



Setting the Standard for Automation™

Garcia-Cammack-Sanchez

Permissive sequencing and the ISA 84

Standards
Certification
Education & Training
Publishing
Conferences & Exhibits

Co-Presenter/Author



Gene Cammack, P.E

- Currently holds the position of Automation Consultant, Oil & Gas Americas, for Siemens Energy and Automation. Responsible for development of Automation Strategy for Oil & Gas industry in the Americas, including development of relevant applications, project pursuit, industry strategies and tailoring new product enhancements for the industry.
- Previously; Gene held the positions of Technical service Manager, Office Manager and Regional manager for Moore Products Company, in Beaumont and Houston, Texas
- With more than thirty years experience in automation and control, Gene has worked in Power Plants and Refineries in Port Arthur, Amarillo and Houston
- BS – Nuclear Engineering, Texas A&M University in 1977 Gene is a Licensed Professional Engineer , a Sr. Member Instrument, Systems and Automation Society (ISA) and a member of Texas A&M Instrumentation Symposium Advisory Committee
- Gene resides with his wife in the Houston area

SIEMENS

Francisco Sanchez

- Currently holds the position of Project Leader in Automation, Instrumentation and Process Safety in PDVSA. Responsible for conceptualizing, design, directing and supervising the implementation of projects for final investors in the area of automation, instrumentation and safety processes which contribute to improve and optimize production while increasing safety in order to protect personnel, facilities and the community of the Puerto La Cruz Refinery in Venezuela.
- BS - Electrical Engineering, Central University of Venezuela UCV, 1997; Francisco is a Functional Safety Engineer for Safety Instruments Systems with ID: 564/07 FS Engineer by TUV Rheinland
- Francisco has been working extensively in the oil and gas, refinery sector for 14 years in Venezuela. As charter engineer, Francisco has join his company safety team in charge of design and development of instrumentation, automation and safety project for PDVSA Venezuela.
- Francisco was born in Venezuela is married to Rosa and has three children, Daniela, Santiago y Diego they currently reside in Puerto La Cruz Venezuela.



Co-Presenter/Author



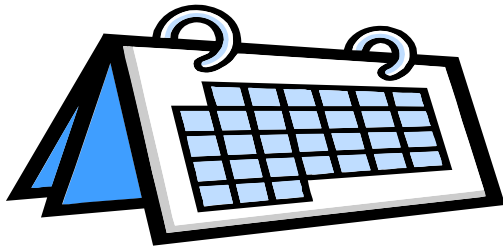
Luis M. Garcia

- Currently holds the position of Business Consultant for Latin America for Siemens Energy and Automation as a Certified Functional Safety Expert by the CFSE Governing Board and as member of the Global Process Safety Group.
- Has been working extensively in the Oil and Gas, Chemical and Petrochemical sector for 27 years helping to develop standards, procedures and projects all around Latin America and Europe.
- Charter Engineer, Luis has participated in the design and development of instruments for Safety Related applications, such as Solenoid Valves since 1989.
- Honors graduated from Liverpool University (1981) as a Metallurgist and Material Scientist, and holds a Mechanical degree from Saint Joseph Technical College from Rosario, Argentina, obtained in 1972.
- Has several white papers, seminars and workshops presented at ISA Mexico, Venezuela, Brazil and other international events in Argentina, Chile, Colombia, Peru, Spain and Great Britain.
- Born in Venezuela, is married to Kathryn and has three Children. They currently reside in the Houston area.

SIEMENS

A blue, curved graphic element resembling a stylized 'S' or a swoosh, located in the bottom right corner of the slide.

Agenda



- 1. Introduction and Justification**
 - 1. Assumptions for suspension of SIS**
 - 2. Assumptions Challenge**
- 2. Permissive sequencing – Cause and Effect Diagrams**
 - 1. Requirements**
 - 2. Tools for Static Logic**
 - 3. Requirements for Dynamic Logic**
- 3. Example of Dynamic Documentation**
- 4. Conclusions and Recommendations**

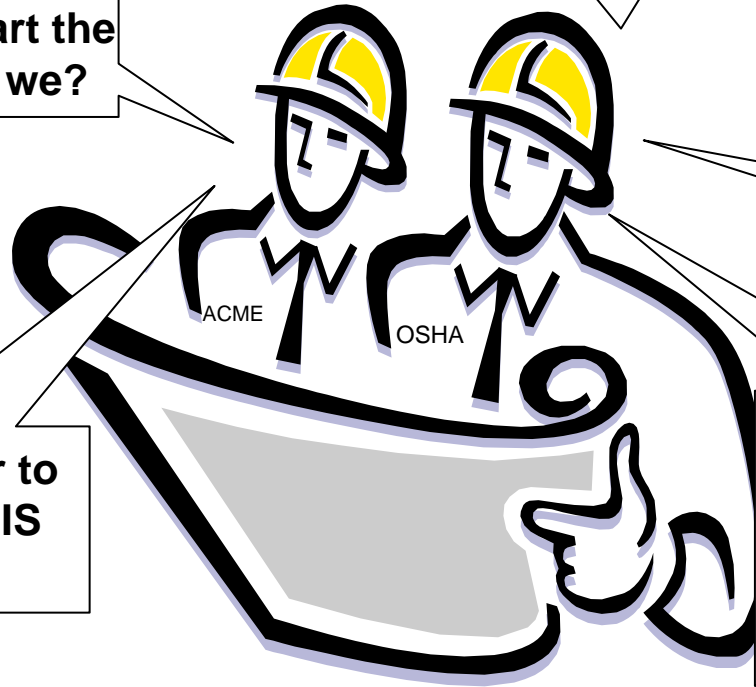
Introduction and Justification



This is what happens ...

I see you comply with Osha 1910.119. You had successfully applied IEC 61511 Mod. Or ANSI/ISA 84.00.01 – 2004. I'm very impressed!

Then we can start the UNIT up, can't we?



ABSOLUTELY!

Then I will order to "bypass" the SIS immediately

Of course! Just follow the guidance provided by the Operation Manual!

