# Sistemas de Segurança e Controle Processos Industriais

Adrielle C. Santana

# Conceitos Básicos

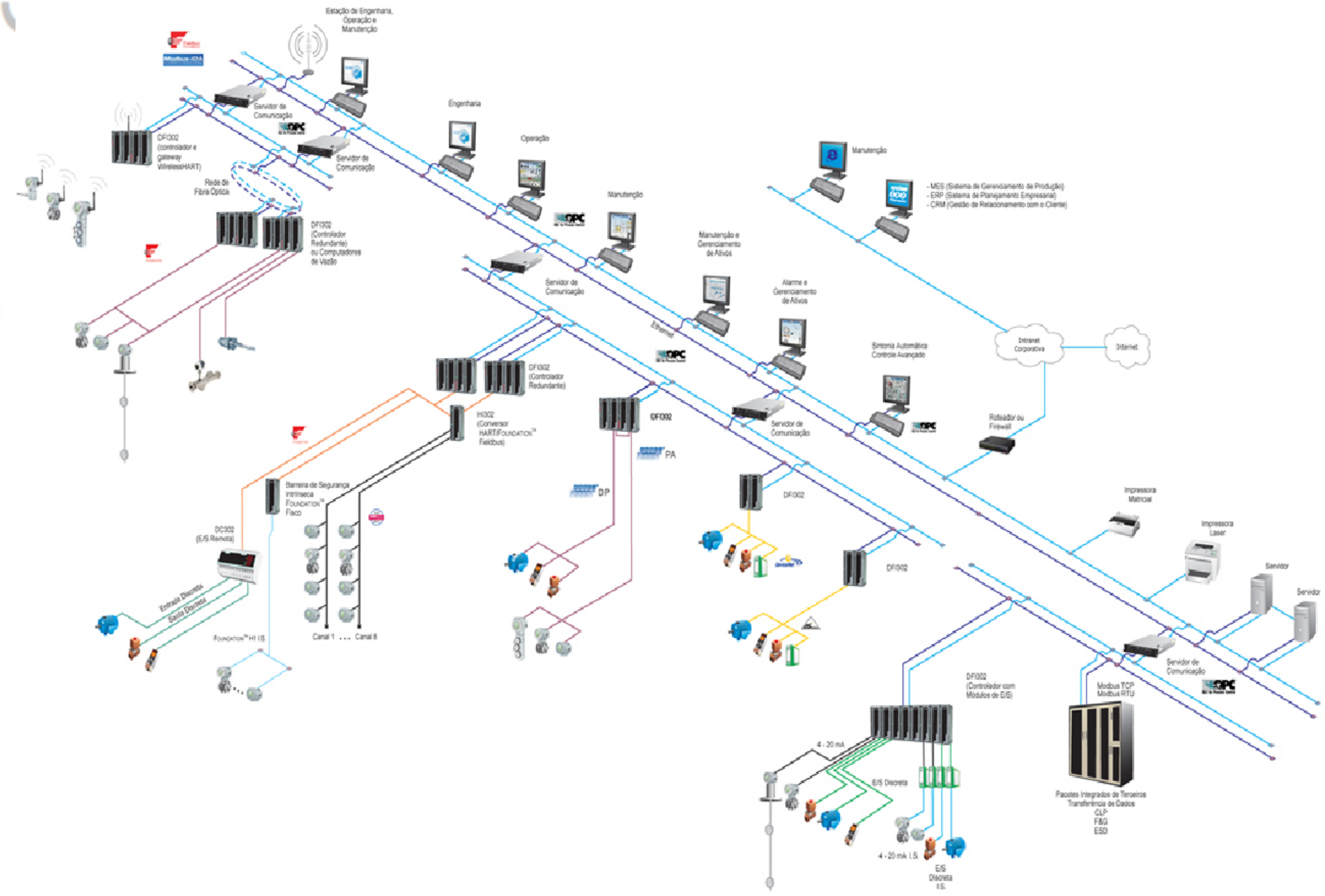
**BPCS - Sistema Básico de Controle de Processo**: Instrumentação e sistema que são instalados para monitorar e controlar operações de produção normais usados mas não limitados a combinações de simples monitores de malha pneumática e eletrônica e controladores, controladores lógico programáveis e sistemas de controle distribuídos.

Um BPCS é necessário para operar uma planta ou processo.

**SDCD:** SDCD é a instrumentação, equipamentos de entrada e saída, equipamentos de controle e equipamentos de interface do operador, que executa as funções de controle e indicação estabelecidas. O sistema permite a transmissão de controle, medição e informação de operação para e de locais únicos ou múltiplos especificados pelo usuário, ligado por um ou vários links de comunicação.

