Risk Management in the process industry

M. Rodríguez, I. Díaz
Autonomous Systems Laboratory
Technical University of Madrid

2014 STAMP Conference

1. Today: Safety in the process industry

2. Tomorrow: STPA for the process industry?
   A simple example. Open Questions

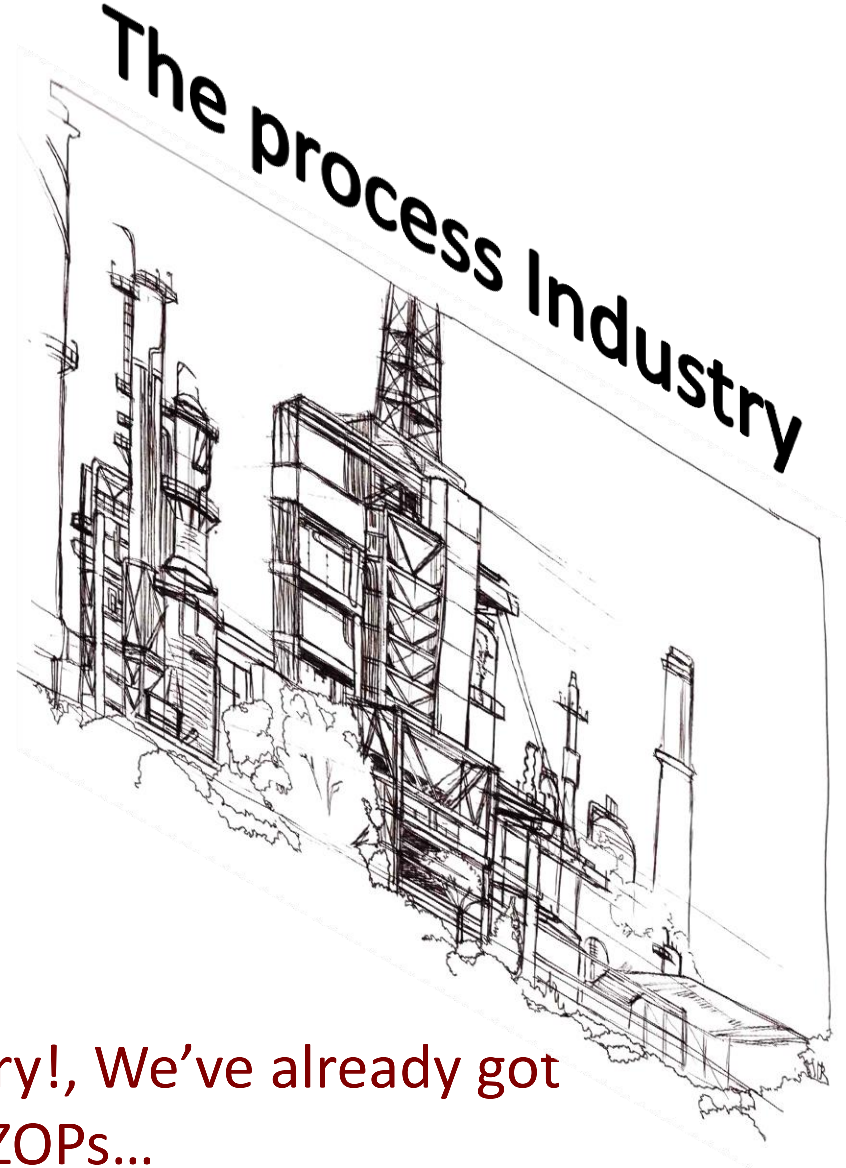
3. Functional modeling & STPA

1. Today: Safety in the process industry

SAFETY CULTURE

CARTOON BY MICHAEL MITTAG, WWW.COOLRISK.COM

Hey listen… I sell STPAs
It’s good for your business



Sorry!, We’ve already got HAZOPs…

I know…. But look!

Unexpected Events Cost 3-8% Capacity

$10B annually lost in production (only in US)

THE HINDU

STATES WORLD S ASIA

Malaysia Chronicle

Home Politics Business Social Features Latest Videos

Saturday, 15 March 2014 05:56

Fertiliser plant EXPLODES in Sarawak town, 8 workers rescued

SERIAN - An explosion ripped through a fertiliser factory here at about 3pm today, causing the building to collapse on workers and sending a shockwave throughout the town, some 60km southeast of Kuching, the capital of Sarawak.

Eight workers buried under the rubble were pulled out by the Fire and Rescue Department, alive but with minor injuries, and sent to Serian Hospital for treatment.

More people are believed to be trapped underneath, The Star reported on its website, adding that rescue efforts are still ongoing.

A spokesperson from the Fire and Rescue Department, who declined to give his name, said a distress call was received around 3.05pm.

Three fire engines each from the Serian, Siburan and Tabuan Jaya stations were despatched to the site of the blast within 10 minutes, the official added.

The cause of the blast is yet unknown, the fireman said, adding that an investigation is underway.

Several other properties in the vicinity of the plant were also damaged.

Serian is a small town with a population of roughly 90,700 people, and is most famed for its durians. -Malaymail

Your Hometown Newspaper

409 W Hill Street |

806-637-4535 |

One killed at Industrial

Friday, March 07, 2014 9:14 AM

A 43-year-old Tyler man died at the scene of an industrial accident Thursday afternoon, which occurred at a chemical plant in southwest Terry County.

Sheriff Larry Gilbreath told the Brownfield News on Thursday afternoon that James Croft, 43, of Tyler was killed while conducting demolition work at Venture Chemicals, located roughly two miles north of Seagraves, just west of FM 62/385, inside the Terry County line.

According to an initial investigation, Croft was operating an excavator while co-workers were attempting to take down a silo tank.

The tank fell unexpectedly and landed on the excavator inside.

Gilbreath said the 600-barrel-capacity silo tank hou

Terry County Justice of the Peace Angie Garza pro an autopsy, according to Gilbreath.

The Indian EXPRESS

Home > Cities > Delhi

Eight workers ... mill explosio...

Ghaziabad | March 14, 2014

SUMMARY

The explosion at the mill carried out in the ...

