DuPont's Approach of Safety Instrumented Functions - Bypassing

Hans van Dongen
January 25, 2018

Content

About

Introduction

- Standards
- Process Technology Review for SIS
- Current topics

Safety Interlock Bypassing

End

About the Presenter

- Hans van Dongen – EMEA Safety Interlock and Alarm Management Consultant
- Over 30 years with DuPont
- E&I Engineer several Dordrecht SBU's
- Special assignment SAP Release update PS module
- Instructor for PSM training
  - Safety Interlock-
  - PFD calculator
  - Alarm Management
  - Functional Safety Assessment
- Development team for S27A Interlock Bypassing and Alarm Suppression

Safety number 1

DuPont was established more than 200 years ago starting a gunpowder facility at the Brandywine river in Wilmington DE

During the last 2 centuries experiences with hazardous chemicals

Anno 2011 globally more than 150 sites with higher hazard processes

Safety is a core value.

Process Safety Standards

S21A Process Safety Management

- Procedures to control the hazards associated with chemical processing
- Protect personnel from serious injuries, prevent environmental harm, property damage and business losses
- Complex because it crosses over many functional areas.
- Integrated systematic approach to implement process safety elements.

S24A Process technology

- Identifying, documenting and managing the process technology element of process safety management.
- Mandatory requirements and advisory guidance apply to Higher Hazardous Processes and Lower Hazard Operations.

S25A Process Hazards Analysis

- Mandatory requirements and advisory guidance for the conduct of process hazards analyses
- Used to identify, evaluate and develop methods to control significant hazards associated with the hazardous processes and operations.
- Conducted on new and existing facilities.

Functional Safety Standards

DX_S Interlock Design / Safety Integrated function

- Methods for selecting appropriate interlock implementation.
- Design criteria for interlocks identified or recommended by the PHA teams to prevent undesired hazardous events.
- Consistent with requirements in ANSI/ISA s84.00.01-1996 (adopted by OSHA as a **R**ecognized **A**nd **G**enerally **A**ccepted **G**ood **E**ngineering **P**ractice)
- Based on Approved Independent Backup principle.

Other design standards

- Bypassing of safety interlocks
- Requirements for periodic testing and inspection of Safety Interlock systems
- Human Machine interface in Safety Interlock Systems
- Field devices in Safety Interlock Systems

Approach to functional safety

- Initiative led by a corporate team comprised of experts for functional safety as well as PSM (Process Safety Management)
- Site leads for functional safety responsible
- Regional experts support
- Process technology review for all safety interlocks
- PFD calculation
- Detailed evaluation during cyclic PHA's – Gap analysis.
- Site PHA resources responsible

Process Technology review for SIS

- DuPont has recognized ANSI/ISA 84.00.01 (IEC61511) as RAGAGEP, through our own clarifying SIS standards.
- Effective January 1, 2008 an analysis of the existing process technology design basis of Safety Instrumented Systems shall be conducted and documented according to current RAGAGEP.
- Finalized January 1, 2011.
- Questionnaire to analyze the gaps of process technology

Process Technology review for SIS

Basic questions e.g.:

- Is the SIS logic solver separated from the BPCS logic solver.
- Watchdog function to monitor communication between SIS logic solver and HMI
- If logic solver not according IEC 61508, have proven in use requirements been met?
- Is HMI designed that operator cannot make changes or forces in SIS.

Questions for each safety interlock.

- Are requirements documented?
- Is documentation of each Safety interlock current and complete?
- Have PFD calculations been made for each interlock?
- Is component redundancy included in SIL 3 designs?
- If online test methods are used, have interlocks been designed to safely perform these tests?
- Location of solenoid valve on control valve correct

SIS evaluation in PHA

- Event classification – required SIL
- Use of conservative AIB method (consequence based) or LOPA
- Gap analysis of current technology and requirements
- No use of risk graph/matrix
- Upgrades of SIS if needed

Current topics

- Update DX_S Standards regarding IEC 61511 Ed.2
- Expanded SIS bypass standard to include general, machine interlocks and suppression of alarms.
- Adopt of WIB / Namur Batch into a Best practice
- Expand FSA
- Cyber security

Content

About

Introduction

- Standards
- Process Technology Review for SIS
- Current topics

Safety Interlock Bypassing

End

Bypassing of Safety Interlocks

One of the High Risk activities.