Sistema Digital de Controle Distribuído

# SDCD


Estação de Engenharia, Operação e Manutenção
Servidor de Comunicação
Servidor de Comunicação
DFI302 (controlador e gateway WirelessHART)
Rede de Fibra Óptica
DFI302 (Controlador Redundante) ou Computadores de Vazão
Engenharia
Operação
Manutenção
Servidor de Comunicação
Manutenção e Gerenciamento de Ativos
Alarme e Gerenciamento de Ativos
Manutenção
- MES (Sistema de Gerenciamento de Produção)
- ERP (Sistema de Planejamento Empresarial)
- CRM (Gestão de Relacionamento com o Cliente)
Ethernet
Sistema Automático Controle Avançado
Servidor de Comunicação
Intranet Corporativa
Internet
Roteador ou Firewall
DFI302 (Controlador Redundante)
HI302 (Conversor HART/FOUNDATION™ Fieldbus)
Barreira de Segurança Intrínseca FOUNDATION™ Fisco
DC302 (E/S Remota)
Entrada Discreta
Saída Discreta
FOUNDATION™ H1 I.S.
Canal 1 ... Canal 8
IDF302
PA
DP
DFI302
DFI302
Impressora Matricial
Impressora Laser
Servidor
Servidor
Servidor de Comunicação
DFI302 (Controlador com Módulos de E/S)
4 - 20 mA
E/S Discreta
4 - 20 mA I.S.
E/S Discreta I.S.
Modbus TCP
Modbus RTU
Pacotes Integrados de Terceiros
Transferência de Dados
CLP
F&G
ESD

# Conceitos Básicos

**CLP** é um controlador, usualmente com várias entradas e saídas, que contem um programa alterável que é tipicamente usado para controlar lógica discreta ou binária ou funções seqüenciais e pode também ser usado pra fornecer funções de controle continuas.

**Sistema Instrumentado de Segurança (SIS)**

Sistema Instrumentado de Segurança é o composto de sensores, resolvedores de lógica e elementos finais de controle com o objetivo de levar o processo para um estado seguro quando condições pré-determinadas forem violadas. O tipo do Sistema instrumentado de Segurança depende do SIL (Nível de Integridade de Segurança)

# Papel do SIS

- Implementar segurança numa planta, que proteja a empresa de qualquer responsabilidade em caso de acidentes.
- Implementar uma estratégia de Segurança em uma planta segundo normas Internacionais reconhecidas IEC61508/61511 previne a empresa de custos por omissão na prevenção em caso de acidentes.

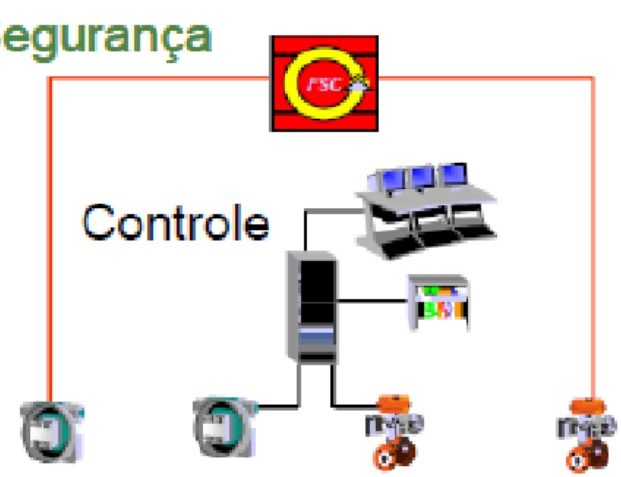
SS49 -plataforma da Bacia de Campos, Fevereiro/2009

- Proteger O Capital e a Rentabilidade da Empresa.
- Proteger a panta, o ambiente, o pessoal e os equipamentos de serem danificados por eventos “não controlados”.
- Melhorar a eficiência.