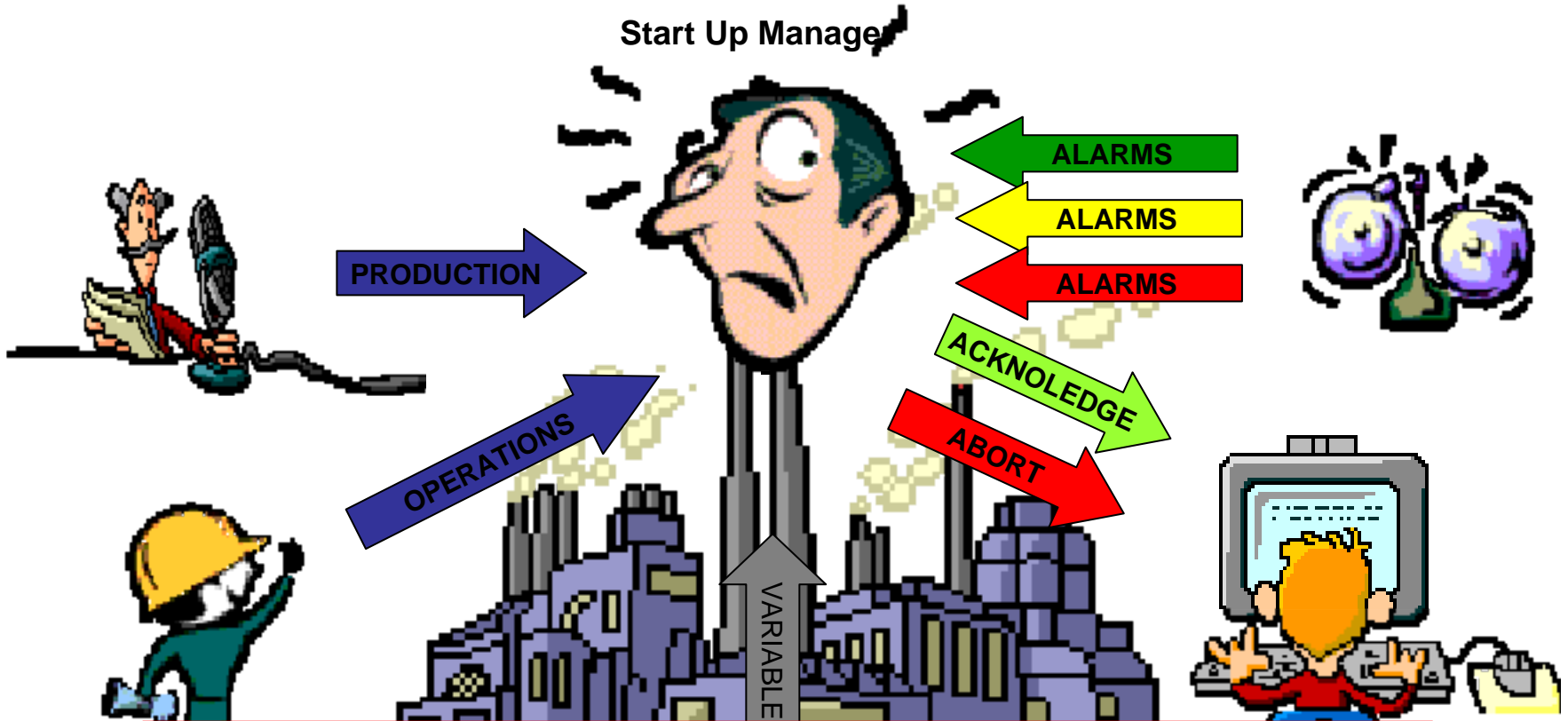
... but is this safe?

Introduction and Justification



All that meant ... Replace the SIS by the operator Criteria...

Start Up Manager



Is this what we would REALLY recommend?



Introduction and Justification



What about the numbers?



For the benefit of this argument, let's consider the unproven fact that only 1% of the total number of accidents occurred were due to startup operations, transition operations or "controlled" shut down operations (a very conservative figure)

In other words. let's accept that only 1 out of 100 accidents occurred during startup operations, transition operations or "controlled" shut down .

Introduction and Justification



What about the numbers?

On average, it is safe to say that on average, a unit operates uninterrupted or without a major overhaul for at least five years

That is; $5 \times 8760 \text{ Hours} = 43.800 \text{ Hours steady state}$

On the other hand a unit takes an average of two days to startup

That is; $2 \times 24 \text{ Hours} = 48 \text{ Hours unstable state}$

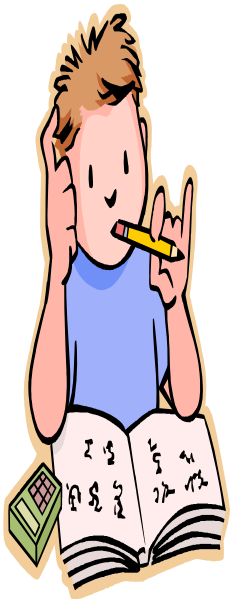
Then, 99 units had an accident rate of;

$99 \text{ accidents} / 43.800 \text{ hours} = 0,00023 \text{ accidents per hour}$

While the accidents rate during startup was;

$1 \text{ accident} / 48 \text{ hours} = 0,021 \text{ accidents per hour}$

A difference of two orders of Magnitude!

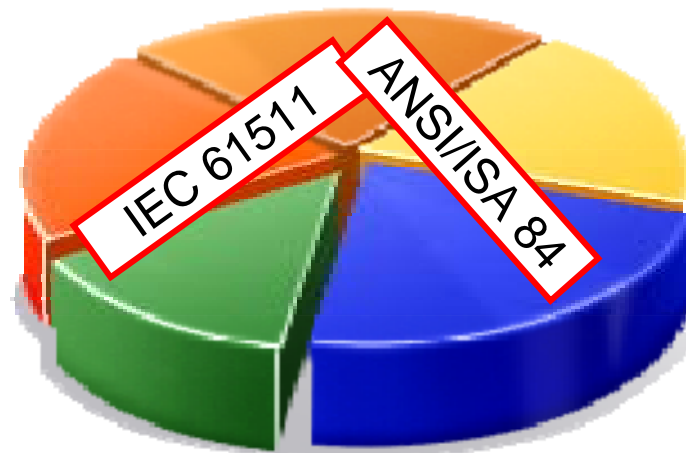


Introduction and Justification



What about the numbers?

While the accident rate in steady state operation has been dramatically decreased, thanks to standards ... From 10^{-3} to 10^{-5} Accidents/Year



Little has been done with accident rates while in unstable state, whether startup, shutdown or process transitions!

What are the assumptions for suspension of an SIS during Startups?

There are several justifications:



- 1. Processes transitions (i.e. start-ups), are not frequent and are of short duration compared to steady state operation.**
- 2. There is a lack of similarity between different processes. This makes prescriptive standards impossible and best practices difficult.**
- 3. There is a lack of similarity between the Process Transition operation and Steady State operation. SIS designers would have to create an entirely new and conflicting SIS to manage process transitions.**

What are the assumptions for suspension of an SIS during Startups?

There are several justifications:



- 4. The process transition operation is more affected by operational subjectivity and procedures than steady state operation, i.e. “How long an interlock should be bypassed?” Therefore automating process transitions require strong operations input in the development process.**
- 5. Because the transition is sequential and dynamic, timing of process steps and interlock changes are critical. These are difficult to validate and verify without both detailed operational knowledge and adequate (proper) simulation routines.**

Introduction and Justification



Assumptions Challenge

Let's analyze one at the time:

1. Processes transitions (i.e. start-ups), are not frequent and are of short duration compared to steady state operation.



- ❑ Transitions are the most volatile and dangerous moments
 - ❑ The BPCS generally is not designed for or to changing conditions
 - ❑ The operators are usually not trained for the use of unstable variables
 - ❑ Usage (in the field) is often not protected because of high demand rate
 - ❑ Human error is often considered a LOP for high demand (see later)
- ... (variable and auditable after the fact)

Note: Human Error (action or inaction) as defined by ANSI/ISA 84.00.01 (part 1) or IEC 61511-1 Mod. Definitions - 3.2.32 page 26 Note: ANSI/ISA 84.00.01 Part 2 or IEC 61511-2 Mod Offers guidance on how to include operator's availability and reliability calculations.

Play it by ear? At the most dangerous moment?

A Human IS NOT the same as a Safety PES. So, should we allow humans to substitute PES in SIF?