Tweet This

Chemical container blast injures woman,3 children

Two killed,five injured in explosion at fireworks factory

Blast at Japanese summer festival injures 59

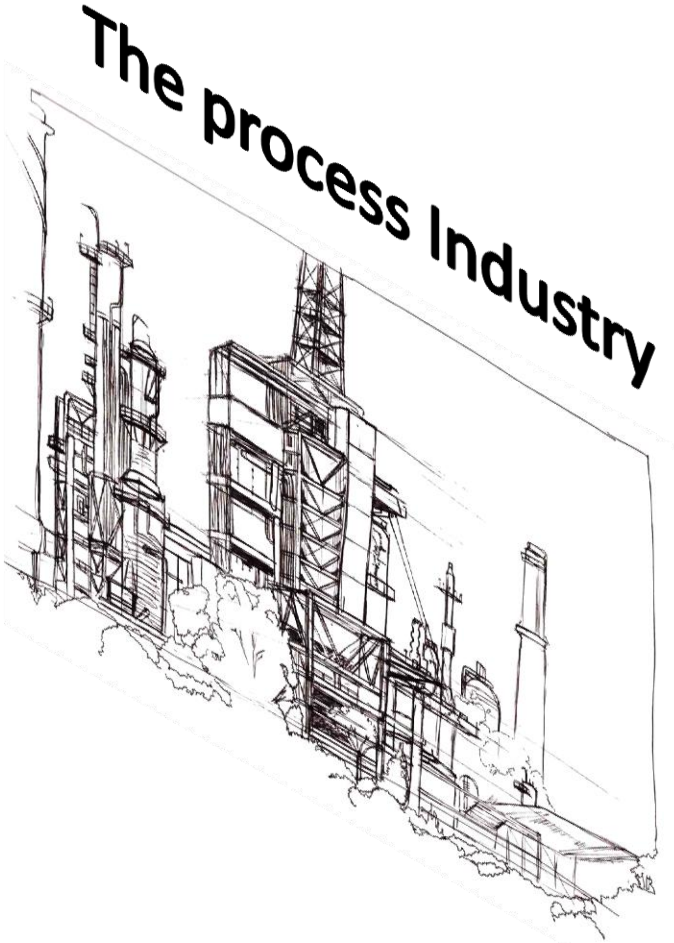
The eight have been identified as Sahil, Chandradev Yadav, Ravindra, Ram Niwas, Jamaluddin, Tilakram, Sunil and Gurwinder Singh.

Тэги: Almalyksy chemical plant

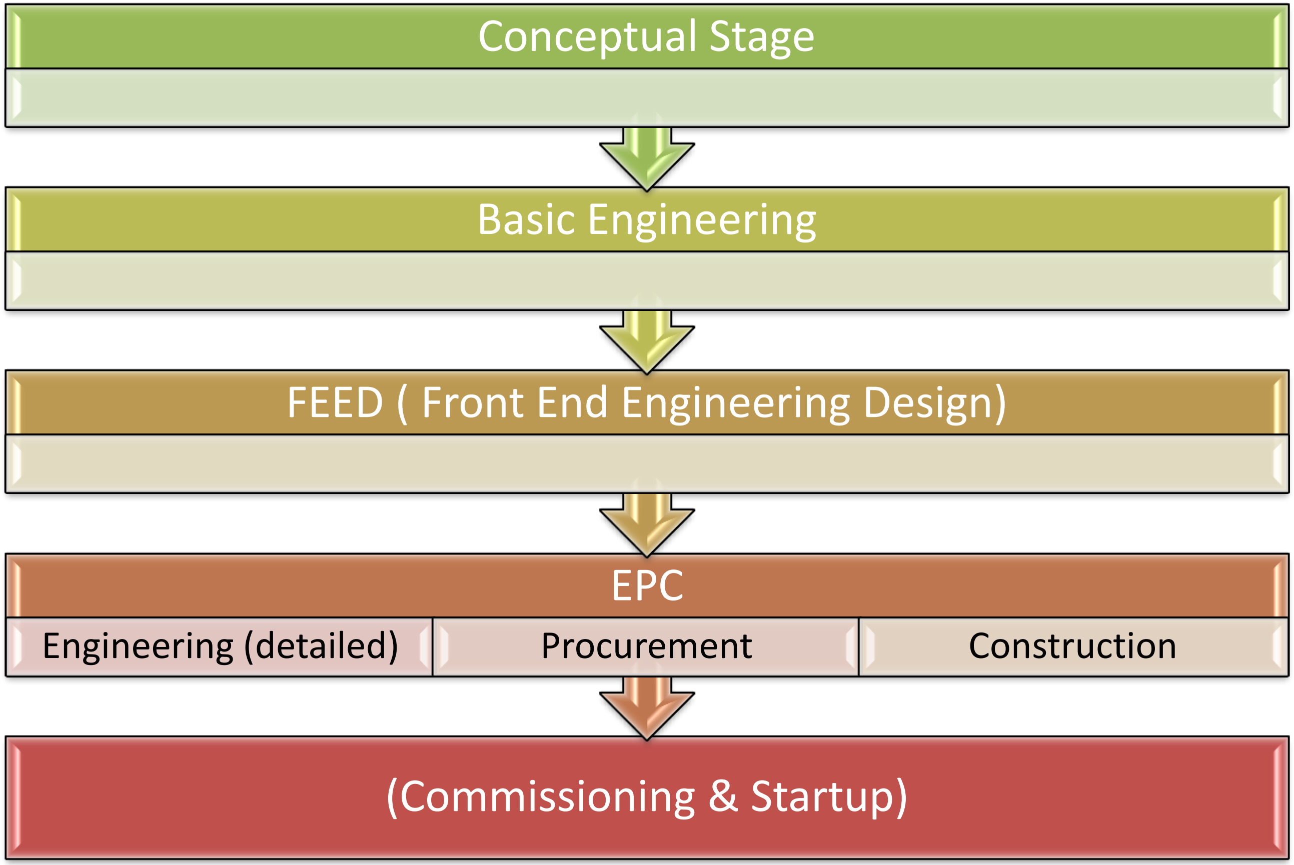
I would say you've still got a problem!!

Ok let's talk.