Requires

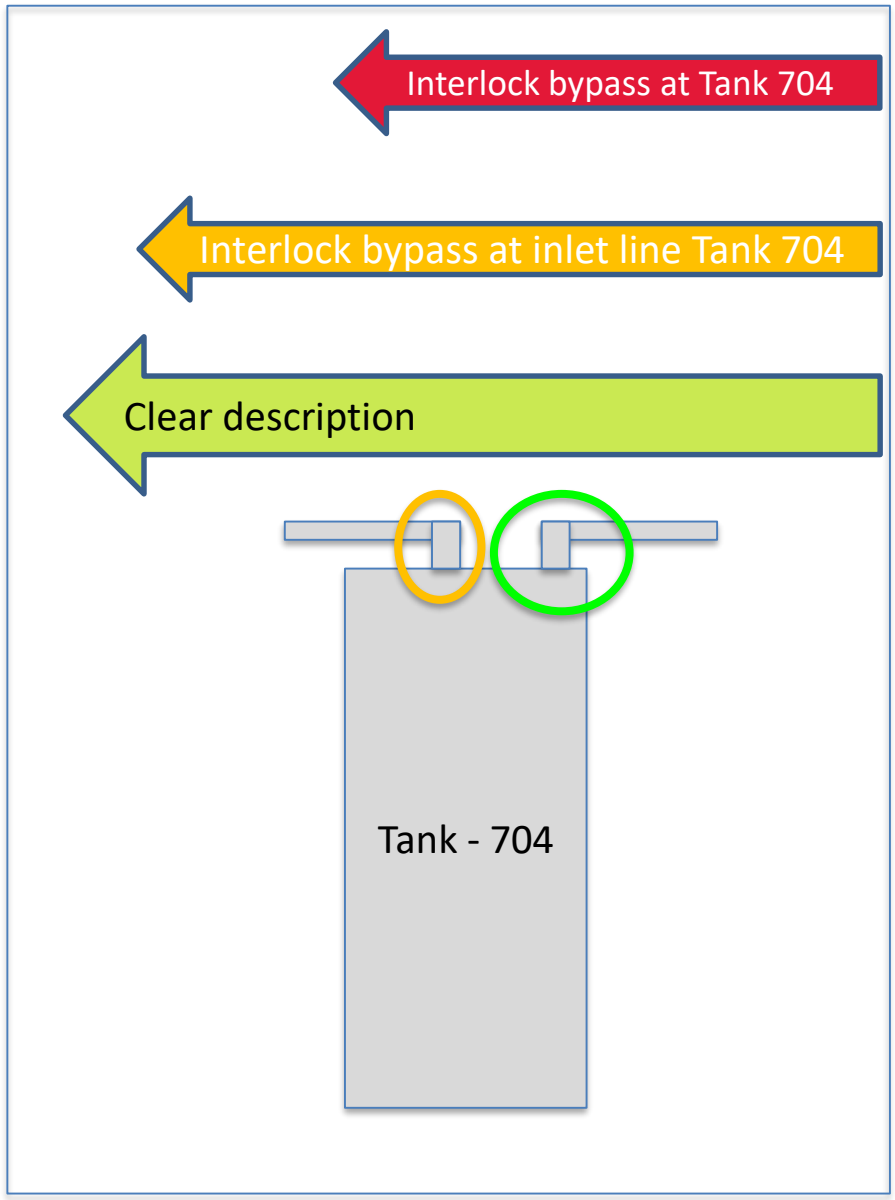
- Preparation
- Involvement Control / Safety Interlock Specialist
- Hazard Identification
- Alternates
- Documentation
- Qualified personnel
- Protection
- Permits
- Extension of permits
- Bypass checklist

Safety Contact

Formosa Incident

1.1. Formal request for interlock by-pass
(not part of existing process technology)

- Exact Location
- Equipment and/or process description
- Date of request
- Interlock description
- SIL classification
- Reason for by-pass
- Proposed by-pass period
- Proposed alternative and action limit



1.2.Consult Control Specialist

- Process Design Base

Interlock functionality description

1. Sensor
2. Logic solver
3. Final element

SIL classification 1 / 2 / 3

Operator alert on LOPA alarm (Layer Of Protection Analysis)

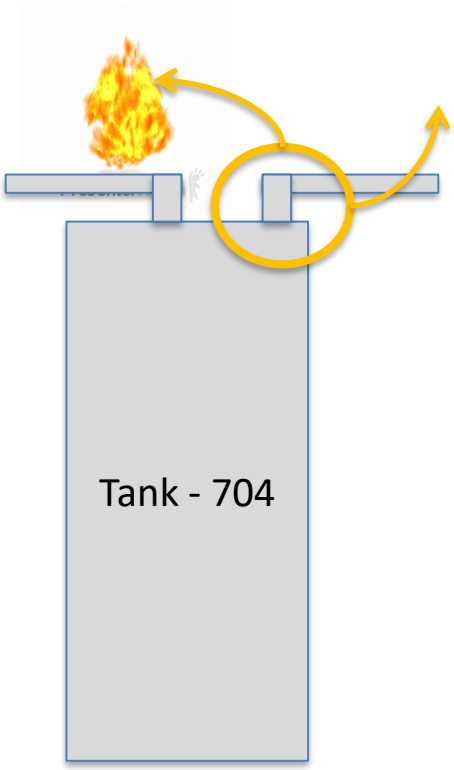
Machine interlock

Process interlock

1.3. Identify & evaluate all interlock by-pass related hazards

- Impact on:
  - Safety, Health, Environment,
  - Facilities
  - Quality
  - Business

- Consult- or perfom additional Risk Analysis / PHA
  - Avoid consequence threshold



What will the impact of not conducting the bypass?

- Evaluation between risk and the cost of e.g. 1 day downtime.
- Think about only one hour downtime... this should encourage people to consider not to place / make a bypass. Eventually adapt the process conditions.

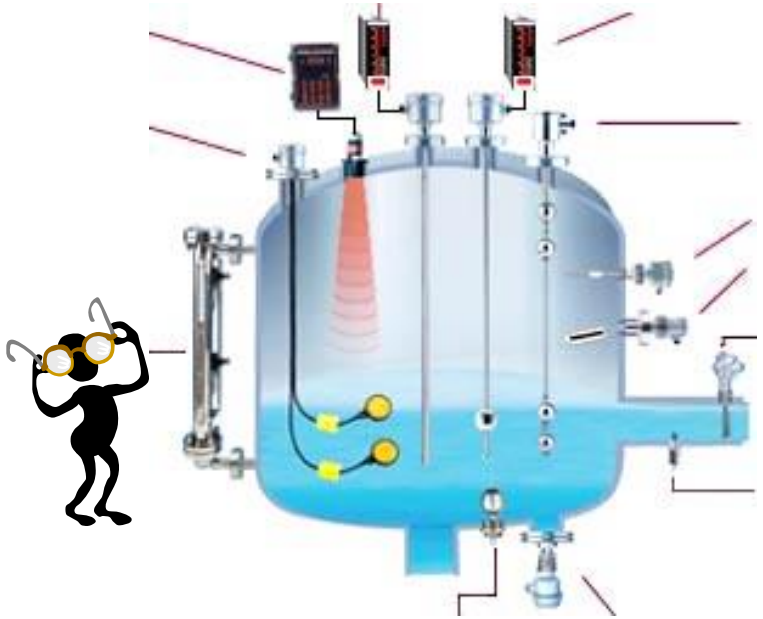
€ $ £

*1.4. Define alternate protective function **

- Can be based on manual or automated actions

- If Manual:
  - Appropriate back-up measurement
  - Define approved limits
  - Qualified and dedicated person to monitor and take action if required

- Examples of alternate manual function:
  - Operator reading local tank gauge on timely base.

