que os perigos potenciais.

Hazop

Palavras-Guia	Desvios Considerados
NÃO, NENHUM	Negação do propósito do projecto. (ex.: nenhum fluxo)
MENOS	Decréscimo quantitativo. (ex.: menos fluxo)
MAIS, MAIOR	Acréscimo quantitativo. (ex.: mais fluxo)
TAMBÉM, BEM COMO	Acréscimo qualitativo. (ex.: também)
PARTE DE	Decréscimo qualitativo. (ex.: parte do fluxo)
REVERSO	Oposição lógica do propósito do projecto. (ex.: fluxo)
OUTRO QUE, SENÃO	Substituição completa. (ex.: outro que ar)

È recomendado para novos projetos ou modificação de processos já existente.

Hazop

Parameter (variable)	Applicable Guidewords
Flow	No, more, less, reverse,
Temperature	Higher, lower (more, less)
Pressure	Higher, lower (more, less)
Level	Higher, lower (more, less)
Composition	No, more of, less, more than, other than
Chemical reaction	No, more of, less, more than, other than
Phase(s)	No, more of, less, more than, other than
pH, viscosity, humidity and other properties	Higher, lower (more, less)
Time sequence	Sooner, later, longer shorter
Sampling, checking, maintenance	No, more, less, more than, other than

Exemplo de uma forma HAZOP

Company: XYZ Polymer Limited			Facility: Hamilton Works		
Design Intent: Raise circulating oil stream temperature flowing at 100 m^3/h from 250 to 400 °C			HAZOP Team Members:		
Drawing: Figure 5.20				Date: Jan 2, 2011	
1.0 Node: Pipe after feed pump before entering heater					
Parameter: Flow					
ID. No.	Guideword / Deviation	Causes	Consequences	Safeguards/ checks	Actions
1.1	No Flow	a. pump motor failure	a. Fluid in pipe being overheated pipe metal overheated and damaged Pipe bursting and releasing oil into the firebox (in contact with flame) Shutdown and loss of production	a. Reliable power supply to motor low flow alarm	a. feed flow sensor and SIS on low flow • Close fuel valves • Open air valve • Alarm with SIS • Manual reset • Short delay to guard against noise • Manual activation of SIS possible • Open stack damper Low flow alarm using controller sensor
		b. coupling failure	b. Hazard from metal pieces at high velocity		b. Install guard over coupling
		c. feed valve closure	See (a) above	c. Flow controller, valve fail open	See (a) above

Safety Integrity Level (SIL)

CONCEITOS BÁSICOS
de Nível de Integridade de Segurança / Safety Integrity Level (SIL)

SIL representa um nível de probabilidade máxima de ocorrência de um acidente, admitido para uma planta ou função.

Seu nível é definido através de métodos de avaliação contingencial

PFD_{avg} exprime a probabilidade média de que um equipamento falhe de forma comprometedora, quando solicitado.

PFD Deve ser o menor possível
Deve ser compatível com o SIL pretendido.

SIL IEC 61508	SIL ANSI/ISA S84	PFD
1	1	0.1 to 0.01
2	2	0.01 to 0.001
3	3	0.001 to 0.0001
4	4	0.0001 to 0.00001

Quão confiáveis são os instrumentos?

- A confiabilidade pode ser estimada usando a seguinte equação:

$$R = e^{-\mu t}$$

Aqui R é a confiabilidade, μ é a frequência de falha anual (falha / ano) e t é o tempo (anos)

- A probabilidade de falha pode ser, então, estimada:

$$p = 1 - R = 1 - e^{-\mu t}$$

p é a probabilidade anual de falha

Outro modelo mais complexo

- ***PFDavg* = D_C x λ^D_{sol} x (MTTR x TI_{PS} / 2) + (1 - DC) x λ^D_{Sol} * TI_{FS} / 2)**
  - *PFDavg = Probabilidade Média de Falha da Demanda*
  - D_C = Cobertura do diagnóstico
  - λ^D_{sol} = Frequência de Falhas de Risco (falhas / ano)
  - TI_{PS} = Intervalo entre testes parciais (Partial Stroke)
  - TI_{FS} = Intervalo entre testes globais (Full Stroke)
  - MTTR = Tempo médio de reparo