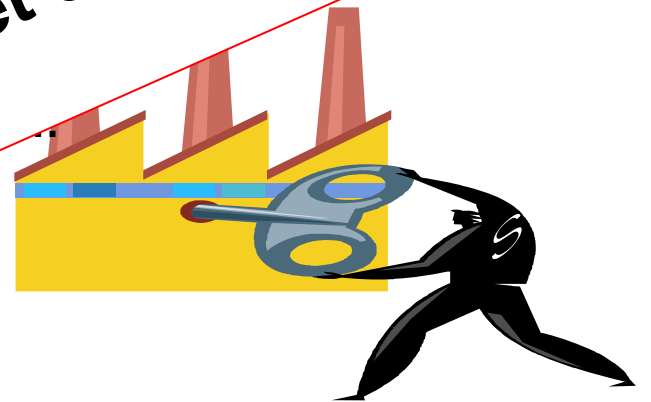
**In High demand mode?
REMEMBER! A PES SIL 1 in high demand mode
requires PFD = 10^{-5} to 10^{-6}**

Let's analyze one at the time:

- 2. There is a lack of similarity between processes. This makes prescribing impossible and best practice is to leave it to the operator.



Too difficult for the SIS, yet easy for the operator?



- ❑ This characteristic makes it difficult for a SIS during Startup.
- ❑ So because it is hard for the SIS, we leave it in the hands of an operator?
- ❑ Thanks to modern software, there are programming strategies that take care of this issue

Introduction and Justification



Assumptions Challenge

Let's analyze one at the time:



3. There is a lack of similarity between the Transition operation and Steady State operations. Designers would have to create new and conflicting SIS to manage these transitions.

- As before, this is a fallacy
- In a manual, operators cannot be tuned for changes and require continuous attention from already busy operators
- Spending time writing procedures in a manual that may or may not be used, same input could be used to write startup subroutines in the SIS. Automate the process
- Startup subroutines could be verified and validated like the rest of the Safety Instrumented Functions (SIF) in a SIS as required by current standards

If it can be documented in a Manual, it can definitely be programmed in an SIS!

Introduction and Justification

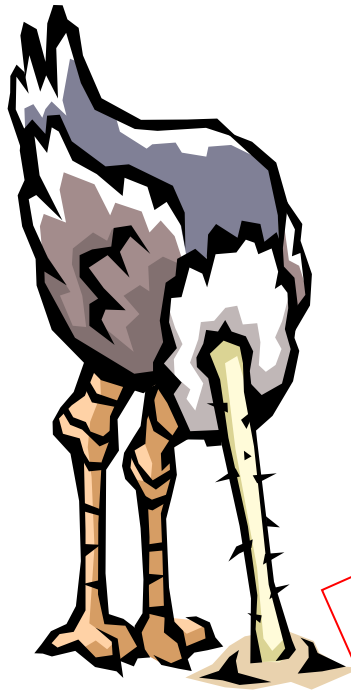


Assumptions Challenge

Let's analyze one at the time:

4. The process transition operation is more...
by operational subjectivity and pro...
steady state operation, i.e. "H...
should be bypassed?"...
process transition...
input in the... process.

□ He... "Safety" to have priority over "Safety"
... participation is required from an experienced operator to write
... procedure as to write up a program subroutine.
... proof of the above are BMS applications as per NFPA 85 and NFPA 86. In
such cases Startups are automatic for exactly the same reasons presented
here



Operators can only transfer knowledge under pressure or to write up a manual?

Introduction and Justification



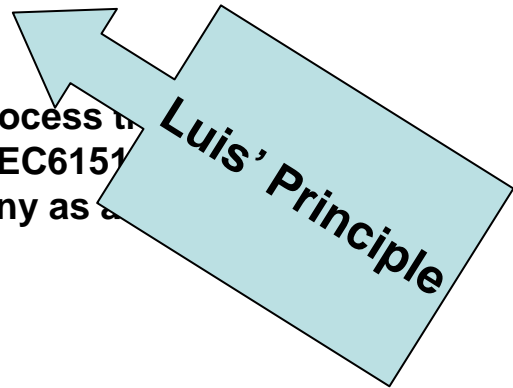
Assumptions Challenge

Let's analyze one at the time:

- 5. Because the transition is sequential of process steps and interlocks. These are difficult to validate without both detailed operation and adequate (proper) simulation.

- The startups and process to be validated following IEC61511-2004 in the same way any as

If it can be documented in a Manual, it can definitely be programmed in an SIS!



Introduction and Justification



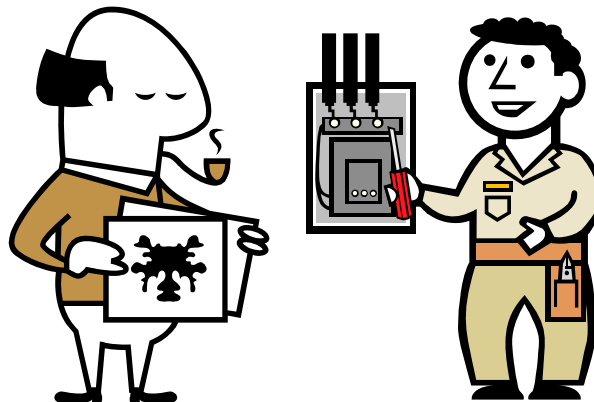
Summarizing

ANSI/ISA-84.00.01-2004 Part 3 (IEC 61511-3 Mod) Page 60



Table F.3 –Typical protection layer (prevention and mitigation) PFDs

| Protection layer | PFD |
|--|---|
| Control loop | $1,0 \times 10^{-1}$ |
| Human performance (trained, no stress) | $1,0 \times 10^{-2}$ to $1,0 \times 10^{-4}$ |
| Human performance (under stress) | 0,5 to 1,0 |
| Operator response to alarms | $1,0 \times 10^{-1}$ |
| Vessel pressure rating above maximum challenge from internal and external pressure sources | 10^{-4} or better, if vessel integrity is maintained (that is, corrosion is understood, inspections and maintenance is performed on schedule) |



Do we have a Psychologist in the committee?

Do we use Psychologists during start-up operations?

Permissive sequencing – Cause and Effect Diagrams

How much really can we expect to avoid the human uncertainty?

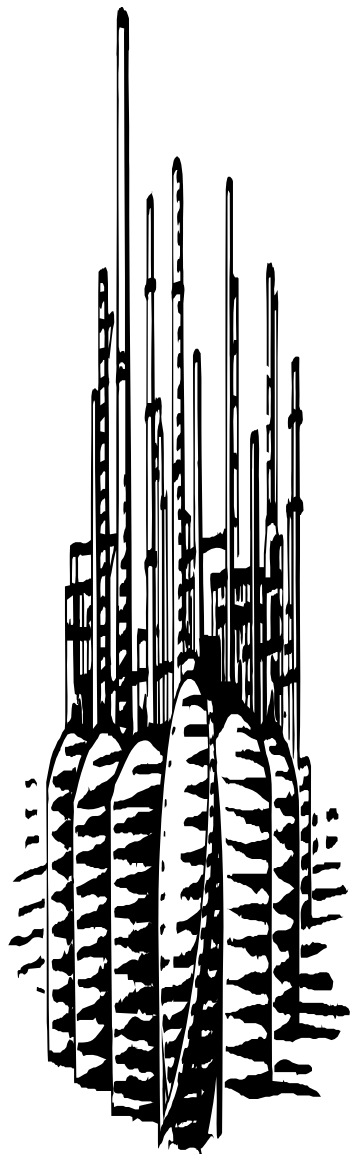
Easy answer: DO NOT rely on human intervention if you can help it!