Let me tell you HOW WE DO THINGS HERE..



The Design Process



The Safety Process

Establish context & Process Info
- Stakeholders

↓

Identify Hazards
- Risk Classes

↓

Risk analysis & assessment
- Analysis methods
- Likelihood & Consequences

↓

Risk Reduction
- Reduce likelihood/consequences
- Transfer full / part
- Avoid Risk

Standards

IEC 61511 / ISA S84.01

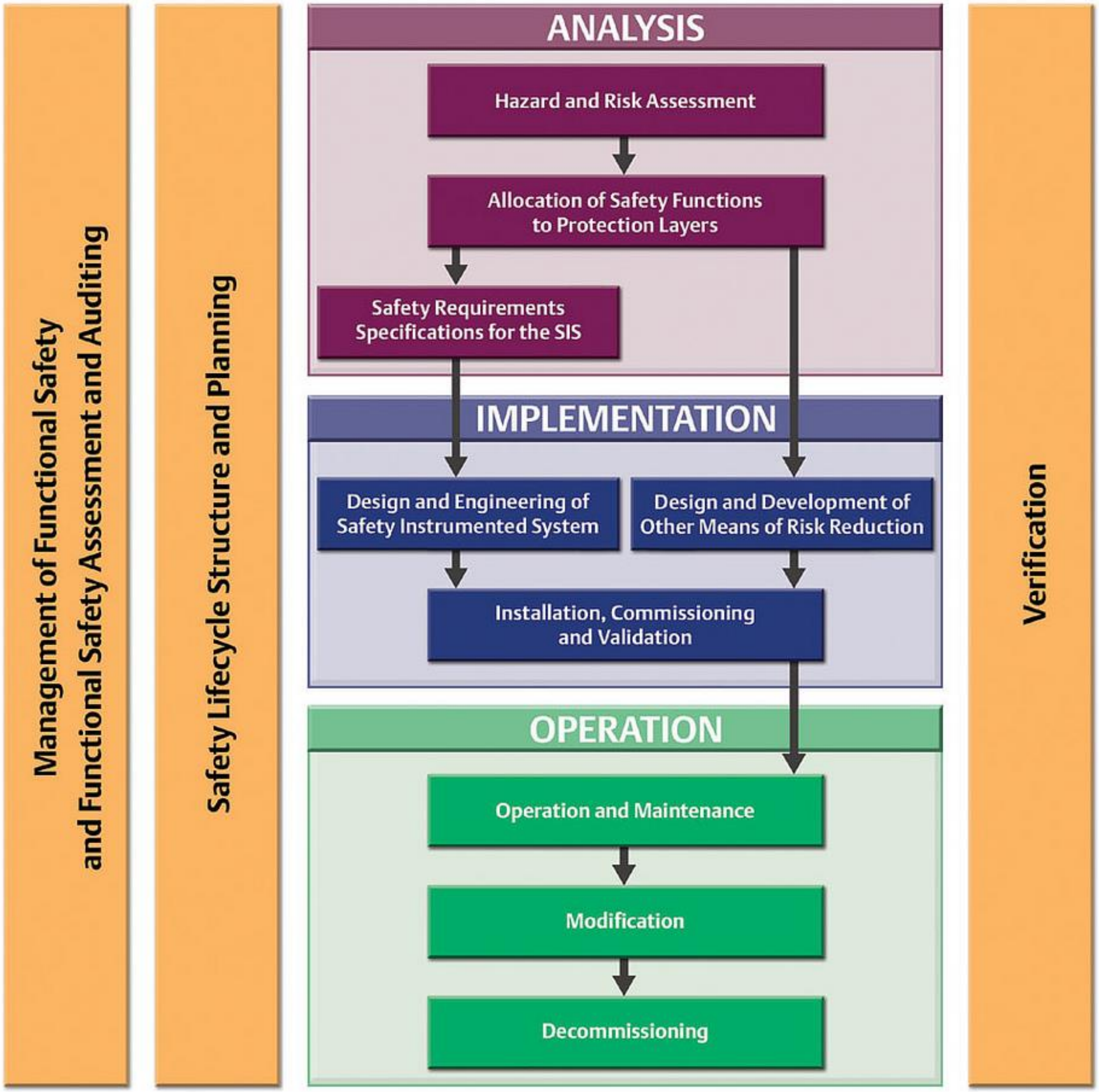
(IEC 61508)