SIL

- O SIL é uma medida de desempenho do sistema de segurança, em termos de probabilidade de falha na demanda (P_{FD}). Quanto maior é o SIL, mais fiável ou eficaz é o sistema.
- Cada função de segurança instrumentada (SIF) tem uma classificação SIL guiada pela norma IEC 61508
- ANSI / ISA S84.01 e IEC 61508 exige que as empresas (fabril) atribuíam um SIL para qualquer SIS novo ou adaptado.
- Três padrões específicos da indústria foram liberados usando a norma IEC 61508: IEC 61511 (processos), IEC 61513 (nuclear) e IEC 62061 (manufatureiras)

SIL x PFD

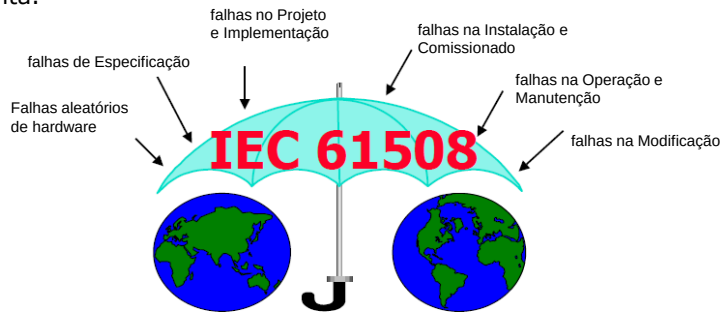
PFD - Probability of Failure on Demand per year

Safety Integrity Level (SIL)	PFD (Low Demand Mode)	PFD (High Demand Mode)
1	> 10^{-2} to < 10^{-1}	> 10^{-6} to < 10^{-5}
2	> 10^{-3} to < 10^{-2}	> 10^{-7} to < 10^{-6}
3	> 10^{-4} to < 10^{-3}	> 10^{-8} to < 10^{-7}
4	> 10^{-5} to < 10^{-4}	> 10^{-9} to < 10^{-8}

Modo de baixa demanda - operação intermitente (menos de 11 anos)
Modo de alta demanda - sistemas de operação contínua ou que atua a mais de 11 anos

Norma IEC-61508

- A Norma IEC-61508 define um valor mínimo de SIL requerido para novos ou modernizados sistemas de instrumentação. Estes sistemas consistem de instrumentação ou controles que estão instalados com objetivo de mitigar riscos ou trazer o processo para condição de operação segura no caso de ocorrência de situações anormais na planta.



Níveis de Automatização

Mitigação

Atualmente um grande número de industrias, principalmente as químicas empregam reagentes que, sob certas condições, podem levar a um total descontrole do processo gerando risco de explosão e emissão de gases tóxicos.

Mitigação, em ambiente consiste numa intervenção humana com o intuito de reduzir ou remediar um determinado impacto ambiental, nocivo. também significa referencia relativa a um determinado ato.

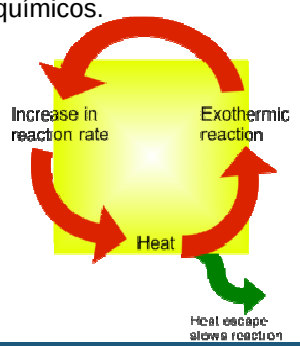
Mitigação

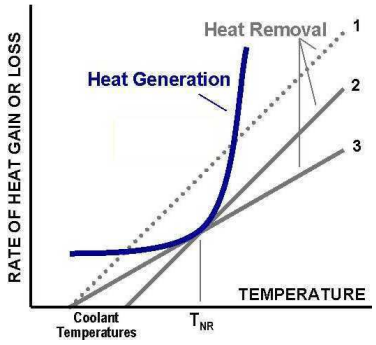
Reações *Runaway*

- As reações sujeitas a descontrole térmico são as mais conhecidas pelo termo em inglês de "*runaway*", "*runaway reaction*" ou "*thermal explosions*".
- Em linhas gerais, as reações *runaway* ocorrem em processos exotérmicos onde o calor gerado excede o que dele pode ser removido.
- Com o aumento da temperatura, a taxa de remoção de calor, que segue um comportamento linear, mas a taxa na qual o calor é produzido aumenta exponencialmente. Uma vez que o controle da reação é perdida, a temperatura pode subir rapidamente deixando pouco tempo para correção ou ações. O reator pode estar em risco de sobrepressurização devido à geração violenta de gás ou rápida ebulição .