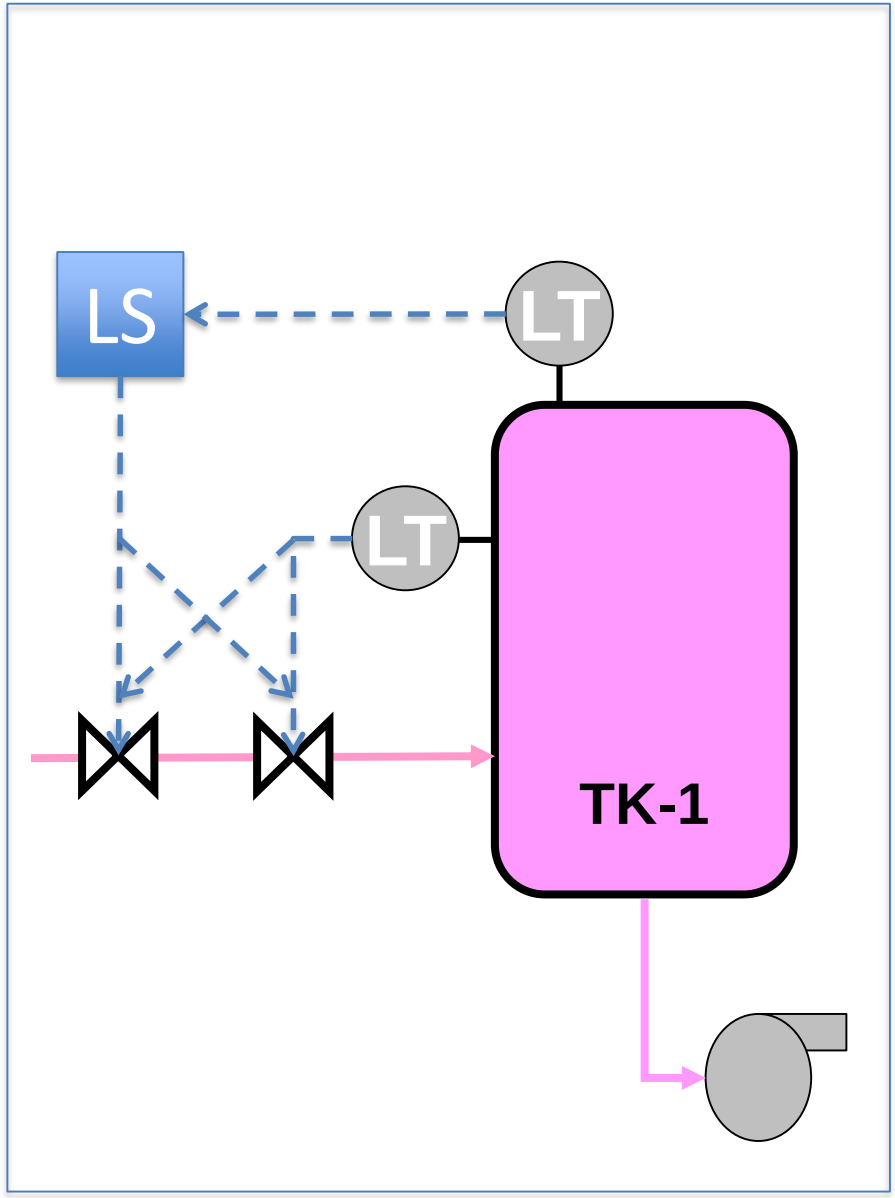


*1.4. Define alternate protective function **

- Can be based on manual or automated actions

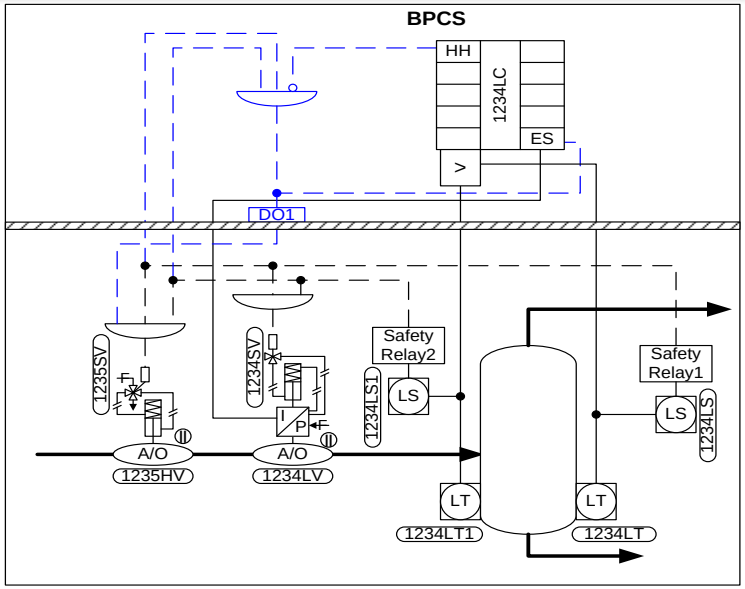
- If automated:
  - Appropriate back-up measurement
  - Define approved limits
  - Alternate to achieve safe state of final element.