Regulations

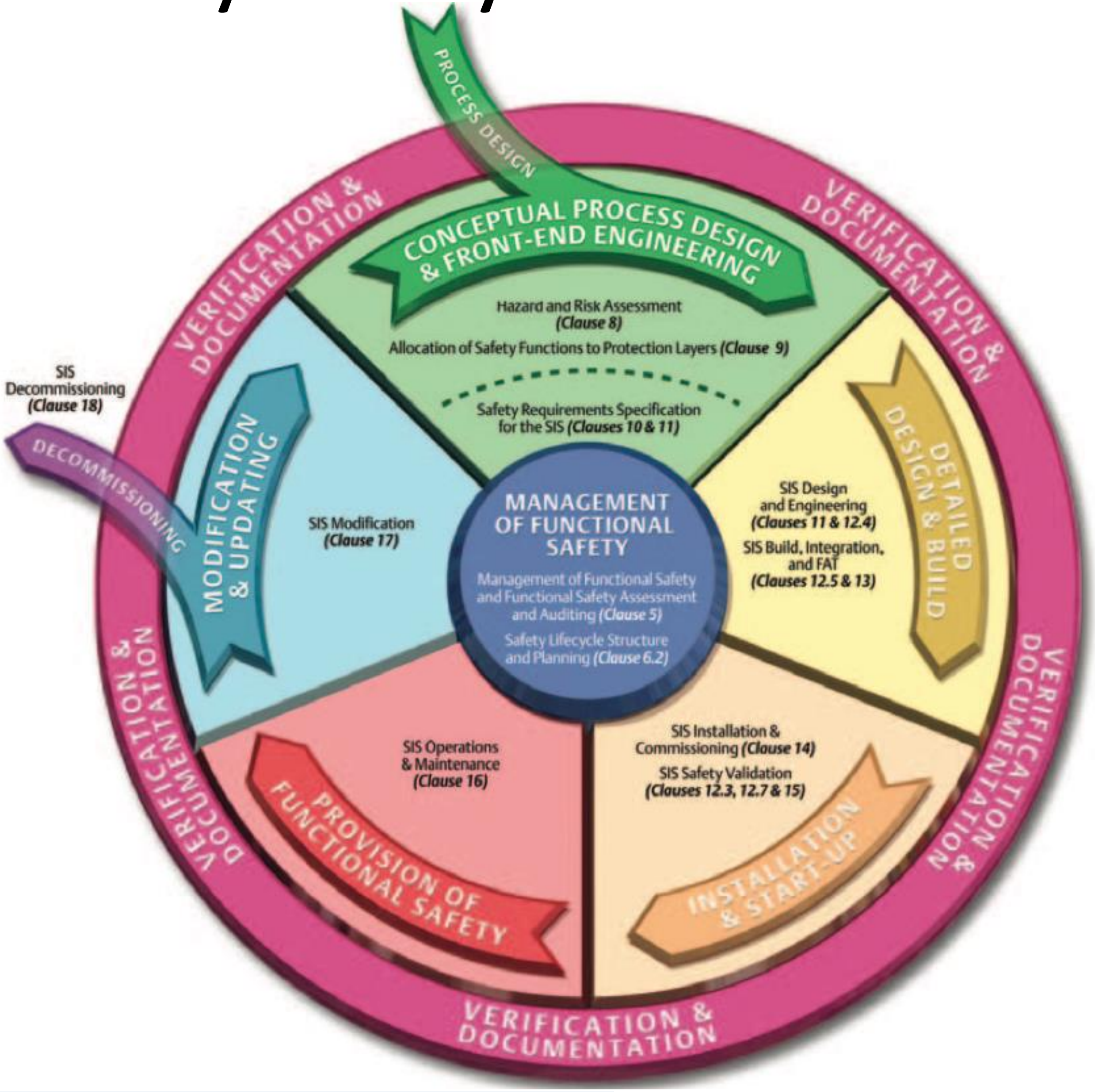
Seveso I, II, III --- Europe

OSHA 29 CFR1910.119 --- USA

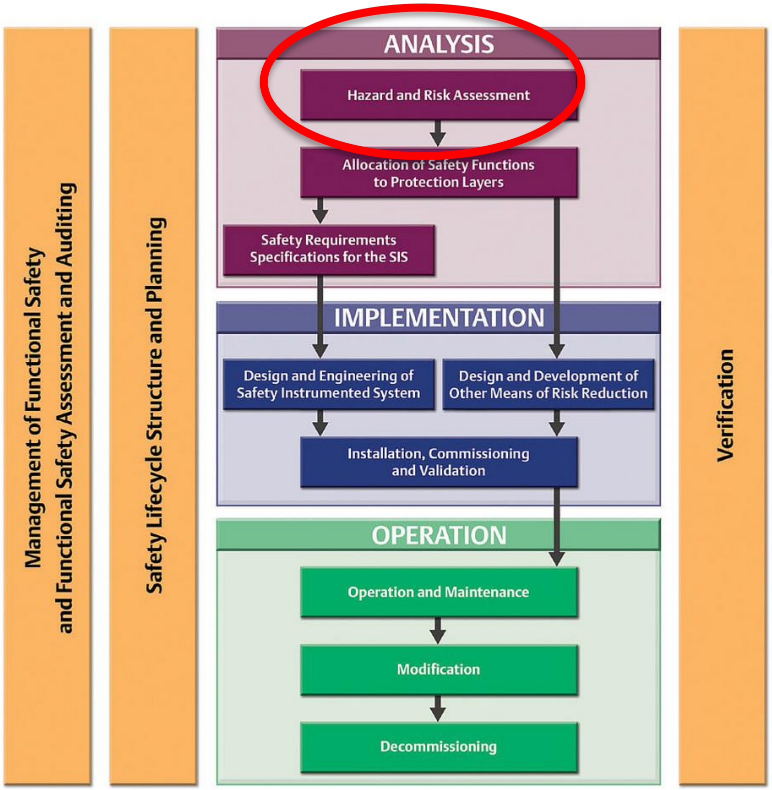
IEC 61511 Safety Lifecycle



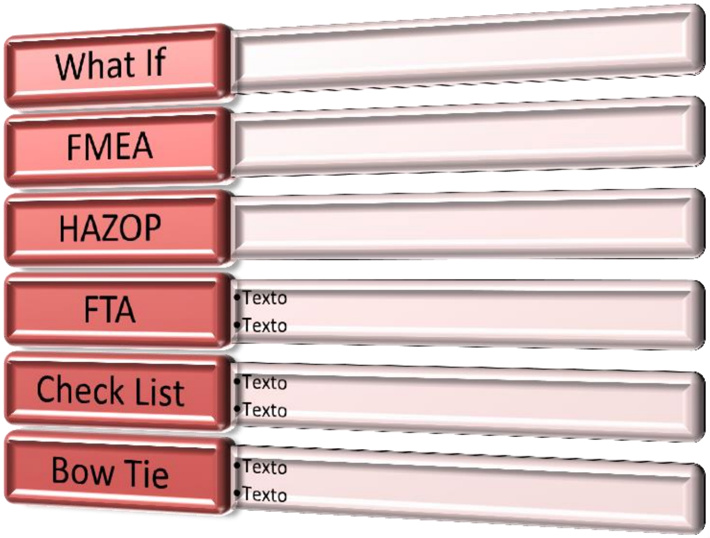
Safety Lifecycle Closed Loop



Hazards studies



1. Hazards types identification
2. Preliminar Hazard Analysis
3. Analysis Methods & Evaluation



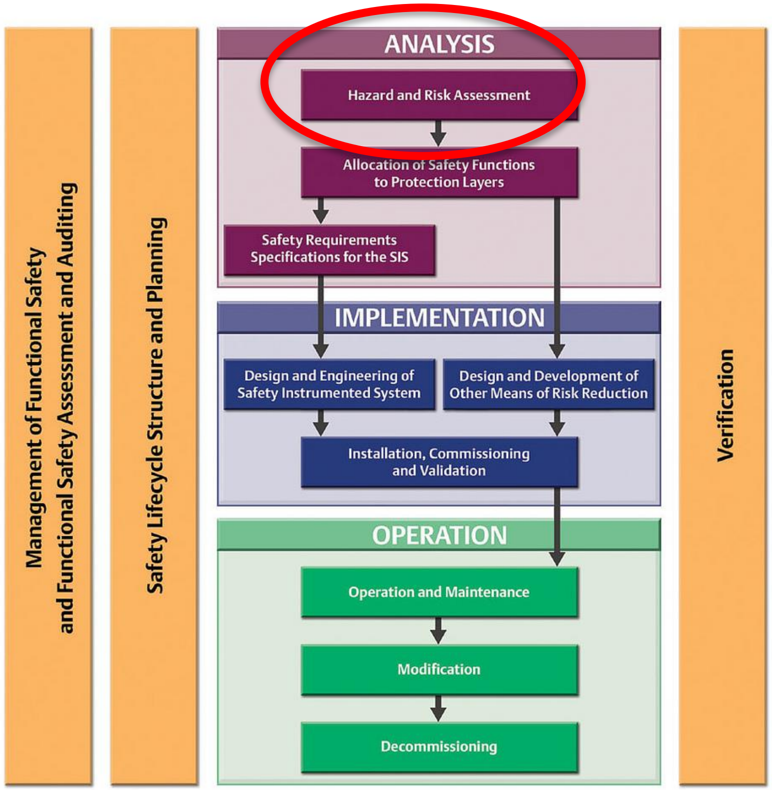
Preliminar PHA example

Hazardous Event/ Situation	Prompts	
External fire	Fuel	Flammable gas, vapour, solid, metal, wood, waste material, pyrophoric material
	Release mechanism	LOC, poor housekeeping
	Ignition	Sparks, flares, static, friction, vehicles, hot spots, welding, lightning, auto-ignition, furnaces
Internal fire (in equipment)	Flammable mixture	Flammable gas, vapour, liquid, solid, metal, dust, residue, pyrophoric material, oxygen, halogen
	Ignition	Sparks, static, friction, welding, decomposition
Internal explosion (in equipment)	Physical over pressure	LOC (Burst-Physical overpressure), head pressure, liquid filling, testing, purging
	Uncontrolled reaction	Runaway reaction, decomposition, polymerization, contamination
	Flammable mixture	Flammable gas, vapour, liquid, solid, dust, mist, oxygen, halogen, NCl_3, explosive/unstable compound, polymerization, loss of ignition/re-ignition
	Ignition	Sparks, static, friction, hot spots, welding, decomposition