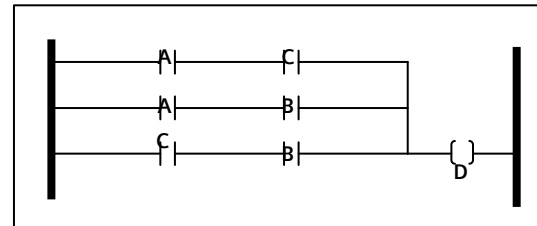
Luis' Principle

If it can be documented in a Manual, it can definitely be programmed in an SIS!

Permissive sequencing – Cause and Effect Diagrams



Requirements

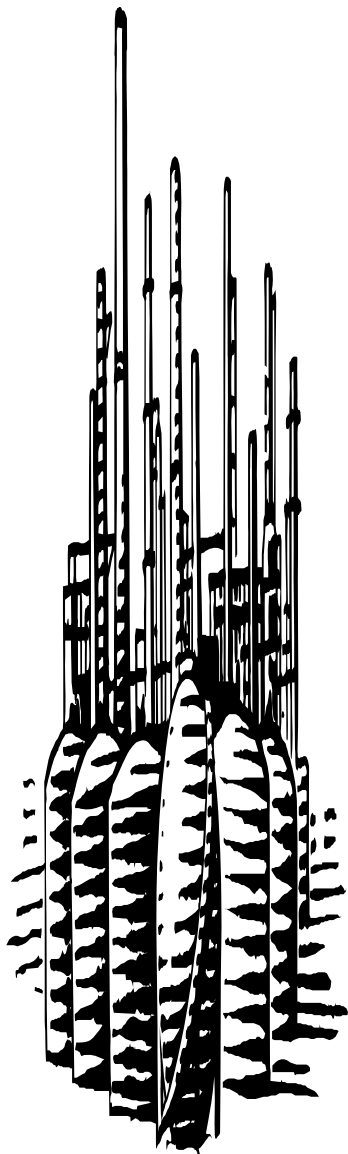


In order to define automatic permissive sequencing, there are two basic requirements:

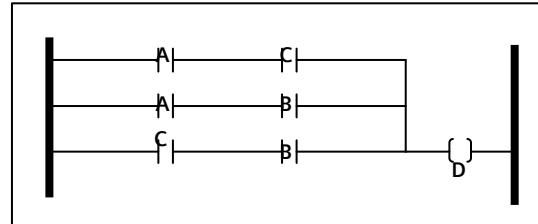
1. Deep knowledge of the process
2. A set of tools that would allow dynamic programming and documenting of the logic.

Because of these requirements, a constant flow of communication between all members of the team is needed, Process Experts, Programmers and System Engineers should communicate in a common language.

Permissive sequencing – Cause and Effect Diagrams



Requirements



There are several methods to assign SIF to Safety Requirement Specifications (SRS)

1. Narrative
2. Ladder Logic
3. Function Blocks
4. Cause and Effect Diagrams, etc.

We will select Cause and Effect Diagrams, because it was precisely created to simplify communications amongst safety Team Members:

Users, Engineers, Operators etc.

Permissive sequencing – Cause and Effect Diagrams

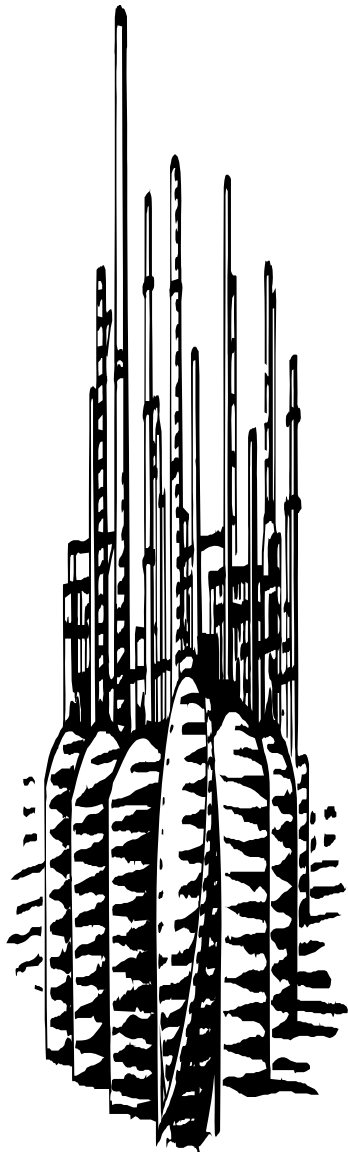
A tool for Steady State Logic

Created in the environment of the "American Petroleum Institute" (API) to facilitate the understanding of interlocks logic

Recommended Practices API 14C, for SIS in Offshore applications

Widely utilize today for safety analysis as an evaluation diagram and documentation tool

Originally a central panel indicates with LEDs, which causes and effect (which interlocks) are active



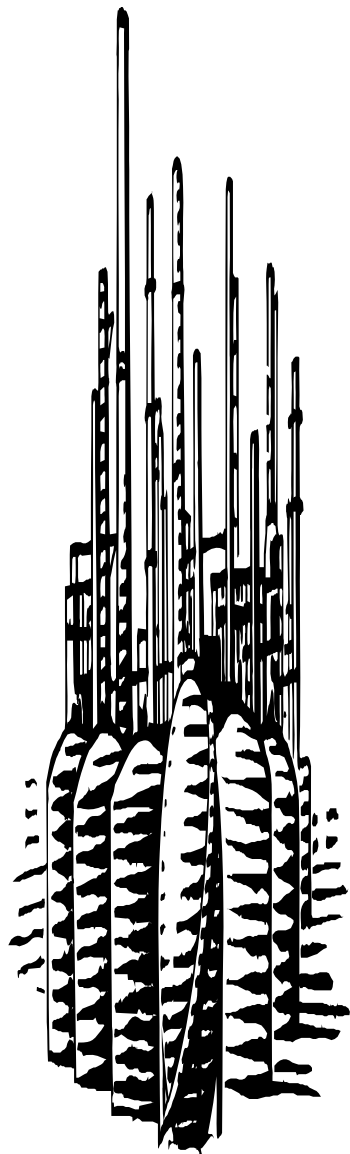
| REVISION | DATE | DESCRIPTION |
|----------|---------|---|
| 1 | 1/14/00 | ISSUED FOR APPROVAL |
| 2 | 06/02 | AS BUILT PER FIELD VERIFICATION WOC# M519L-07 |

| | | |
|--|--|--------------------|
| Company ABC | | FUNCTION PERFORMED |
| SAFETY ANALYSIS FUNCTION EVALUATION CHART (SAFE) | | |
| PLATFORM IDENTIFICATION | | FUNCTION PERFORMED |
| SHEET 13 OF 13 | | FUNCTION PERFORMED |

| IDENTIFICATION | PROCESS EQUIPMENT | SERVICE | DEVICE ID | ALTERNATE PROTECTION | | CAUSE | EFFECT |
|----------------|-------------------------------------|---------|-----------|----------------------|---------------------------|-------|--------|
| | | | | NO. OF NO. NUMBER | ALTERNATE DEVICE PROBABLE | | |
| KAH1000 | DEPARTING SALES GAS PIPELINE | PSH | | | | | |
| | | PSL | | | | | |
| | | PSV | A.9.c.3 | PSV | MAF 2500 | | |
| | | FSV 1 | | PSV | MAF 2500 | | |
| | | FSV 2 | | | | | |
| | | FSV 3 | | | | | |
| KAH2000 | DEPARTING SALES CONDENSATE PIPELINE | PSH | | | | | |
| | | PSL | | | | | |
| | | PSV | A.9.c.3 | PSV | MBD 3100 | | |
| | | FSV | | | | | |
| MBF 7100 | GENERATOR F/G SCRUBBER (THERMAL) | PSH | A.4.a.3 | PSH | MBF 7000 | | |
| | | PSL | A.4.b.3 | PSL | MBF 7000 | | |
| | | PSV | A.4.c.2 | PSV | MBF 7000 | | |
| | | LSH | A.4.d.4 | | | | |
| | | LSL | A.4.e.2 | | | | |

Permissive sequencing – Cause and Effect Diagrams

A tool for Steady State Logic



How does it work?