Mitigação

- Reações de "*runaway*" estão normalmente associadas às reações de nitração, polimerização, processos envolvendo ligações insaturadas (duplas ou triplas) e compostos de ligações: N-N; N-O; CI-O; O-O e N-CI.
- Essas reações podem ocorrer tanto em reatores quanto em tanques de estocagem estando também associadas à decomposição de produtos químicos.





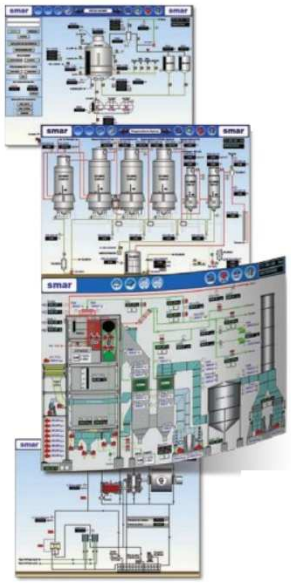
Mitigação

Efeitos das reações *runaway* :

- Transbordamento da massa reacional conduz à ruptura do vaso ou reator.
- As ondas de choque e o efeito míssil resultantes da explosão poderiam causar sérios danos materiais.
- Em alguns casos a mudança dos mecanismos reacionais pode resultar diretamente numa detonação interna com efeitos desastrosos.

Causas de incidente com reações *runaway* :

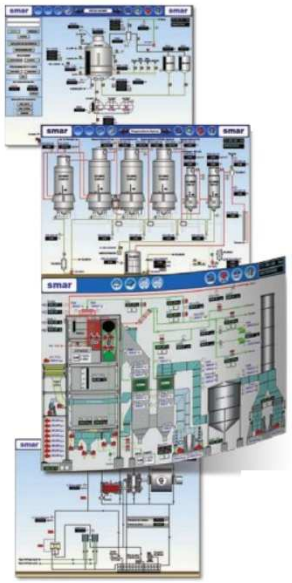
- Conhecimento insuficiente do processo termoquímico.
- Projeto de troca térmica (remoção de calor) inadequado.
- Sistemas de controle insatisfatório
- Sistemas de segurança impróprios
- Procedimentos operacionais inadequados e treinamento insuficiente.



Identificando os riscos

O conhecimento do processo constitui o primeiro passo para se traçar um plano de identificação e mitigação dos riscos relacionados a reação *runaway*.

Nesse contexto, destaca-se alguns dos aspectos que podem facilitar essa análise:



Identificando os riscos

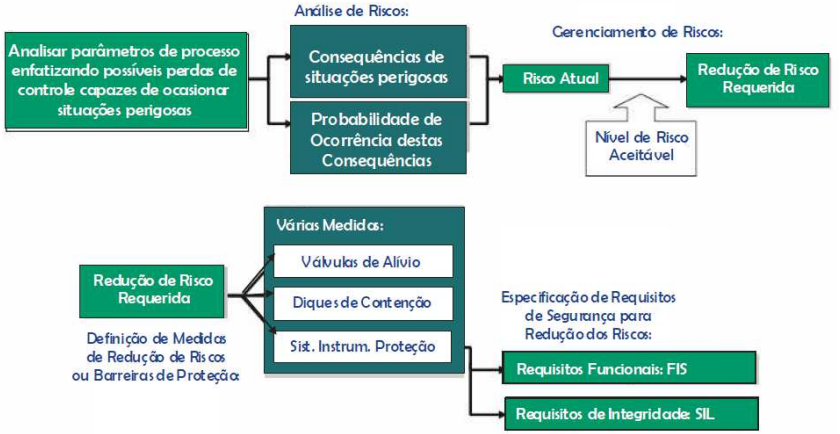
- Reunir toda a documentação pertinente ao processo: planta de P&ID, balanços de massa e energia, etc.
- Elaborar um fluxograma e inclua as informações básicas (tais como volume de reator, etc.) e estabeleça as condições normais de operação; verifique quais os controle existente (manuais e automáticos)
- Observar se existem redundâncias no controle do processo e na instrumentação.
- Informar-se sobre a cinética das reações envolvidas no processo bem como o seu comportamento termoquímico, ou seja, a taxa de calor produzida.
- Verificar a possibilidade de decomposição térmica de algum produto ou matéria prima envolvida na reação bem como a produção de gases pela reação.