Hazardous event/situation	Immediate consequences	Ultimate consequences
Chronic harmful/ noxious exposure	Chronic effect on employees, Chronic effect on public	B, D, M
Pollution	Visual (inconvenience/disturbance), harm to flora and fauna, fish kill	H, I, J, K, L
Violent release of energy	Equipment damage, knock-on-loss of containment, missiles	A, E, F, G, J, K, M
Noise	Nuisance/hazard to employees, Nuisance/hazard to public	J, K
Visual impact	Nuisance/annoyance to public	J, K
Major financial effect	Direct damage, Consequential loss	F, G

Code	Group	Consequences
A	Employees	Injuries/fatalities
B		Ill health/long-term fatalities
C	Public	Injuries/fatalities
D		Ill health/long-term fatalities
E	Fire fighters	Injuries/fatalities
F	Plant damage	Damage to plant and equipment
G		Loss of production
H	Environmental damage	Harm to Flora and Fauna
I		Fish kill
J	Publicity/media	Bad publicity
K		Public/product concern/site licence
L	Authorities	Environmental protection
M		Industrial incidents/accident investigators
N	Other effects	Evacuation of site
O		Evacuation of public
P		Obnoxious odor

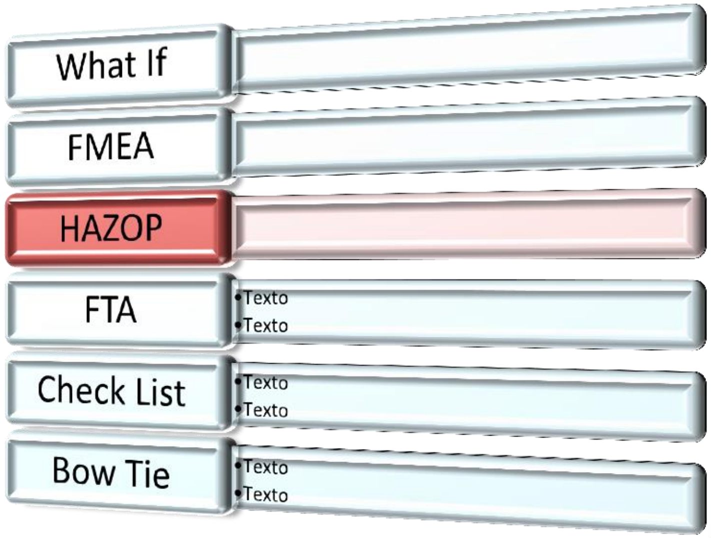
Hazards studies



1. Hazards types identification

2. Preliminar Hazard Analysis

3. Analysis Methods & Evaluation



HAZOP

DESIGN INTENTION

MIXING
PHASE
LEVEL
TEMP.
PRESSURE
COMPOSITION
FLOW
REACTION
COMM

DEVIATION
=
ELEMENT + GUIDEWORD
(PARAMETER/
CHARACTERISTIC)