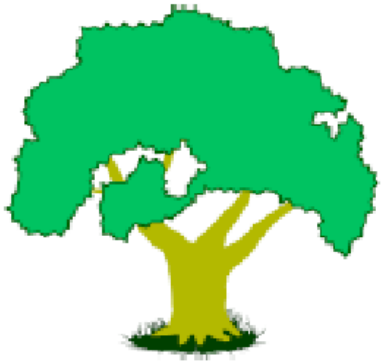
# Conceitos Básicos

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

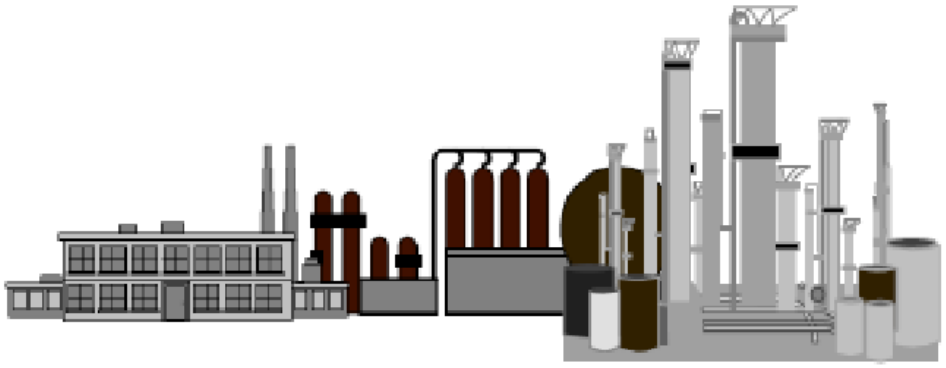
Segurança das pessoas




Proteção do Equipamento



Proteção do Entorno



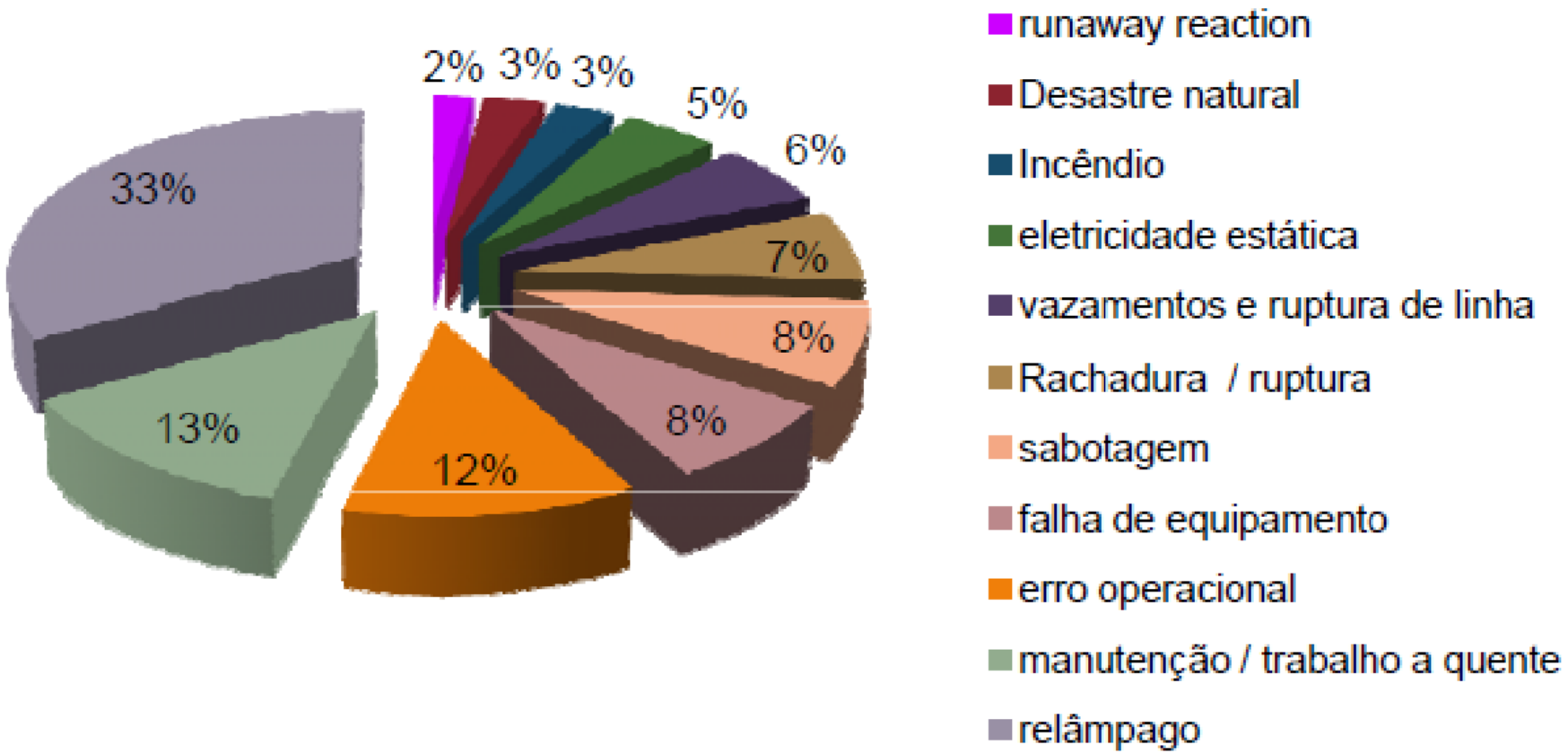
# Principais Riscos de Processo

# Acidentes x Causalidade

- Os acidentes nas indústrias 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 nas Indústrias




FONTE: Safe Control– Professora Ninoska Bojorge – Departamento de Engenharia Química e de Petróleo - UFF