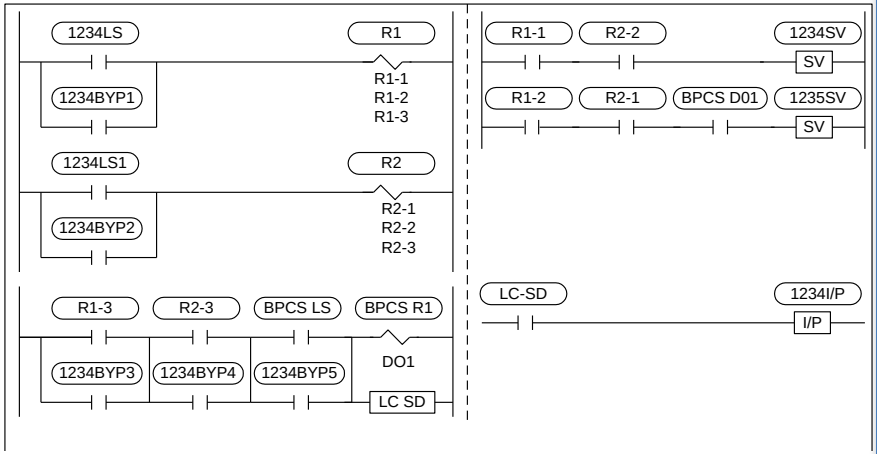
- Examples of alternate automated functions:
  - Redundant interlock.
  - Alternative process value.
    - Correlation Pressure / Temp



1.5. Establish and verify technical proposal is prepared

- *P&ID*
- *Schematics*
- *Logic*
- *Matrix diagrams*
- *If needed : develop technical description to provide additional essential information.*

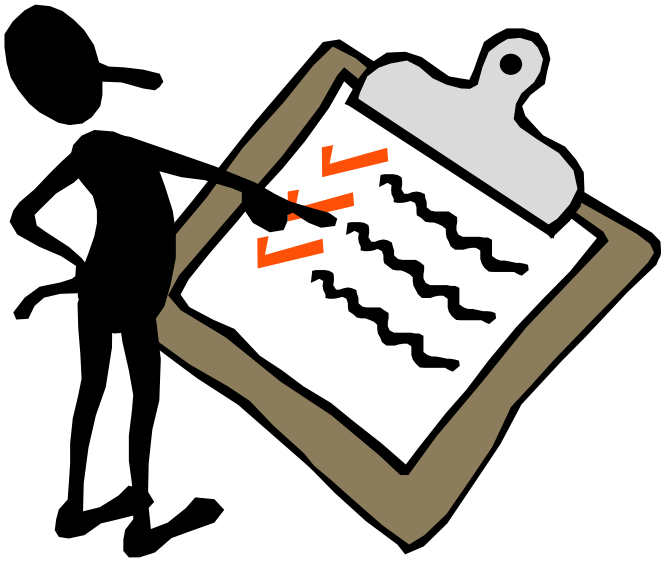




1.6. Complete and document all relevant aspects

Bypass permit best practice:

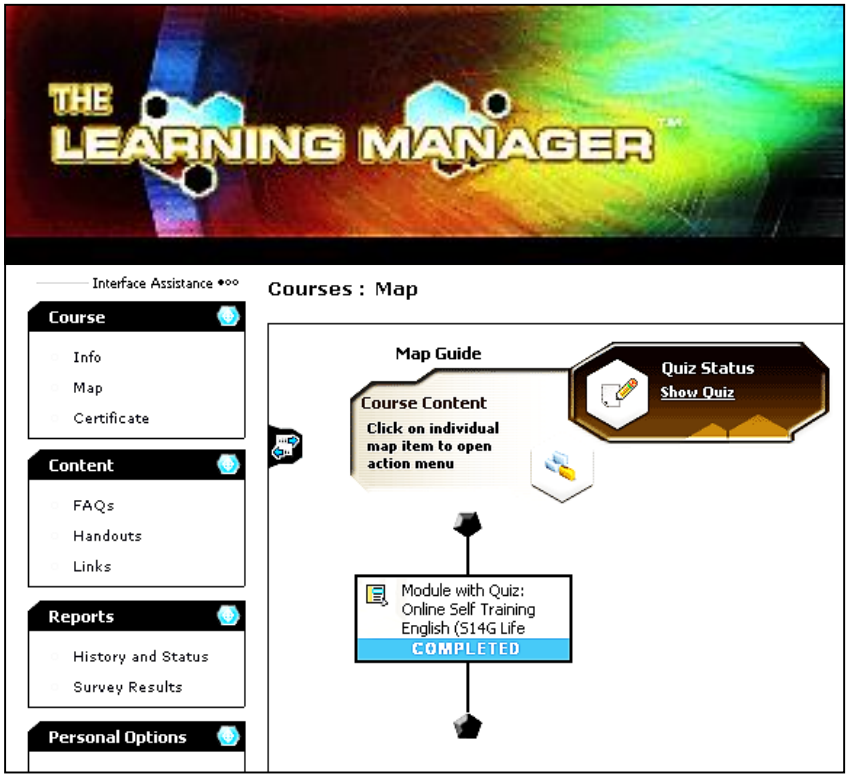
- Unique number
- Date of request
- Duration
- By-pass period
- Exact Location
- Equipment and/or process description
- SIL classification
- Reason for by-pass
- Alternative and action limit
- By-pass installed / removed by: ....
- Approval by interlock guardian
- Authorization by line manager
- Additional authorization for extending duration by-pass permit at higher level