NO / NONE
MORE
LESS
AS WELL AS
PART OF
REVERSE
OTHER THAN

WHERE ELSE
BEFORE / AFTER
EARLY / LATE
FASTER / SLOWER

[NOT ALL DEVIATIONS FEASIBLE]
DIRECT CAUSALITY →

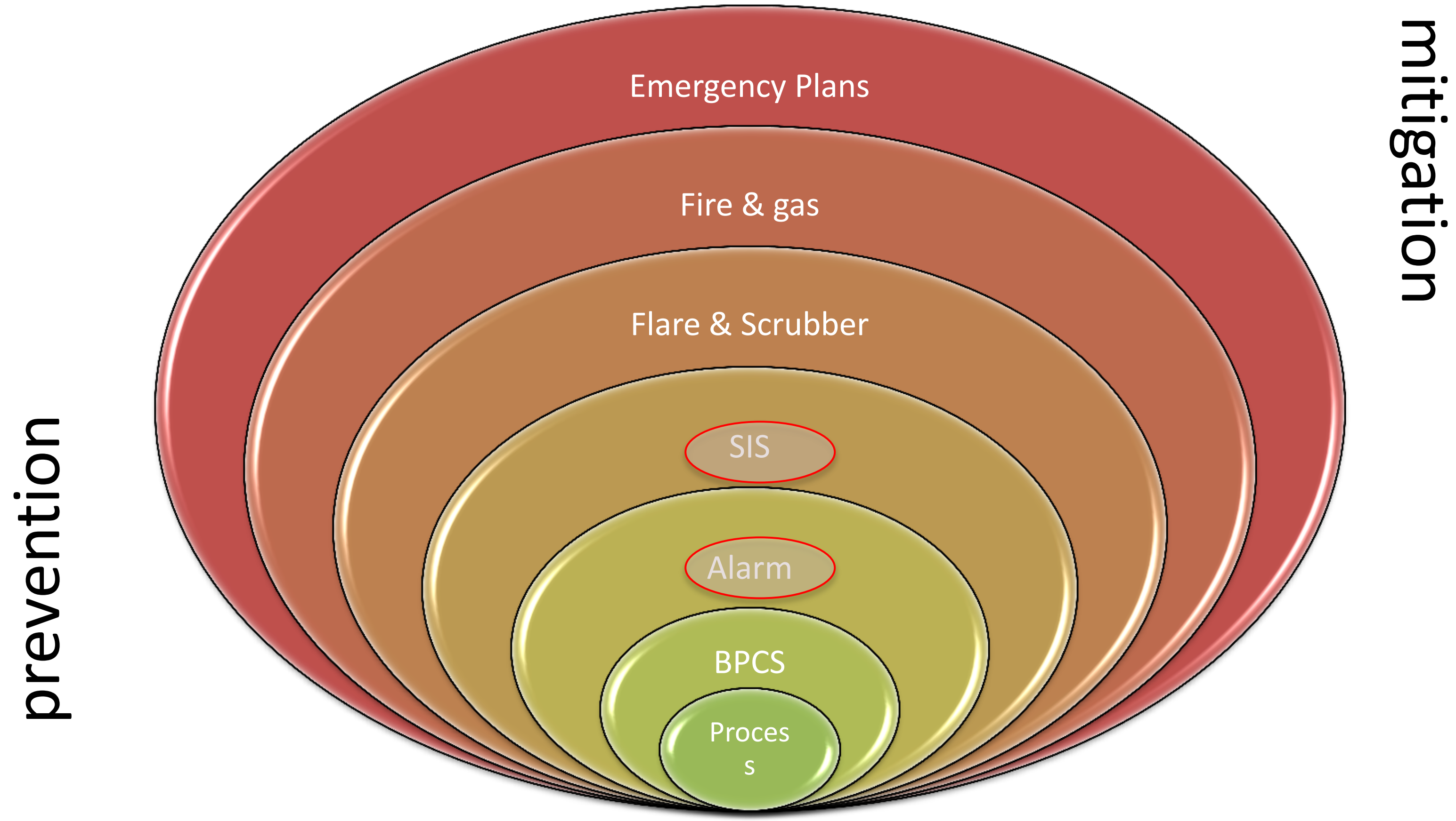
CAUSES

CONSEQUENCES

SAFEGUARDS

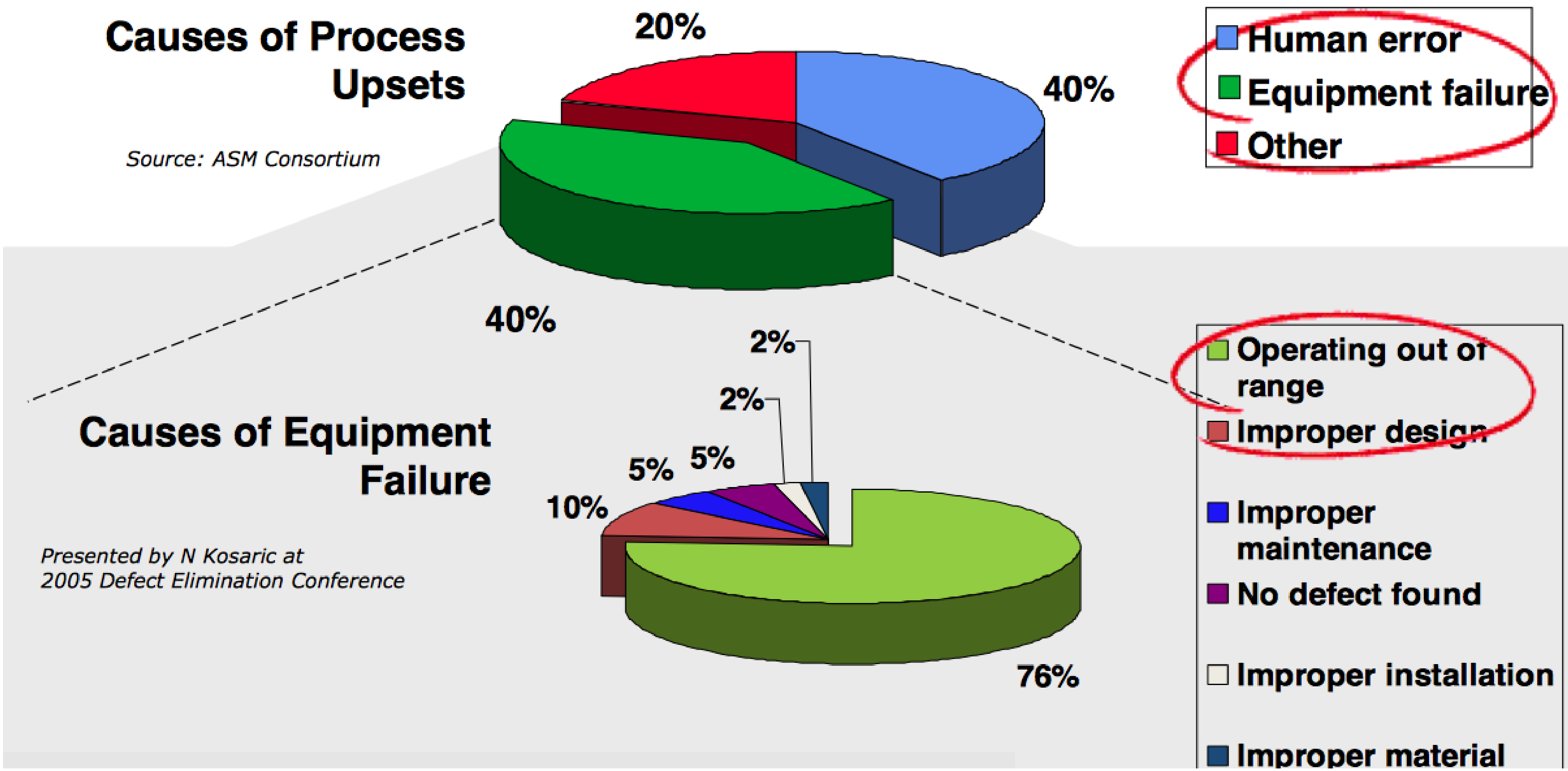
ALARMS/SIS ← RECOMMENDATIONS /ACTIONS

The Result: Layers of Protection



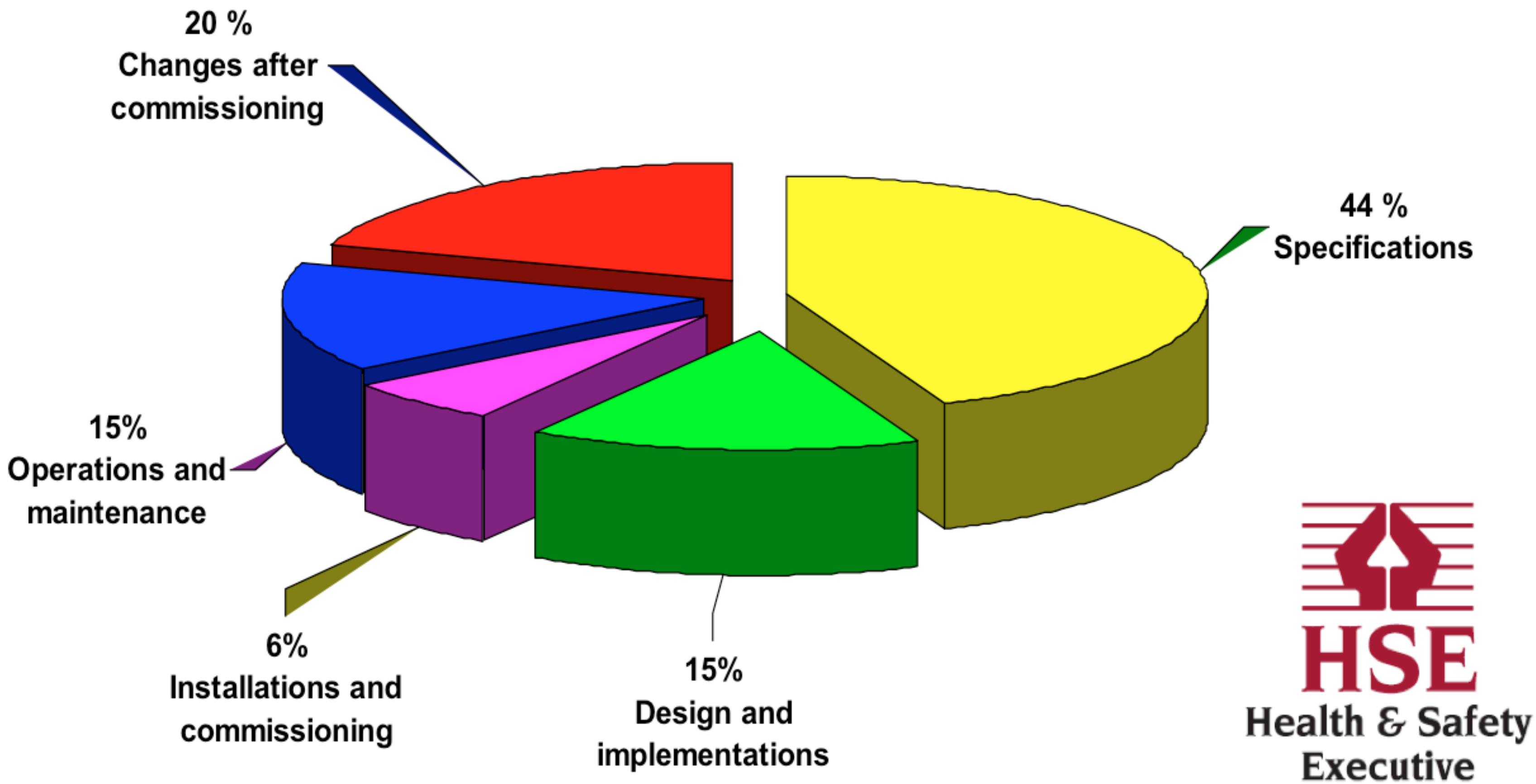
Nice!. Let me show you something….

Accidents causes



Accidents causes

(SIS layer)



"I think we need to take another look at your risk-management strategy."

2. Tomorrow: STPA for the process industry?

What I do (and HAZOP doesn't)

- Include socio-technical analysis (human factor)
- Include systemic factors
- Include all the hierarchy (from regulations to the process): Safety culture
- Fill the design operation gap: avoid higher risk states

What I do not do (vs. traditional safety)

- Put the blame on you
- Consider only reliability and probability
- Work only in the design stage

Basically I don’t follow chains of events!