# Causas de Acidentes nas Indústrias

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

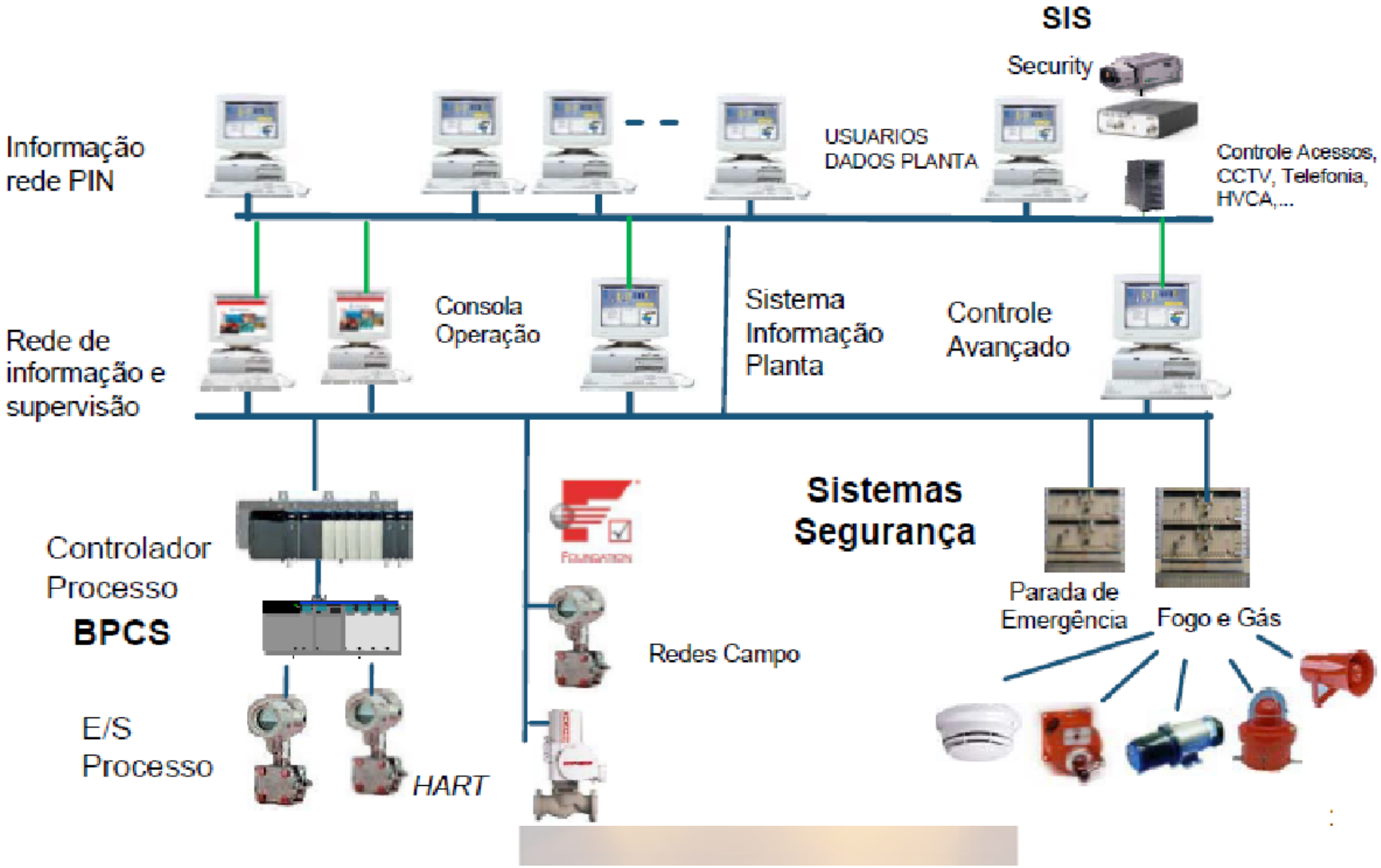
- **Causa humana** :
  - Maus hábitos de trabalho
  - Falta de experiência
  - Falta ou deficiente formação profissional
  - Cansaço
  - Stress

# Trabalho sem segurança ainda é muito comum...

# Trabalho sem segurança ainda é muito comum...

# Trabalho sem segurança ainda é muito comum...

# Segurança e Controle de Processo na Industria



# Medição 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 pelo operador, através de 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.

# Operação e Supervisão do Processo

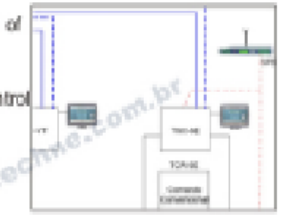
## Supervision, Control and Protection Systems

- 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

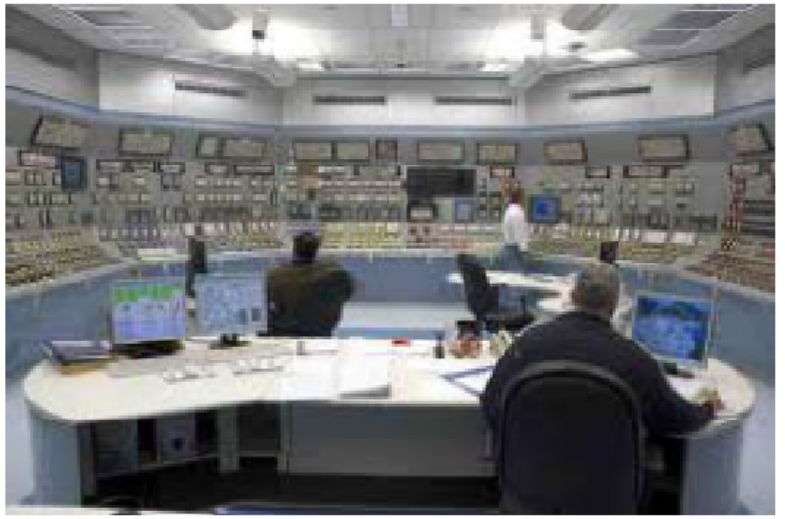
Intertechne implemented **Front end engineering designs, Pre-detailed engineering designs and detailed engineering designs of supervision and control** systems of several hydroelectric plants and substations as well as design electrical protection systems for these installations.

**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.

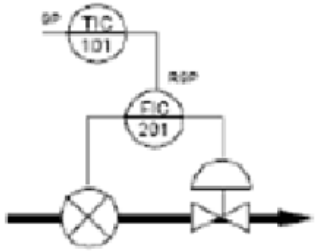


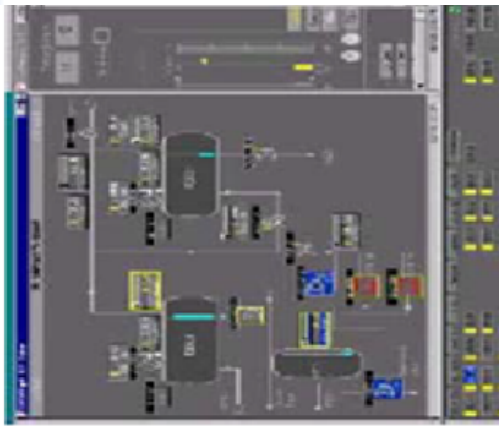
Sala do centro de controle do Tevatron, no Fermilab