Identificação de Riscos

- Identifique os vents e as válvulas de alívio existentes nos equipamentos, suas condições de trabalho, especificações e seu direcionamento em caso de abertura.

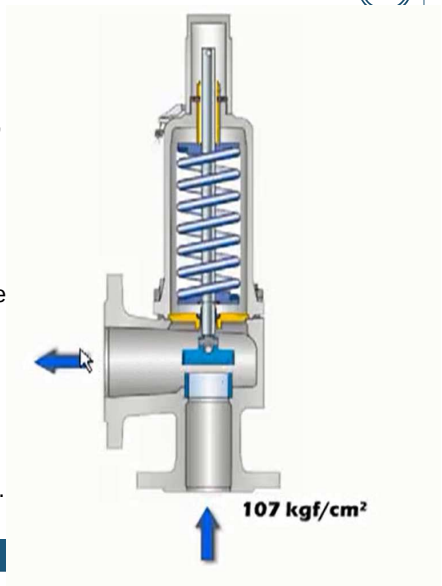
Algumas informações necessárias podem ser obtidas na literatura (data sheets, calores de reação, etc.). No entanto, dependendo da complexidade do sistema, as reações deverão ser testadas e analisadas em equipamentos específicos, como calorímetros adiabáticos ou isotérmicos, necessitando-se de laboratórios especializados.

Identificando os riscos

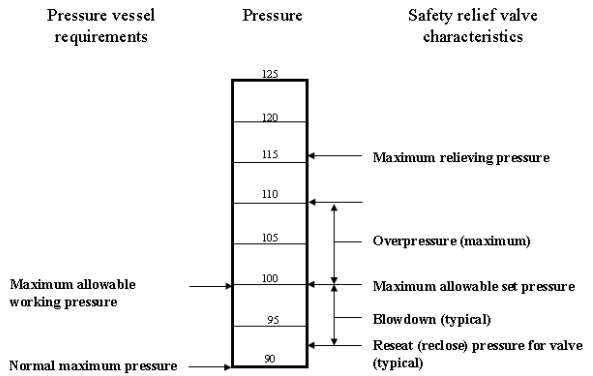


Válvulas de segurança (PSV)

- Este tipo de válvulas se utiliza para o controle da pressão em equipamentos ou linhas, evitando danos tanto a pessoas como a equipamentos a consequência de uma excessiva pressão, ou pelo contrario, por vácuo. As válvulas automáticas também serão de aplicação em sistema nos que se requere um corte imediato da corrente de fluido antes falhas do equipamento.
- O acionamento deste tipo de válvulas é de tipo automático e autónomo não necessitando nenhuma sinal externa para entrar em funcionamento. Seu projeto se baseia em mecanismos simples e fiáveis, tais como a pressão da mola, para o movimento do haste fugindo de sistemas mais complicados mais propensos a falha.



Válvulas de segurança (PSV)



Algumas características típicas da válvula de segurança (Fonte: API RP 521, Guide to Pressure-Relieving and Depressurizing Systems (2nd Ed.), Washington, DC, American Petroleum Institute, 1982.)