1.7. Ensure availability qualified personnel to perform the interlock bypass

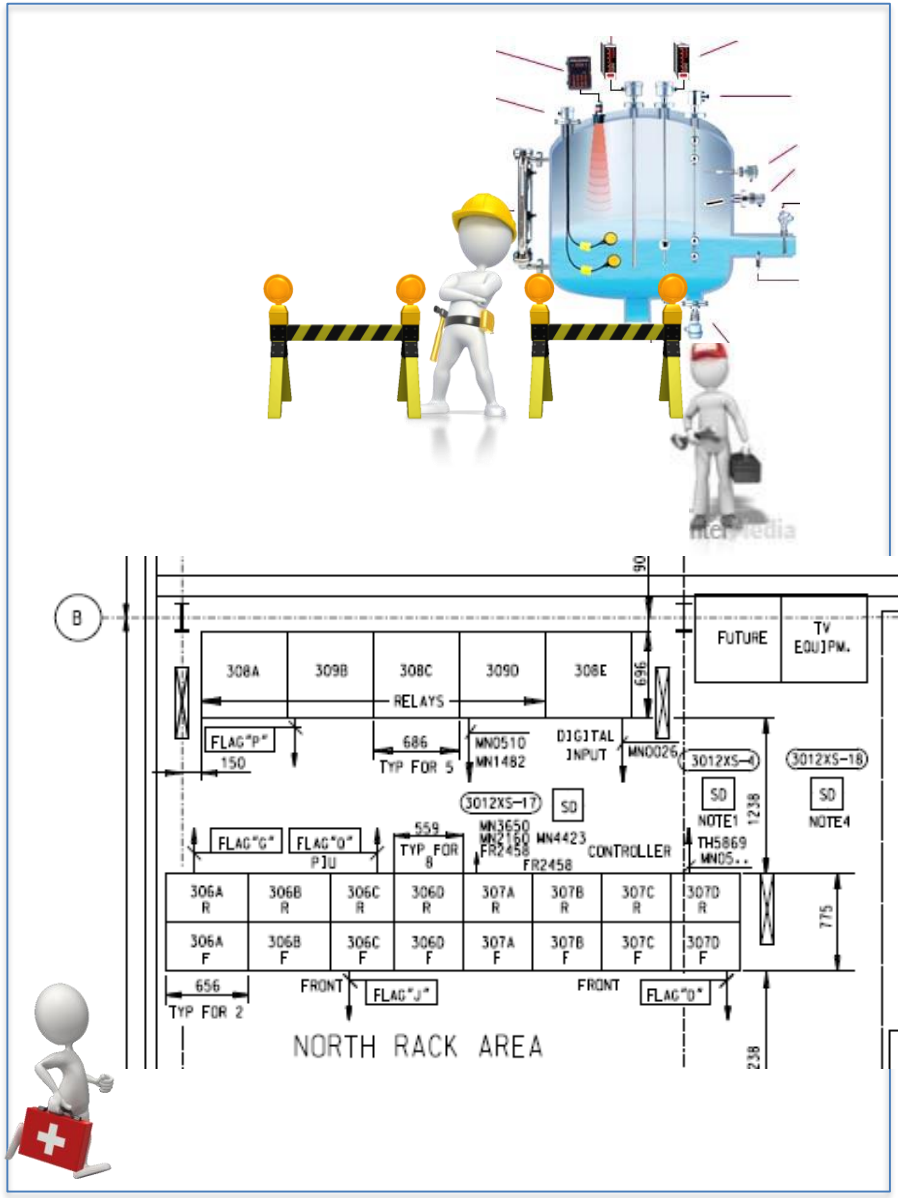
- All own employees shall be trained and qualified to the degree warranted by their job assignment (ref. training matrix)

- Documentation for each employee shall include:
  - Employee's name and job assignment
  - Date of training
  - Content of the training received
  - Name of the trainer
  - Method of verifying the employee's understanding of the training



2.1. Establish and Verify that the area / equipment is prepared as per risk analysis / job plan

- Identify Line of fire
- Area barricading (operations)
- Area barricading at location of bypass
- Access control
- Rescue ways / access & egress possible as per plan



2.2. Establish and Verify that the personnel is prepared as per risk analysis / job plan

- Personnel Protective Equipment:
  - release check (e.g. label / certificate)
- PPE correctly worn
- Communication

3.1.Job turnover and authorization and signing bypass permit by <u>all</u> involved

- Involved:

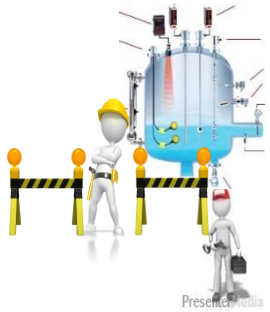
1.Proprietor / owner

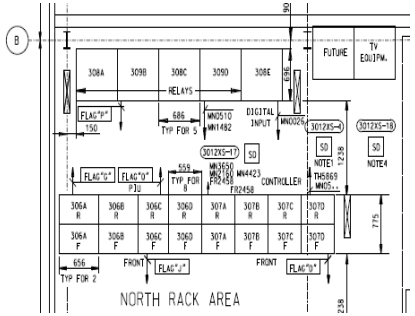
2.Operator direct related to by-passed equipment / process