- A CAUSE is a process aberration (deviation)
- An EFFECT is the process response
- Intersections define Cause-Effect relationship

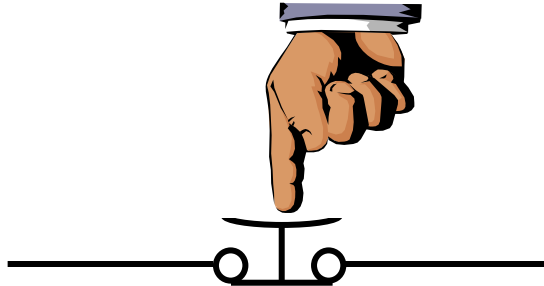
| Company ABC | | | | | | |
|---------------------------|---------|---------|---------|---------|---------|-------------|
| Safety Analysis | | | | | | |
| Function Evaluation Chart | | | | | | |
| Plant ID | | | | | | |
| Sheet 1 of 20 | | | | | | |
| Cause No | VALVE 1 | VALVE 2 | VALVE 3 | VALVE 4 | VALVE 5 | Master Trip |
| Effect No | 1 | 2 | 3 | 4 | 5 | 6 |
| Condition A | 1 | N | | | | S |
| Condition B | 2 | | N | N | | S |
| Condition C | 3 | | 2N | | | S |
| Condition D | 4 | | 2N | | | S |
| Condition E | 5 | | 2N | | | S |

Permissive sequencing – Cause and Effect Diagrams

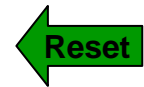
A tool for Steady State Logic

How does it work?

- ❑ In order to document appropriately, we need to expand little further:
 - ❑ There are intersections type “N” or Normal
 - ❑ There are intersection Type “S” or with Memory (Latched)
 - ❑ Voting of causes (or/and) are indicated by Intersections type “XN” or “XS” (Example below: 2oo3)

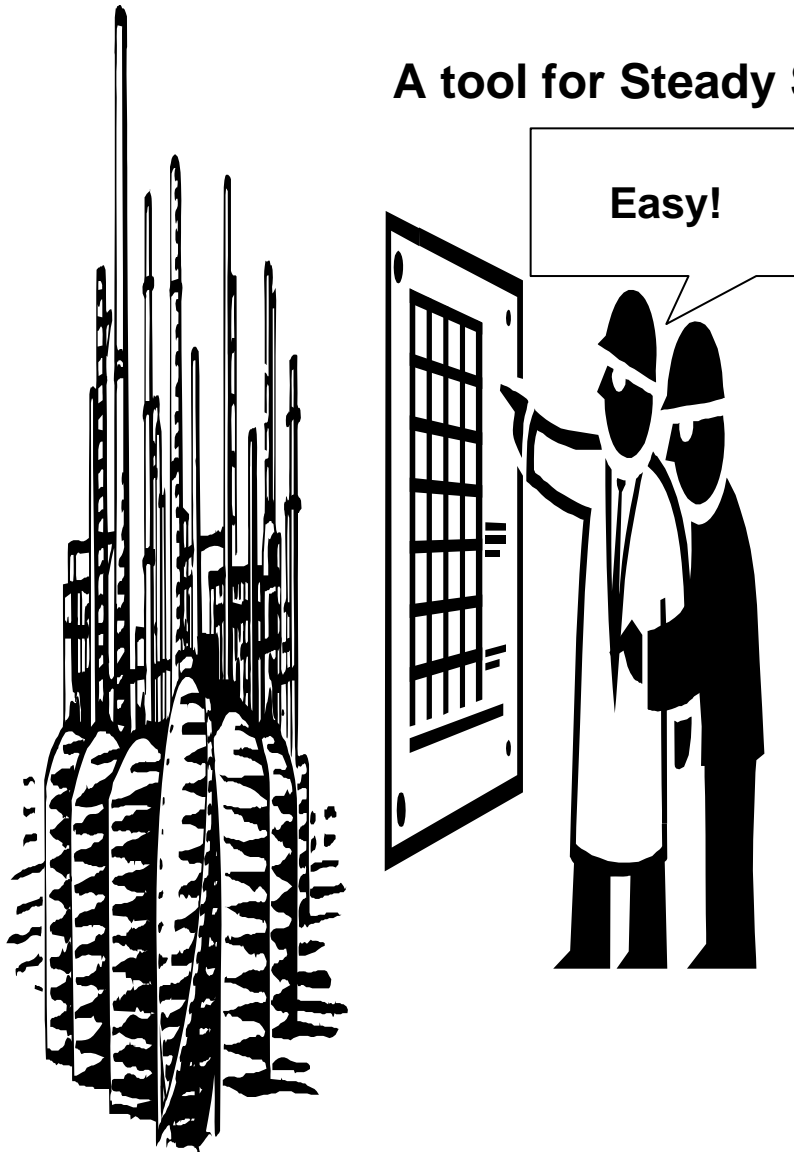


| Company ABC | | | | | | | |
|---------------------------|----------|---------|---------|---------|---------|---------|-------------|
| Safety Analysis | | | | | | | |
| Function Evaluation Chart | | | | | | | |
| Plant ID | | | | | | | |
| Sheet 1 of 20 | | | | | | | |
| Effect No | Cause No | VALVE 1 | VALVE 2 | VALVE 3 | VALVE 4 | VALVE 5 | Master Trip |
| | | 1 | 2 | 3 | 4 | 5 | 6 |
| Condition A | 1 | N | | | | | |
| Condition B | 2 | | | N | N | | S |
| Condition C | 3 | | 2N | | | | |
| Condition D | 4 | | 2N | | | | |
| Condition E | 5 | | 2N | | | | |