Sistemas de Alivio

- **Disco de ruptura ou diafragma:** é um dispositivo de alívio de alternativo e complementar Quando a pressão no interior do recipiente excede o limite superior, o disco irá romper, e o fluido irá escapar do recipiente. O limite de pressão desejada é alcançado através do ajuste do material do disco e da sua espessura. Naturalmente, o disco tem de ser substituídos depois de ter rompido.

  Vantagens: evita vazamento, ideal para manipulação de fluidos corrosivos, liberação rápida de grandes volumes de fluido e aplicação de altas pressões.

  Desvantagens: desligamento processo para substituição e precisão ajuste da pressão.

Sistemas de Alivio

- Os dispositivos de alívio devem estar localizados em qualquer recipiente fechado, ou seja, qualquer espaço confinado significativo tendo um acesso potencialmente restrito para o alívio. Por exemplo, um tanque que ventila para a atmosfera através de um tubo que possui uma válvula de isolamento deve ter alívio de pressão.
- Lembre-se, que o processo deve ser seguro, mesmo quando uma pessoa ou sistema de controle realiza um erro e fecha a válvula de forma inadequada.
- Deve-se fornecer dispositivos de alívio mesmo que os tanques normalmente não experimentem pressões altas, pois o sistema sob um evento de falha poderia experimentar pressões excessivas, tais como numa reação química runaway, falha de uma válvula ou devido a incêndio na planta.

Locais típicos de instalação de sistemas de alívio de segurança

Location and Reason	Process Examples
Vessel or large pipe that can be isolated by existing valves (including manual values that should be open)	Distillation tower Chemical reactor Flash drum
Vessel due to loss of cooling (e.g., loss of cooling water due to pump failure or power loss)	Distillation Chemical reactor Vapor compression refrigeration
Vessels, pipes (liquid filled) due to external heating from fluid or fire	Water side in condenser Jacket cooling stirred tank (loss of water flow)
Pipe overpressure due to failure of valve or regulator with upstream pressure above downstream limits	Equipment using steam at lower pressure than steam source Exhaust of turbine
Pipe or vessel due to high pressure from equipment	Exit of positive displacement pump Exit of compressor
Heat exchanger shell due to rupture of tube	Shell and tube heat exchangers
Vaporizers due to excess vapor	Distillation Flash drum
Reactors due to sudden condensation (protect against low pressure)	Equipment being cleaned with steam that can condense when contacting cold metal

Identificando os riscos

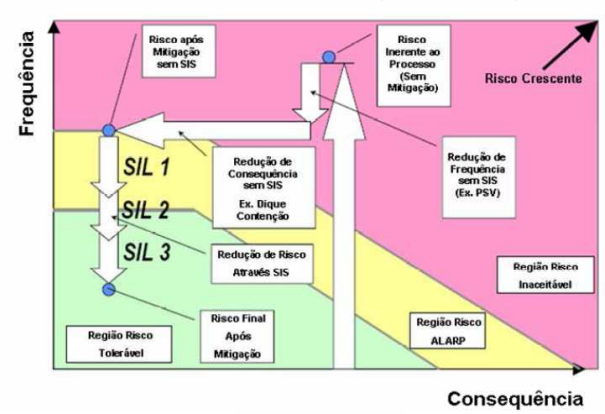
- Os equipamentos cujas falhas contribuem para cada um destes principais perigos são identificados e usualmente classificados como relevantes para a segurança.
- A taxa de falha máxima tolerável para cada perigo identificado, nos fornece um nível de integridade necessário para cada peça deste equipamento, dependendo da sua contribuição para o perigo em questão.
- Este nível de integridade são chamados de "Safety Integrity Levels" (SIL), ou níveis de integridade de segurança, e são descritos por faixas determinadas de frequências de falha na demanda, variando de SIL 1 ao 4.
  - SIL 4: estado da arte, e usualmente inviáveis,
  - SIL 3 : menos oneroso de ser obtido que o SIL 4, porém ainda exige o uso de tecnologias e projeto sofisticado.
  - SIL 2: exige um bom projeto, práticas operacionais avançadas e alto nível de confiabilidade.
  - SIL 1: boas práticas de projeto e confiabilidade.