Sala do centro de controle de usina nuclear

# Segurança da Planta Controle Básico

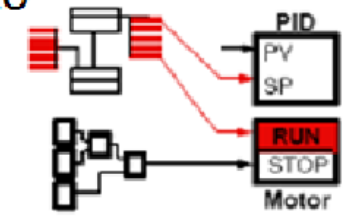


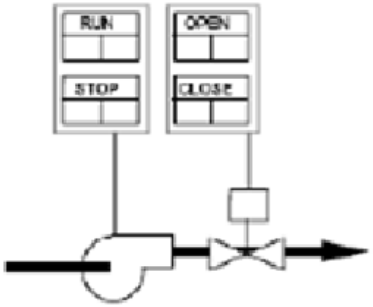



Controlador: Funções básicas

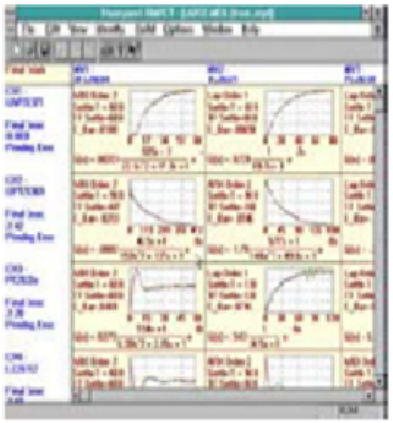
- Controle convencional
- Controle de dispositivos discretos
- Controle de sistemas de intertravamento de segurança
- Lógica de intertravamento
- Comunicações Peer-to-peer

  Integração com outros equipamentos da rede de Controladores
- Simulação de Entradas/Saídas
- Controle avançado







Ex.: De repente uma válvula de sucção apresenta defeito não deixando uma bomba ligar. Desconectar ela fisicamente e simular sua abertura para a bomba ligar.

# SIS

- Um sistema instrumentado de segurança (SIS) executa ações automáticas para manter uma planta em estado seguro, ou levá-lo a um estado seguro quando uma situação anormal se apresenta,
- O SIS pode implementar uma única função ou funções múltiplas para proteger vários riscos do processo na planta.

# SIS

A solução para um sistema instrumentado de segurança SIS é composta de sensores, processadores (resolvedores lógicos) e elementos atuadores, projetados com a finalidade de:

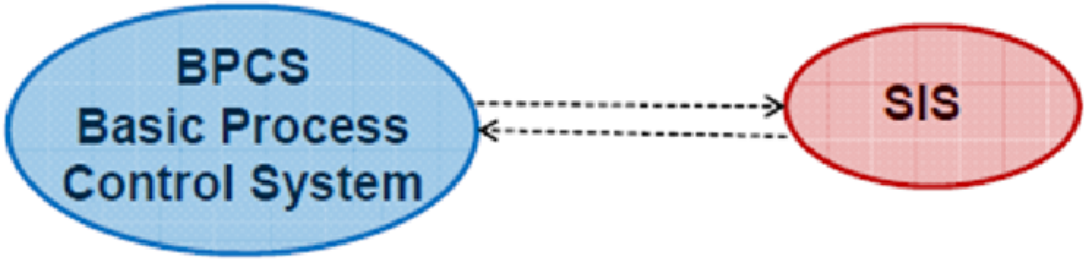
- Levar automaticamente um processo industrial para um estado seguro quando condições específicas forem violadas;
- Permitir que o processo seja executado normalmente quando condições específicas permitirem (funções que dão permissão); ou
- Executar ações que reduzam as consequências de um acidente industrial.

# SIS

**Sistema Instrumentado de Segurança – SIS**

SIS é fundamentalmente diferente do BPCS

- O objetivo do BPCS é produção de qualidade / quantidade.
- O objetivo do SIS é monitoramento de uma condição de processo insegura e a eventual parada da planta se se precisar.




O SIS é fisicamente separado do BPCS para manter sua integridade ainda em caso de falha do BPCS.