Permissive sequencing – Cause and Effect Diagrams

A tool for Steady State Logic



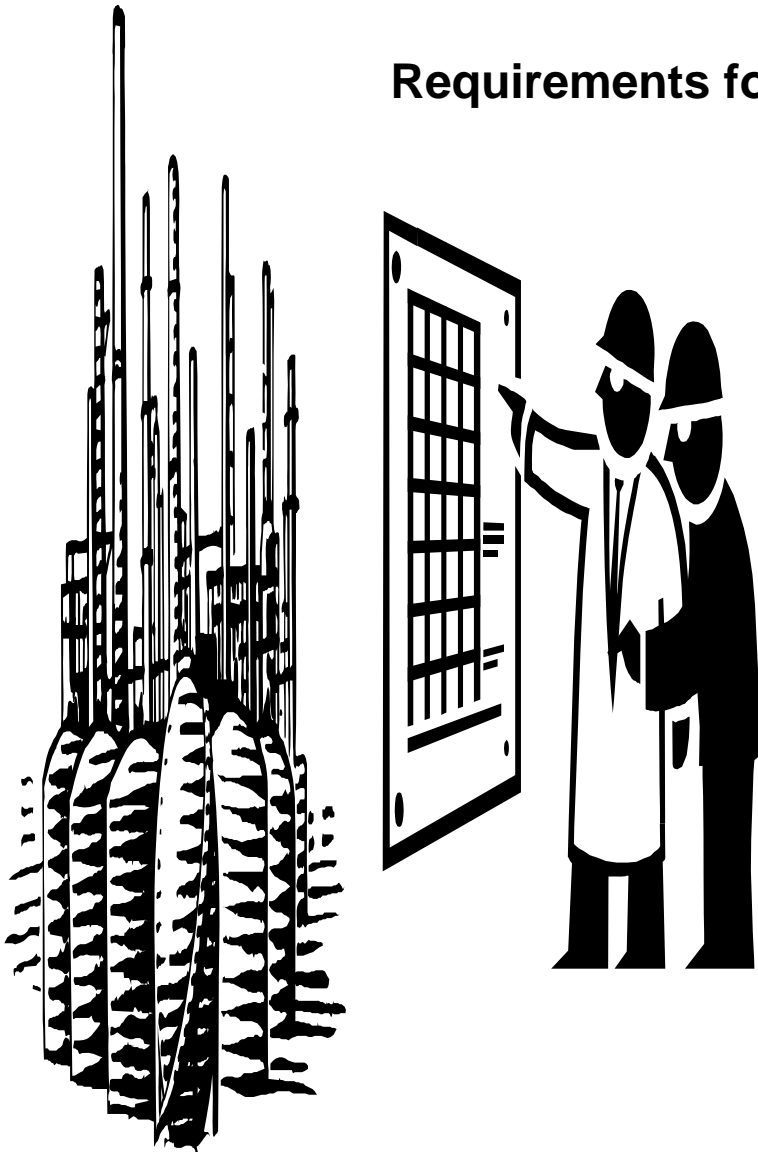
This Diagram or Matrix documents how each SRS is satisfied by a SIF.

If triggering points and final control elements actions are indicated, there is no much more needed in the form of documentation to explain the logic of the SIF

| Company ABC | | | | | | |
|---------------------------|------------|------------|-------------|------------|------------|-------------|
| Safety Analysis | | | | | | |
| Function Evaluation Chart | | | | | | |
| Plant ID | | | | | | |
| Sheet 1 of 20 | | | | | | |
| Cause No | V 101 Open | V 201 Open | V 301 Close | V 401 Open | V 501 Open | Master Trip |
| Effect No | 1 | 2 | 3 | 4 | 5 | 6 |
| Temperature > 120 °F | N | | | | | |
| Pressure > 200 Psi | | | N | N | | S |
| Flow < 56 Gal/m | | 2N | | | | |
| Flow < 56 Gal/m | | 2N | | | | |
| Flow < 56 Gal/m | | 2N | | | | |

Permissive sequencing – Cause and Effect Diagrams

Requirements for Dynamic Logic



In order to make a Cause & Effect Diagram dynamic, that is, a diagram that allows for startup sequencing, we must have:

1. The possibility of forcing effects with “overrides”, even in causes are triggered.
 1. With time limits
 2. With the appropriated intersections
2. Timers to govern the action and duration of causes
3. Causes supervision of effects or feedbacks

Permissive sequencing – Cause and Effect Diagrams

Requirements for Dynamic Logic

“Overrides” to force effects

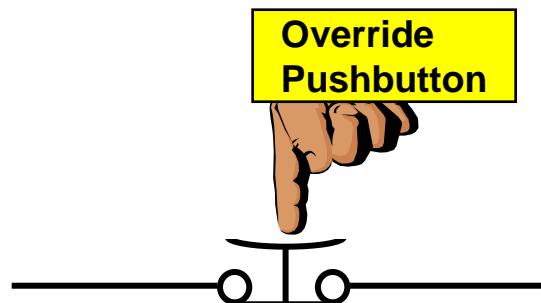
Overrides must act when switching from “de-energized” to “energized” state, similarly to resets.

Overrides must have a time limit as a function of risk assessments studies.

Their action must be allowed to be delayed if necessary

They must have special intersections :

1. Type Norma (V – effect overridden even if cause is present)
2. Type Latched (R – latched effect can be overridden)
3. Type XV or XR for voting as before

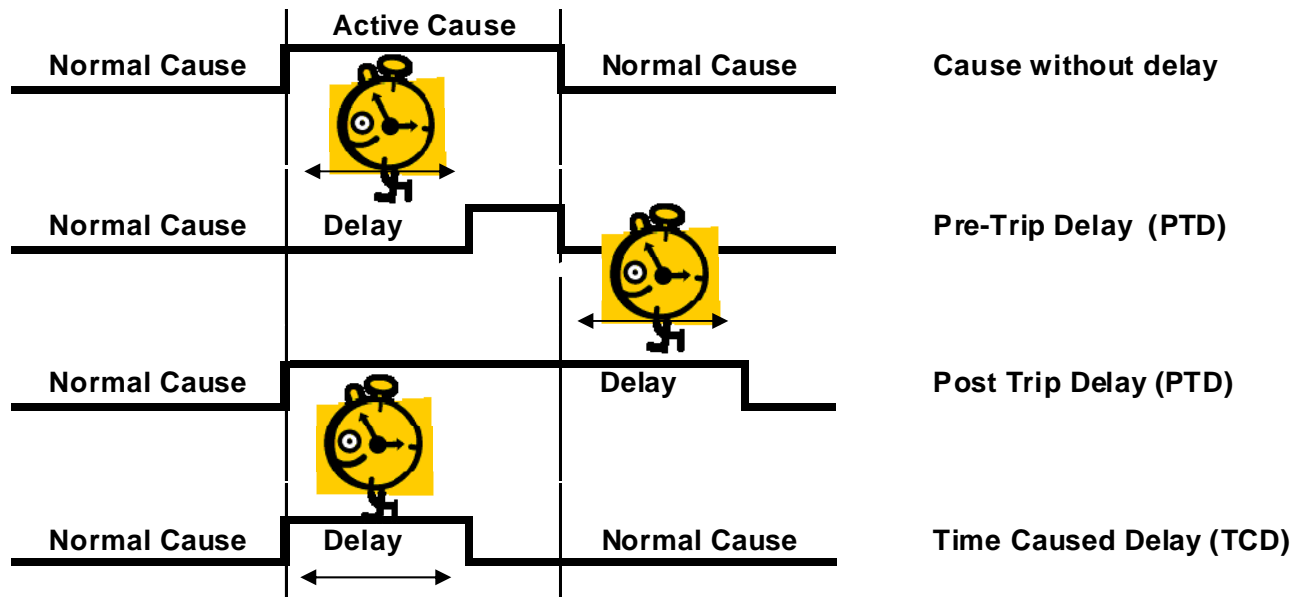


Permissive sequencing – Cause and Effect Diagrams

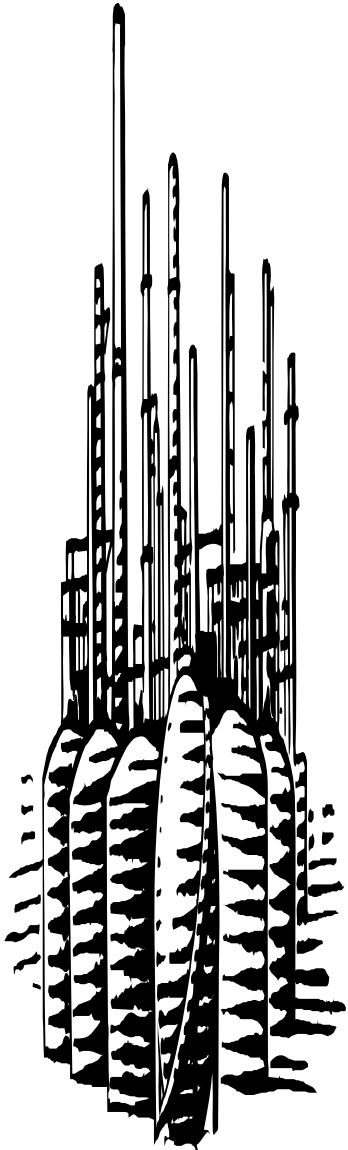
Requirements for Dynamic Logic

Cause Timers

Causes must have timers to delay their action. There are three basic ways in which such timers could function:



Example of Dynamic Documentation



Let's consider the following example:

In this petrochemical process, an hydrocarbon needs to be dried. For such purposes the fluid passes through a reactor packed with absorbent granules.