Níveis de integridade inferiores ao SIL 1, indicam que o equipamento não é relevante para a segurança.

Identificando os riscos

- **RISCO X SIL**

Um SIS é apenas mais uma camada de proteção, dentre outras que podem ser usadas para manter o processo em condição de operação segura.

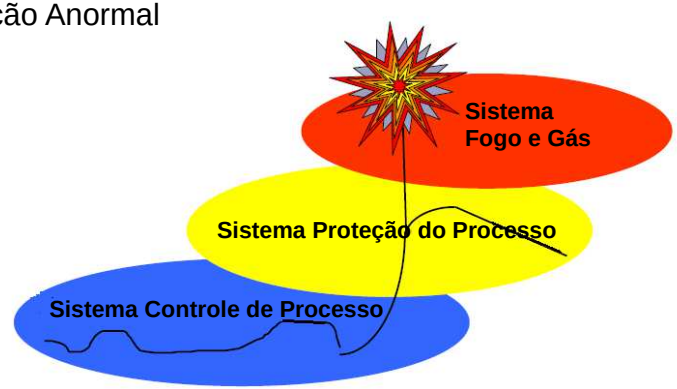


Custos

- **Segurança nas industrias de processo - Thai Oil Dezembro 1999**

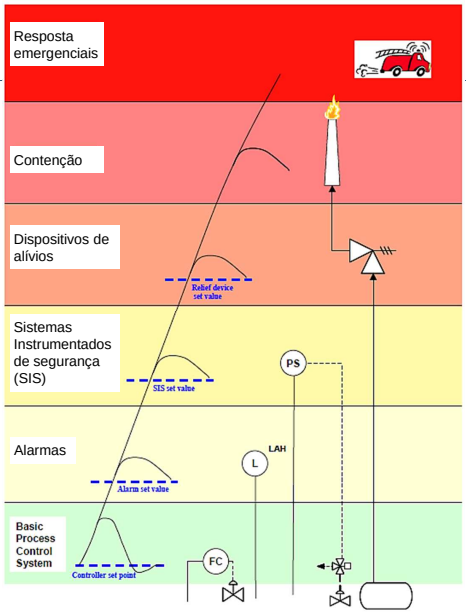
Mitigação

Situação Anormal



Tendência da Hierarquia de Segurança

As respostas das camadas são mostradas para um cenário hipotético em que aumenta o desvio de operação normal ao longo do tempo.



Solução de Segurança para Prevenção e Mitigação

Figura 9 de IEC 61511

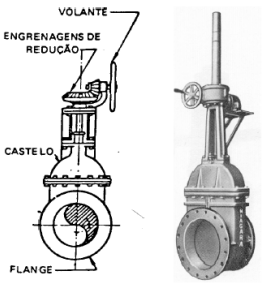
Válvulas manuais

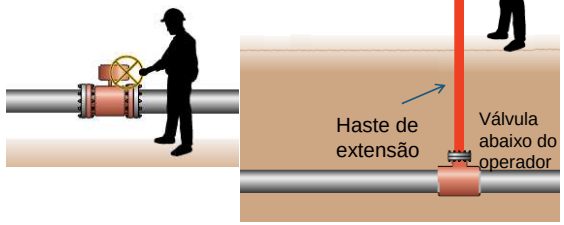
Válvulas manuais

- as válvulas manuais exigem a ação direta do usuário sobre elas para efetuar sua regulação.
- O obturador é movido pela mesma força exercida pelo operador, existindo diversos mecanismos de transmissão da força como podem ser redutores, trens de engrenagens, etc. através dos quais se transforma a ação humana numa variação da posição do obturador.
- Este tipo de válvula exige a presença física de um operador no equipamento para sua regulação. Devido que não é possível seu acionamento remoto estas válvulas não admitem seu uso como elementos finais de regulação de um sistema de controle de processos.