Algumas comunicações limitadas são permitidas entre o BPCS e o SIS

# SIS

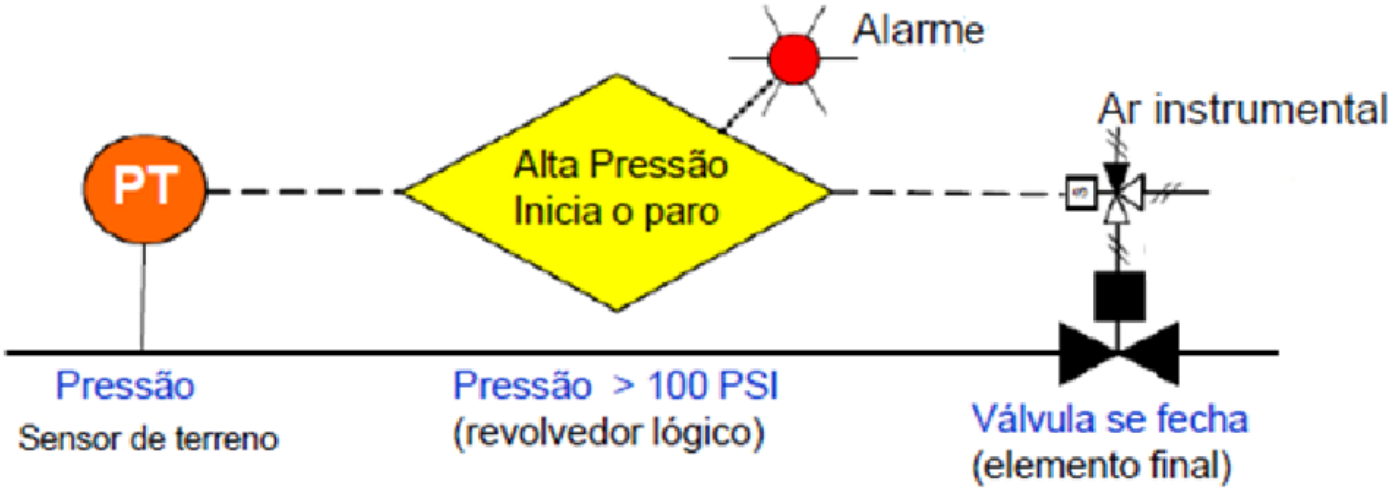
- Os Sistemas Instrumentados de Segurança (SIS) são os sistemas responsáveis pela segurança operacional e que garantem a parada de emergência dentro dos limites considerados seguros, sempre que a operação ultrapassar estes limites.
- O objetivo principal é se evitar acidentes dentro e fora das fábricas, como incêndios, explosões, danos aos equipamentos, proteção da produção e da propriedade e mais do que isto, evitar riscos de vidas ou danos à saúde pessoal e impactos catastróficos para a comunidade.
- Deve-se ter de forma clara que nenhum sistema é totalmente imune a falhas e sempre deve proporcionar mesmo em caso de falha, uma condição segura.
- Exemplos típicos de sistemas de segurança:
  - Sistema de Shutdown de Emergência (ESD)
  - Sistema de Shutdown de Segurança (SSD)
  - Sistema de intertravamento de Segurança
  - Sistema de Fogo e Gás

# 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)*.

# SIS




SIS consiste de 3 componentes:

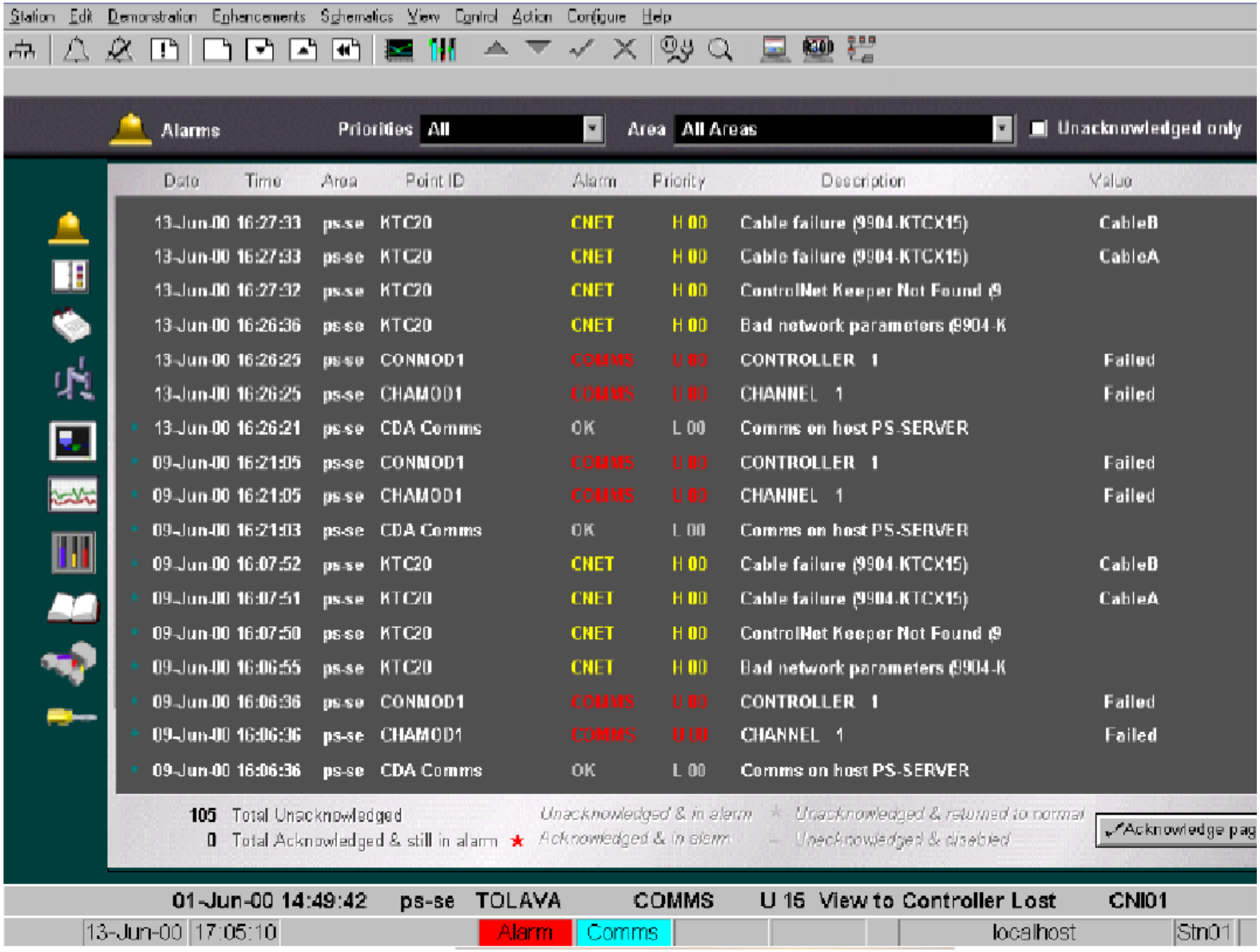
- Sensor que segue o processo para detectar uma alteração ou condição anormal;
- um dispositivo lógico que recebe o sinal do sensor, determina se a condição é perigosa, e, se é, envia um sinal para executar uma ação;
- um dispositivo final de controle que recebe o sinal do dispositivo lógico, e implementa a ação apropriada na planta (p. ex. abrindo ou fechando uma válvula, parando uma bomba).