3.Capable Person: installing and removing the by-pass

4.Capable Person: executing repair and / or testing activities

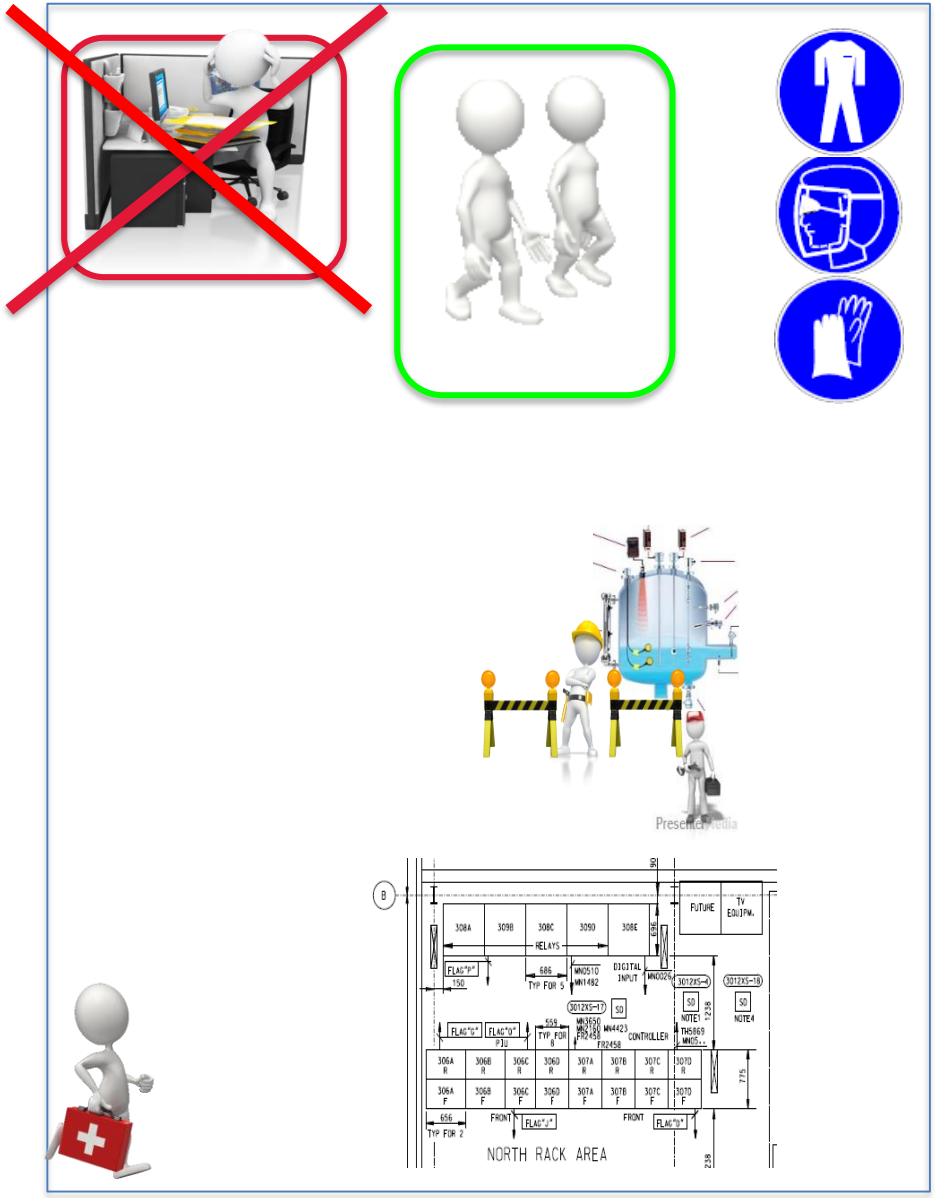
- In the field at the work location and at shift turn-over





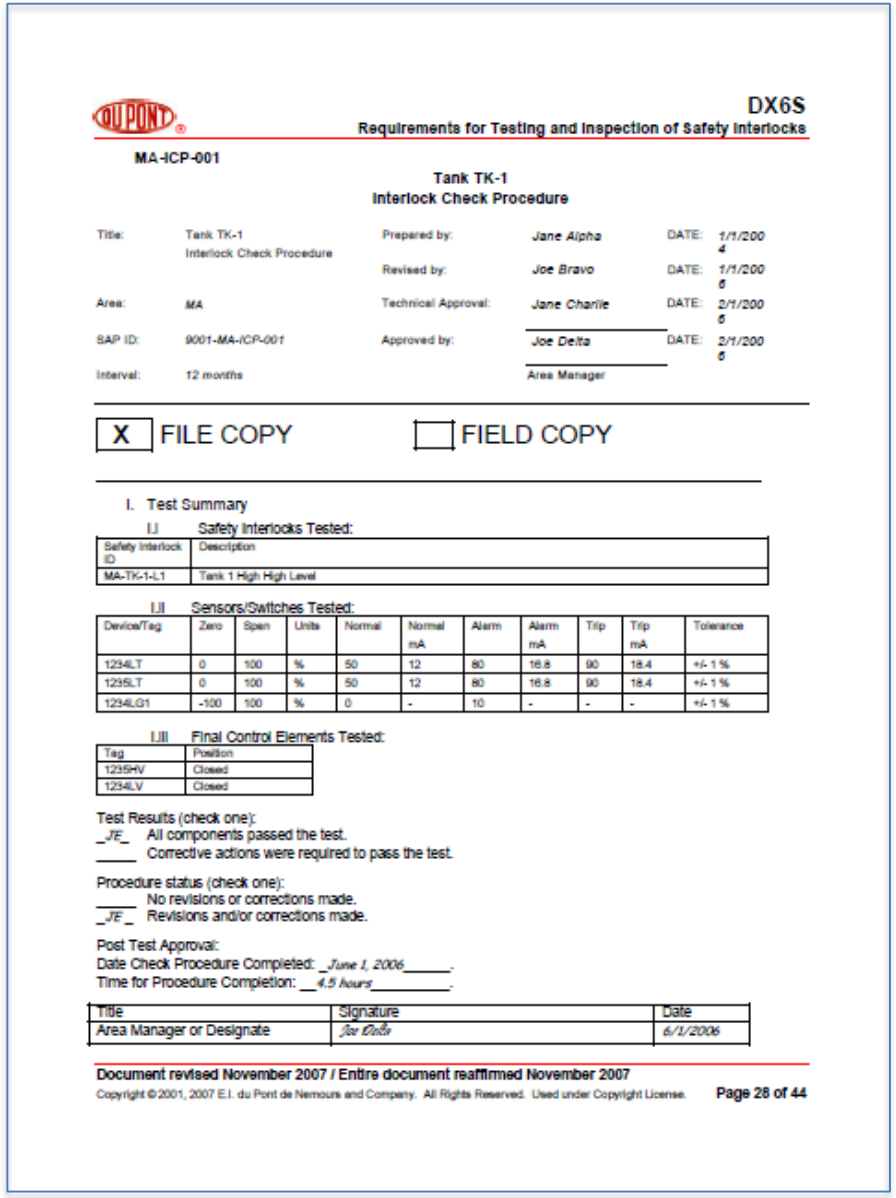
3.1.Job turnover and authorization and signing bypass permit by <u>all</u> involved