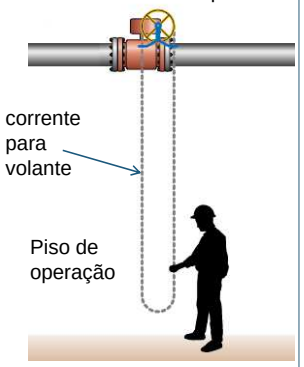
Válvulas Manuais

OPERAÇÃO MANUAL





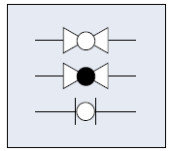
Válvula acima do operador



Válvulas manuais

Válvulas manuais

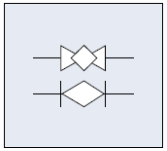
Válvula Esfera (ball valve)

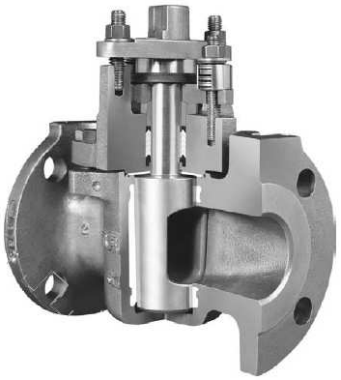


Válvulas manuais

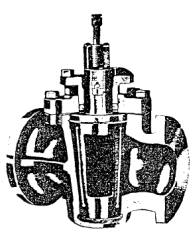
Válvulas manuais

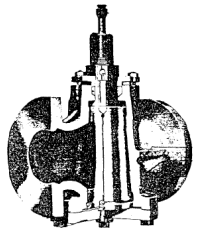
Válvula Macho (plug valve)



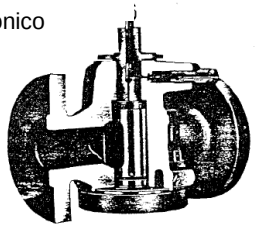


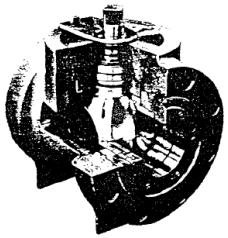
Válvulas manuais: Tipos





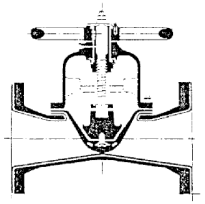
Válvulas de obturador cónico

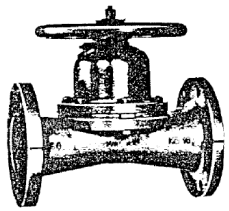




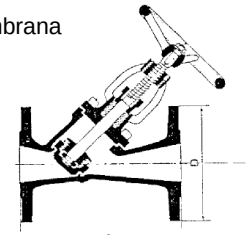
Válvulas de obturador cilíndrico e esférico

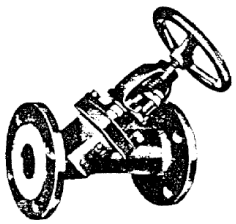
Válvulas manuais: Tipos





Válvula de membrana





Válvula de obturador inclinado

Válvulas manuais: Instalação

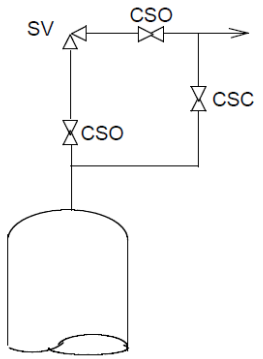
- as válvulas de acionamento manual se usam em linhas onde não seja necessário uma regulação frequente da corrente para manter e controlar o régime do processo.
- Salvo exceções, numa planta de processo industrial as válvulas manuais se utilizam unicamente como elementos de bloqueios de linhas, já que as aplicações onde se requer a modulação da corrente de passo se recorre a válvulas automáticas.
- Existem situações onde por razoes de segurança é necessário garantir a circulação ou o bloqueio de uma linha, surgindo assim as válvulas CSO e CSC.
- Estas se caracterizam por encontrar-se seladas, impossibilitando assim sua manipulação incontrolada. Quando seja necessário bloquear ou abrir a linha, segundo os casos, se terá que romper o precinto da válvula e trás sua manipulação se deverá de novo precintar e selar.