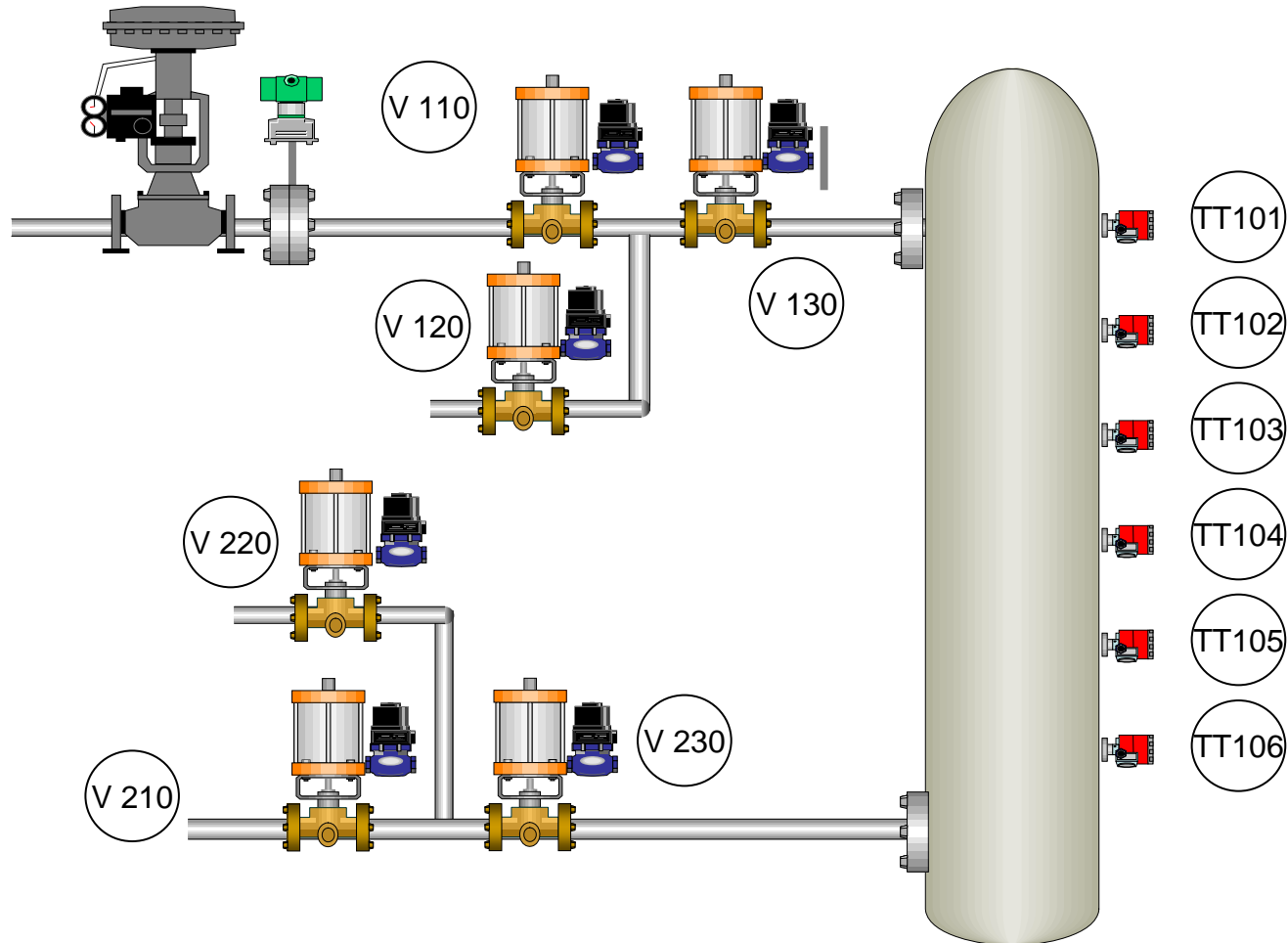
An exothermic reaction takes place in the “drier” allowing to use temperature to evaluate its performance

If the temperature goes below certain level, (110 °F), it is an indication that the granules are saturated and lost their capacity of drying the gas. But because of thermal inertia, a 20 seconds delay must be allowed before the temperature is recognized as being too low.

On the other hand, humidity is extremely harmful for the process downstream, and the SIF that protects the process has been ruled to be SIL 3 in a LOPA followed by a GAP analysis.

Example of Dynamic Documentation

Let's consider the following example:



Example of Dynamic Documentation

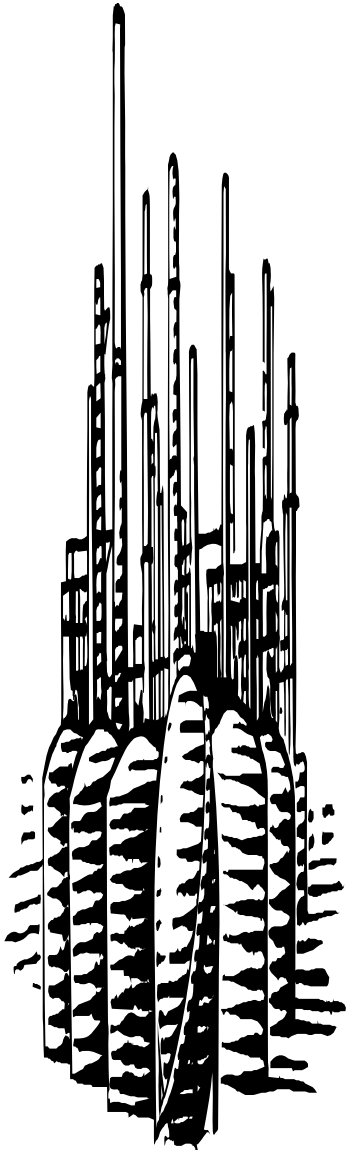
Let's consider the following example:

If 4006 measurements are below 110 °F, the process is aborted and the blocking valves would close while the bleeding ones would open

| Company ABC Safety Analysis Function Evaluation Chart Plant ID Sheet 1 of 20 | | Cause No | | | | | |
|---|---|-------------------|------------------|-------------------|-------------------|------------------|-------------------|
| Effect No | | Valve 110 - Close | Valve 120 - Open | Valve 130 - Close | Valve 210 - Close | Valve 220 - Open | Valve 230 - Close |
| Temperature TT 101 < 110 °F | 1 | 4S | 4S | 4S | 4S | 4S | 4S |
| Temperature TT 102 < 110 °F | 2 | 4S | 4S | 4S | 4S | 4S | 4S |
| Temperature TT 103 < 110 °F | 3 | 4S | 4S | 4S | 4S | 4S | 4S |
| Temperature TT 104 < 110 °F | 4 | 4S | 4S | 4S | 4S | 4S | 4S |
| Temperature TT 105 < 110 °F | 5 | 4S | 4S | 4S | 4S | 4S | 4S |
| Temperature TT 106 < 110 °F | 6 | 4S | 4S | 4S | 4S | 4S | 4S |

A traditional Steady State Cause & Effect diagram would be:

Example of Dynamic Documentation



Let's consider the following example:

Unit Startup Procedure as per operation Manual:

- 1. Bypass all temperature sensors**
- 2. Manually, open Valves V110, V130, 230 and V220, and keep Valves V210 and V120 closed.**
- 3. From the BPCS, increase flow at a rate of 5 Gallons per minute every two minutes until reaching a stable flow of 30 Gallons per minute.**
- 4. Remove bypasses on sensors, one at a time, once each have been at a stable temperature above 110 °F for at least 20 seconds. This should happen within the first 10 minutes of operation.**
- 5. Ten seconds later, Open Valve V210 and Close Valve V220.**

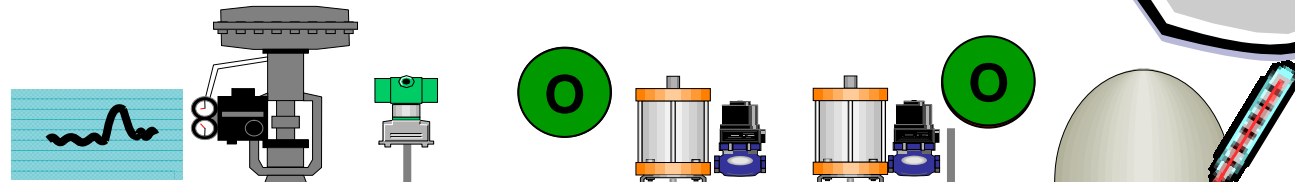
Example of Dynamic Documentation



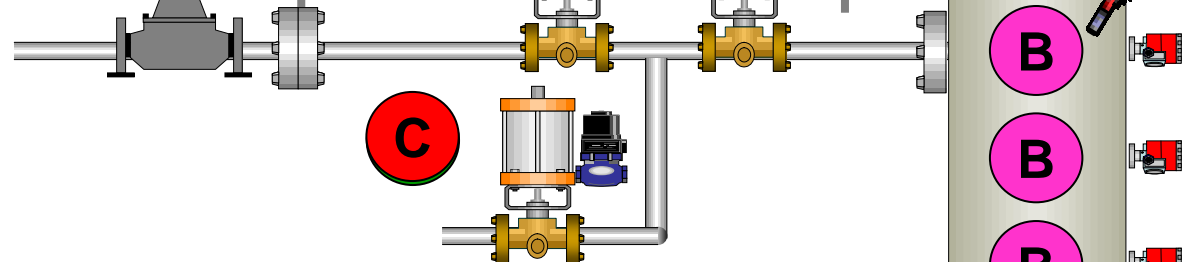
Let's consider the following example:

Manually:

1.



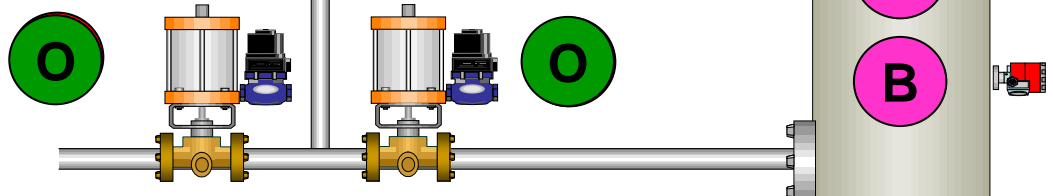
2.



3.



4.



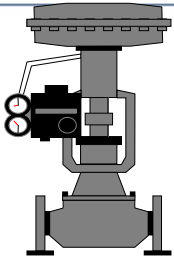
OPERATOR

NOT STRESSED!



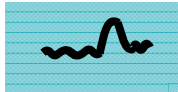
Accidents may occur. Too many manual operations

Example of Dynamic Documentation





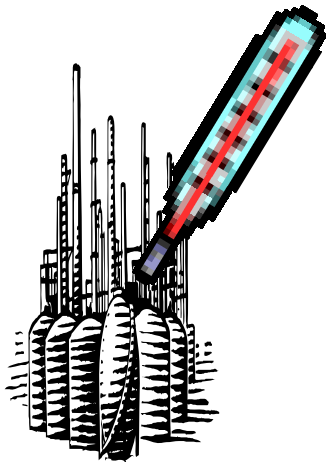
Pb_START

Let's consider the following example:  ... How does it work?



Steady State

| Company ABC | | Timers | Max Override 10 Minutes | Max Override 10 Minutes | Max Override 10 Minutes | Max Override 10 Minutes | Delay Output 10 seconds | Delay Output 10 seconds |
|-----------------------------|---|----------------------|-------------------------|-------------------------|-------------------------|-------------------------|-------------------------|-------------------------|
| Safety Analysis | | | | | | | | |
| Function Evaluation Chart | | | | | | | | |
| Plant ID |  MAX 10 M | Override - Reset Tag | PB_START | PB_START | PB_START | PB_START | | |
| | Sheet 13 of 13 | Cause No | Valve 110 - Close | Valve 120 - Open | Valve 130 - Close | Valve 230 - Close | Valve 220 - Open | Valve 210 - Close |
| |  DELAY 10 S | | | | | | | |
| Effect No | Timers | | 1 | 2 | 3 | 4 | 5 | 6 |
| Temperature TT 101 > 110 °F | PTD 20 s | 1 | 4R | 4R | 4R | 4R | 4N | 4N |
| Temperature TT 102 > 110 °F | PTD 20 s | 2 | 4R | 4R | 4R | 4R | 4N | 4N |
| Temperature TT 103 > 110 °F | PTD 20 s | 3 | 4R | 4R | 4R | 4R | 4N | 4N |
| Temperature TT 104 > 110 °F | PTD 20 s | 4 | 4R | 4R | 4R | 4R | 4N | 4N |
| Temperature TT 105 > 110 °F | PTD 20 s | 5 | 4R | 4R | 4R | 4R | 4N | 4N |
| Temperature TT 106 > 110 oF | PTD 20 s | 6 | 4R | 4R | 4R | 4R | 4N | 4N |
| Effect No 1 | | 7 | R | R | R | R | N | N |



Conclusions and Recommendations



Luis' Principle:
If it can be documented in a Manual can be Programmed in an SIS!

1. Planning Startup Sequences is as complex and complicated to do in an operation manual as it is in a logic tool.
2. In fact, more prescriptive standards like NFPA 85 and 86 already require the automation of startup sequences for Boilers and BMS in a BMS.
3. More tools or tools to automate startup sequences. In such way, the processes are always at all times. Furthermore generate necessary documentation to verify and validate the sequences as any steady state logic.
4. Performance based standards (like ANSI/ISA 84.00.01 or IEC 61511 Mod.) should consider addressing the issue of permissive sequencing for Startup, shutdowns and process transitions in a more prescriptive way.

End of the presentation

Any Question?

**Thank you for your
time**