- Communication of:
  - •<u>Hazards</u>
  - •Alternate protective function
  - •Rescue methods
  - •Job plan / task execution
- All personnel performing the work sign for understanding and acceptance via Bypass Permit
- Additional permits may apply



3.2. Perform the bypass as per approved plan

- According to the planning / instructions
  - Bypass permit(s)
- Best practices:
  - Use of red- or labeled wire.
  - Put permit on the door of cabinet, or somewhere else on the spot.
  - Information board in Control Room.



DX6S

Requirements for Testing and Inspection of Safety Interlocks

MA-ICP-001

Tank TK-1
Interlock Check Procedure

Title:	Tank TK-1 Interlock Check Procedure	Prepared by:	*Jane Alpha*	DATE:	*1/1/2004*
		Revised by:	*Joe Bravo*	DATE:	*1/1/2006*
Area:	*MA*	Technical Approval:	*Jane Charlie*	DATE:	*2/1/2006*
SAP ID:	*9001-MA-ICP-001*	Approved by:	*Joe Delta* Area Manager	DATE:	*2/1/2006*
Interval:	*12 months*				

[X] FILE COPY [ ] FIELD COPY

I. Test Summary

I.I Safety Interlocks Tested:

Safety Interlock ID	Description
MA-TK-1-L1	Tank 1 High High Level

I.II Sensors/Switches Tested:

Device/Tag	Zero	Span	Units	Normal	Normal mA	Alarm	Alarm mA	Trip	Trip mA	Tolerance
1234LT	0	100	%	50	12	80	16.8	90	18.4	+/- 1 %
1235LT	0	100	%	50	12	80	16.8	90	18.4	+/- 1 %
1234LG1	-100	100	%	0	-	10	-	-	-	+/- 1 %

I.III Final Control Elements Tested:

Tag	Position
1235HV	Closed
1234LV	Closed

Test Results (check one):
_*JE*_ All components passed the test.
_____ Corrective actions were required to pass the test.

Procedure status (check one):
_____ No revisions or corrections made.
_*JE*_ Revisions and/or corrections made.

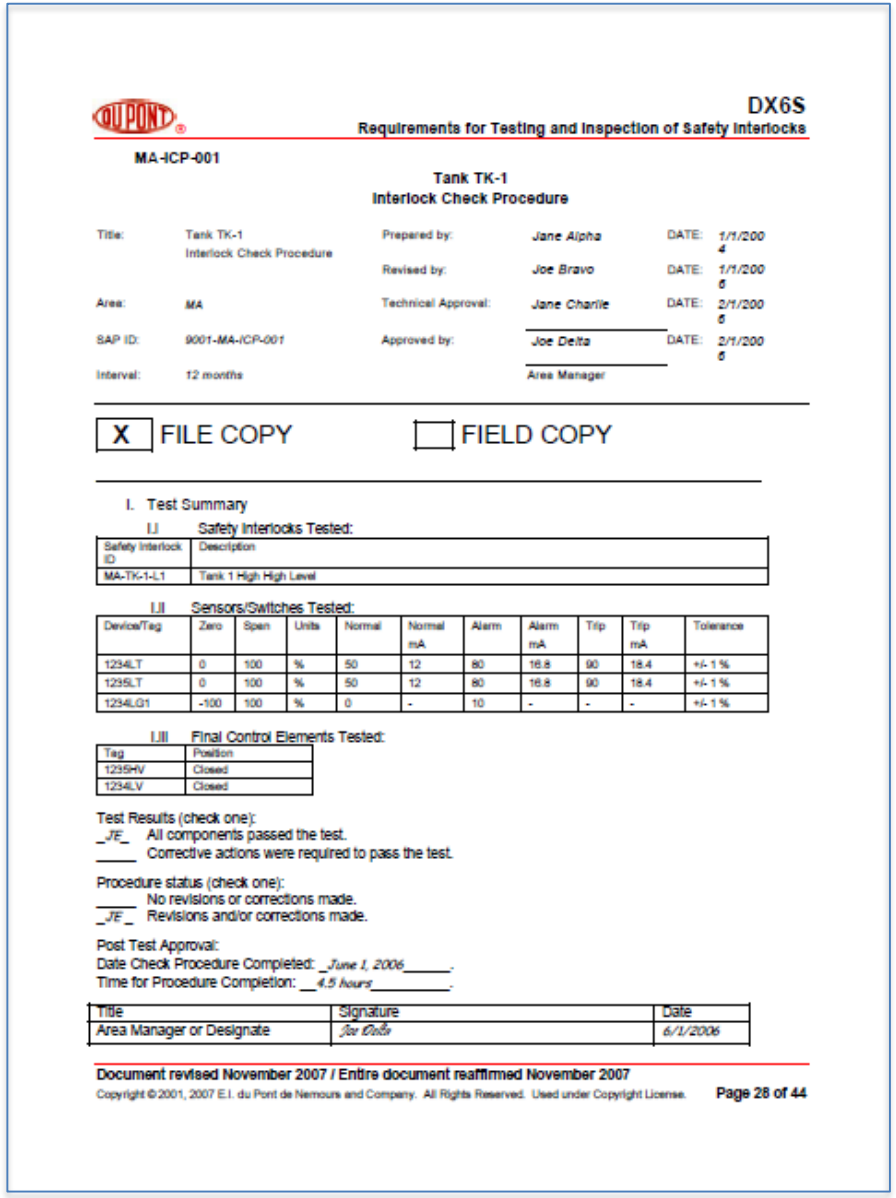
Post Test Approval:
Date Check Procedure Completed: _*June 1, 2006*_____.
Time for Procedure Completion: __*4.5 hours*_____.