Os SIS se projetam a diferentes níveis de integridades de segurança (SILs), segundo o risco que apresenta o processo. Quanto mais alto o SIL, mais provável é que tenha componentes múltiplos e redundantes (Ex. mais de 1 sensor, dispositivos lógicos, ou elementos finais) e requerimentos mais rigorosos de ensaios e administração.

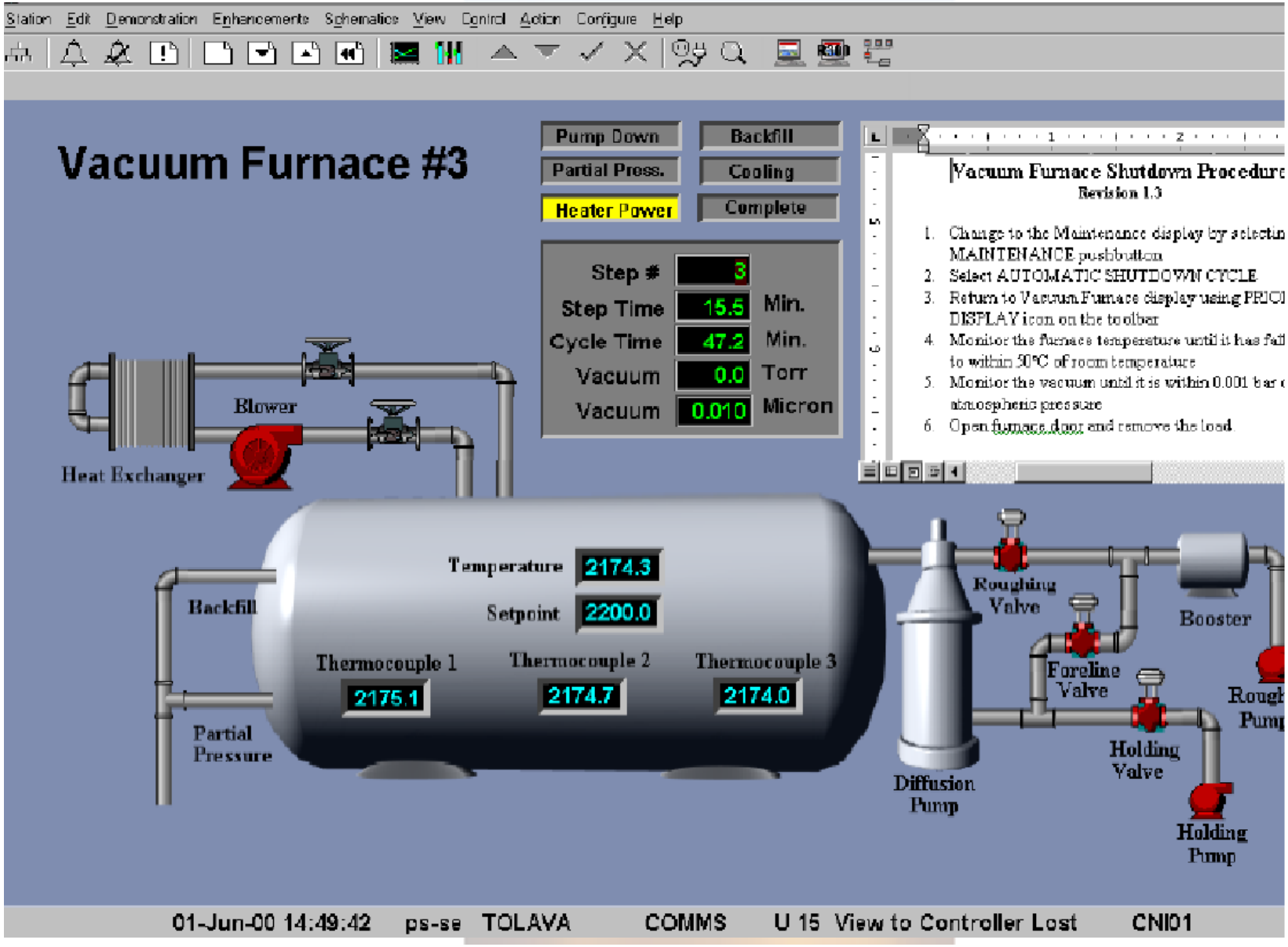
# Alarme do Processo

- 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



# Alarme do Processo



# Segurança no Projeto da Planta (BPCS)

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

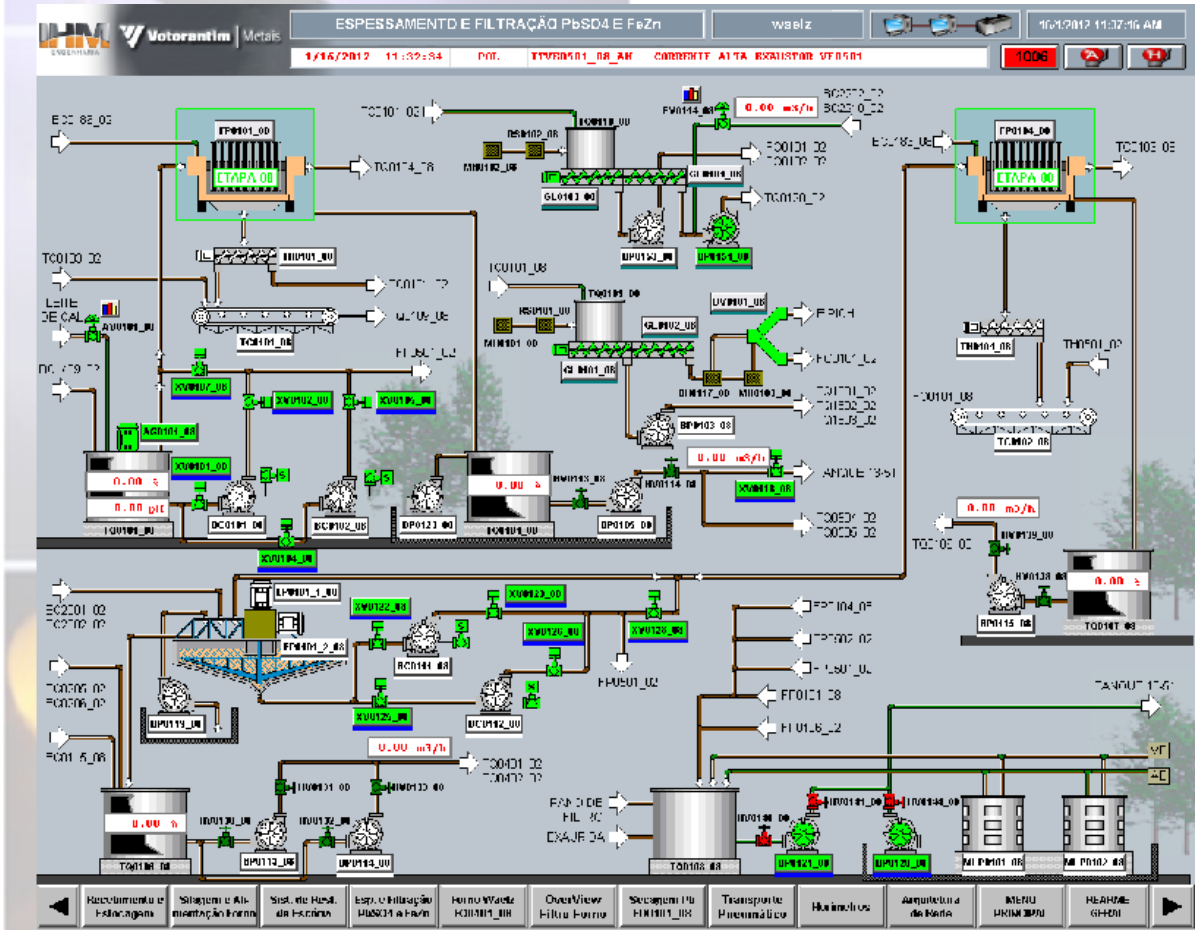
Pode-se perceber quatro níveis distintos de atividade da planta:

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

# Intertravamentos

- CLP
- Supervisório

->Bomba não liga se válvula de recalque não estiver aberta;
-> Válvula de sucção não abre se nível do tanque estiver em nível baixo;
->Bomba de enchimento não liga se nível do tanque estiver alto.
->Agitador não liga se nível do tanque estiver baixo;
-> Etc.



# Safe CLP

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.