Válvulas manuais: Instalação

- **Válvulas CSO (*Car Seal Open)*.** Este tipo de válvula se instala em linhas onde se deve assegurar que a válvula se encontre aberta permitindo o passo livre de corrente pela linha.
- **Válvulas CSC (*Car Seal Close*).** Estas válvulas se usam em conduções onde se requere que a linha esteja fechada e uma mudança de posição da válvula implicaria uma situação de risco.

Vejamos agora uma montagem tipo no que podemos ver o funcionamento deste tipo de válvulas.

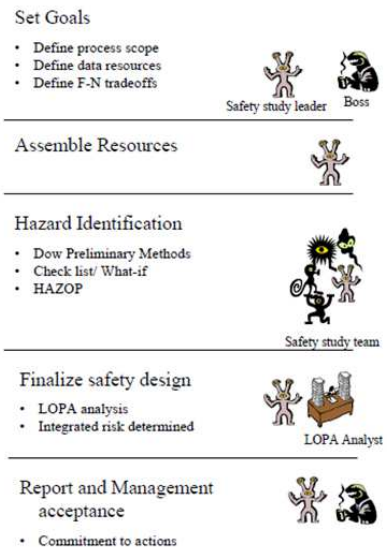
- as válvulas CSO asseguraram o correto funcionamento da válvula de segurança (SV) ao não impedir o passo do fluido pela linha. Por outro lado a função da CSC é inabilitar o *bypass*, já que de outro modo o fluido passaria por ele em vez de ir à SV.
- No suposto de que por questões de manutenção ou reparação fosse necessário trabalhar na válvula de segurança esta se isolaria mediante as duas CSO, passando a corrente pelo *bypass* habilitado pela abertura da CSC.



Em conclusão

- A segurança de processos é um sistema complexo, o que se justifica pela importância do tema segurança em todo os ambitos (pessoas, equipamentos, processos) e os muitos sistemas de engenharia empregados para alcançar um projeto seguro.

- A análise de segurança abordadas nesta unidade são resumidas na figura a seguir, que mostra os principais passos, detalhes importantes em cada etapa, e as pessoas envolvidas. Este processo é seguido tanto para novos projetos e para avaliações de segurança periódicas dos processos existentes



Principais etapas no projeto de segurança com os participantes em cada etapa

Mas, trabalho sem segurança ainda...

Mas, trabalho sem segurança ainda...

Como nós da área de instrumentação e automação podemos ajudar a proteger o meio ambiente ???

Detectar e eliminar emissões fugitivas de gases em :

- ✓ Válvulas, Flanges, Conexões, Vents, Compressores, Turbinas e etc.
- ✓ Reduzir o consumo de recursos naturais (Água, Gás natural, etc)
- ✓ Colocar detectores de gases na planta
- ✓ Medir e Reduzir as emissões de gases e particulados
- ✓ Manter as válvulas sempre com a manutenção em dia.
- ✓ Inverter em Sistemas de Segurança.

Referências

AIChE (1994) *Dow's Fire and Explosion Index Hazard Classification Guide, 7th Ed.*, American Institute of Chemical Engineers, New York

AIChE (1994) *Dow's Chemical Exposure Index, 1st Ed.*, American Institute of Chemical Engineers, New York

API (2007) Pressure Reliving and Depressuring Systems, ANSI/API Standard 521, 5th Ed., January 2007

Beckman, L. (1995) Match Redundant System Architecture with Safety Requirements, *CEP*, 54-61, Dec 1995

Bradsby, M. and J. Jenkinson (1998) The Management of Alarm Systems, Health and Safety Executive (UK) Contract Report, (1998) http://www.hse.gov.uk/humanfactors/topics/alarm-management.htm

Britannica: http://www.britannica.com/EBchecked/topic/250771/Haber-Bosch-process

Cameron, I. and R. Raman (2005) *Process Systems Risk Analysis*, Elsevier Academic Press, Amsterdam

Thomas Marlin (2014) - Operability in Process Design: Achieving Safe, Profitable, and Robust Process Operations, Center for Chemical Plant Safety of the AIChE