Title	Signature	Date
Area Manager or Designate	*Joe Delta*	*6/1/2006*

Document revised November 2007 / Entire document reaffirmed November 2007

3.3. Process or equipment running with active bypass

- Continued operation
- Testing of redundant interlock channels.
  - As per approved test procedure
- Instrument calibration by-pass



DX6S

Requirements for Testing and Inspection of Safety Interlocks

MA-ICP-001

Tank TK-1
Interlock Check Procedure

Title:	Tank TK-1 Interlock Check Procedure	Prepared by:	*Jane Alpha*	DATE:	*1/1/2004*
		Revised by:	*Joe Bravo*	DATE:	*1/1/2006*
Area:	*MA*	Technical Approval:	*Jane Charlie*	DATE:	*2/1/2006*
SAP ID:	*9001-MA-ICP-001*	Approved by:	*Joe Delta*	DATE:	*2/1/2006*
Interval:	*12 months*		Area Manager		

[X] FILE COPY [ ] FIELD COPY

I. Test Summary

I.I Safety Interlocks Tested:

Safety Interlock ID	Description
MA-TK-1-L1	Tank 1 High High Level

I.II Sensors/Switches Tested:

Device/Tag	Zero	Span	Units	Normal	Normal mA	Alarm	Alarm mA	Trip	Trip mA	Tolerance
1234LT	0	100	%	50	12	80	16.8	90	18.4	+/- 1 %
1235LT	0	100	%	50	12	80	16.8	90	18.4	+/- 1 %
1234LG1	-100	100	%	0	-	10	-	-	-	+/- 1 %

I.III Final Control Elements Tested:

Tag	Position
1235HV	Closed
1234LV	Closed

Test Results (check one):
_*JE*_ All components passed the test.
_____ Corrective actions were required to pass the test.

Procedure status (check one):
_____ No revisions or corrections made.
_*JE*_ Revisions and/or corrections made.

Post Test Approval:
Date Check Procedure Completed: _*June 1, 2006*_____.
Time for Procedure Completion: __*4.5 hours*_____.

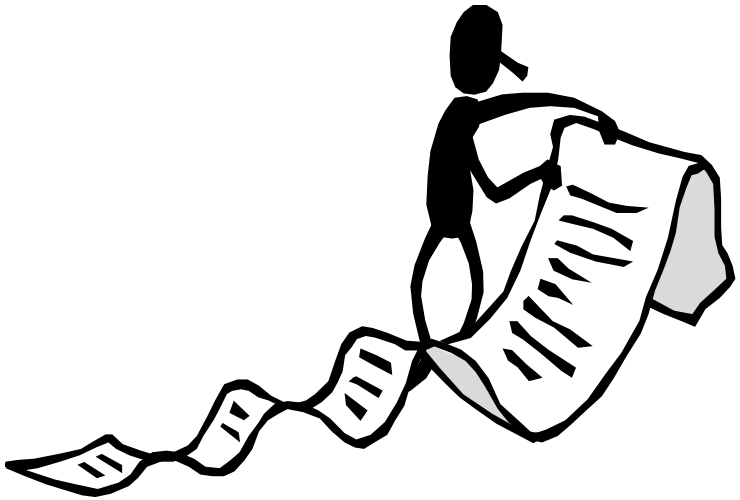
Title	Signature	Date
Area Manager or Designate	*Joe Delta*	*6/1/2006*

Document revised November 2007 / Entire document reaffirmed November 2007

4.1. Extend bypass approval

- Special attention for Safety interlocks
- Limited to 10x 24h
- By-pass permit shall be limited to 24 h duration withy a maximum of 10 re-authorizations

  •Unless authorized by plant manger or documented by Management of Change



4.2. Remove bypass , document and return to Standard Operating Conditions

- Who ?:

1) Capable Person: executing repair and / or testing activities
   - Testing is not always possible.
   - 4 eye principle can help to create a higher level of confirmation that system is put back in original status.

   Capable Person: installing and removing the by-pass

   Operator direct related to by-passed equipment / process

4) Proprietor / owner

- Documentation include
  - Date / Name
  - By-pass checklist
- Sign off permit

By-Pass checklist

Loop nr	By-pass installed by:	Date	By-pass descirption	By-pass removed by:	Date

Summary: Bypassing of Safety Interlocks

Requires

- Knowledge of the Hazards
- Alternates as good as the safety interlock
- Documentation
- Qualified personnel
- Permits
- Limited time
- Bypass checklist

Thank You!

The miracles of science™