# Safe CLP

## 1756 GuardLogix Integrated Safety System

GuardLogix® Integrated Safety Systems provide the benefits of standard ControlLogix® systems, plus safety features that support SIL 3 safety applications. GuardLogix safety controllers offer integrated safety, discrete, motion, drive and process control, as well as seamless connectivity to plant-wide information systems, all in the same controller. Use EtherNet/IP™ or ControlNet™ networks for safety interlocking between GuardLogix controllers. Connect field devices over EtherNet/IP or DeviceNet™ networks.

## 1756 GuardLogix Safety Controllers

Bulletin 1756 GuardLogix® Safety Controllers have a two-processor architecture (1oo2) and are suitable for SIL 3 PLe applications. As part of the Rockwell Automation® Integrated Architecture™ system, these controllers use RSLogix™ 5000 programming software, offer common information capabilities, and support CIP Safety over EtherNet/IP™ and ControlNet™ networks. These high-performance controllers provide a common control engine with a common development environment for all control disciplines. Consider these controllers for more sophisticated machines and for connectivity to business systems.

# Safe CLP

- Os CLPs de segurança são empregados em sistema de:
  - shutdown do processos químicos (plataformas de petróleo)
  - sistemas de fogo e gás,
  - bombeamento de petróleo, ou produtos químicos tóxicos.
  - 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.