STPA

HAZARDS TYPES
HAZID

1. ESTABLISH SYSTEM ENGINEERING FOUNDATION

↓ FUNCTIONAL CONTROL STRUCTURE

2. IDENTIFY UNSAFE CONTROL ACTIONS (UCAs)
   - PROVIDED
   - NOT PROVIDED
   - EARLY / LATE
   - TOO SOON / TOO LONG
   - NOT FOLLOWED THE CA

↓

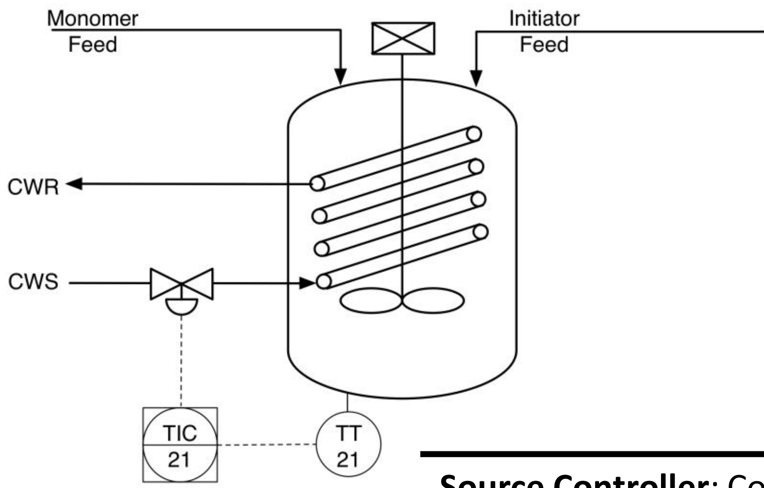
3. USE UCAs TO CREATE SAFETY REQUIREMENTS / CONSTRAINTS

↓

4. DETERMINE HOW EACH HAZARDOUS CONTROL ACTION COULD OCCURR

A simple example

STPA for the process industry



States considered:

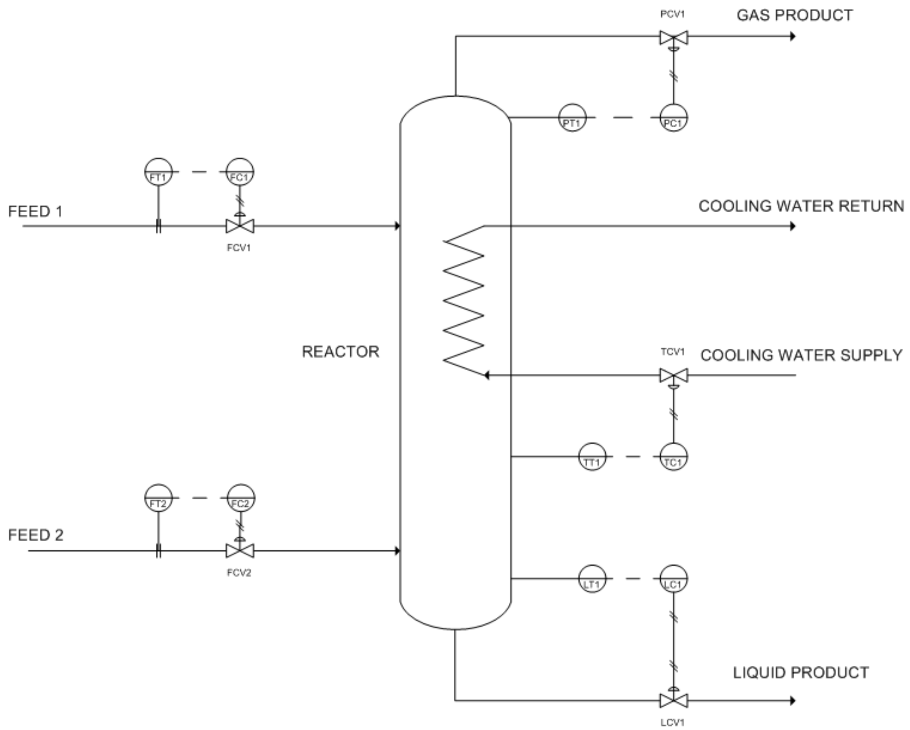
- Desired (D)
- More (+)
- Less (-)
- No / none (N)

Source Controller: Cooling Water Supply. **Type** Not provided				
Process Variables: Context		System state		
Fmonomer	Finitiator	Reaction Rate	Temperature	Hazard
D	D	+	+	Yes
+	D	+	+	Yes
+	N	N	D	No
N	+	N	D	No
D	+	+	+	Yes
…	…	…	…	…

Preventive actions can be obtained from the analysis!!

They can be ranked following some criteria, for example less deviation from current hazardous state

STPA for the process industry



Accident	Hazard	Safety Constraint
Explosion	H1: Temperature too high	Temperature must never violate maximum value
	H2: Pressure too high	Pressure must never violate maximum value
Leakage	H3: Level too high	Level must never violate maximum value

Source Controller: Open level control valve. **Type**: Not Provided

ID	Fcw	Fgas	F1	F2	Hazard
1	+	+	+	+	H1, H2, H3
2	+	+	+	-	H2, H3
3	+	+	+	N	H2
4	+	+	+	D	H2, H3
5	+	+	-	+	H3
6	+	+	-	-	H3
7	+	+	-	N	--
8	+	+	-	D	H3
9	+	+	N	+	H3
10	+	+	N	-	H3
11	+	+	N	N	--
12	+	+	N	D	H3
…	…	…	…	…	…
…	…	…	…	…	…
…	…	…	…	…	…
252	D	D	N	D	H3
253	D	D	D	+	H3
254	D	D	D	-	H3
255	D	D	D	N	--
256	D	D	D	D	H3

Long tables

States considered:

- Desired (D)
- More (+)
- Less (-)
- No / none (N)

Open Questions

- STPA explicit step? Be sure that there is at least one control action for every hazard identified
- A chemical plant has thousands of variables and controllers: How to define the system limits for the analysis? Physical equipment? Functionally?
- How many states must be considered for the Process Variables (discretize)?
- How many variables have to be considered (pressure, flow, composition, temperature, etc.)?
- Can STPA cope with hazards like pipe leaks, dust accumulation, static electricity, HTHA cracking, alarms problems, etc.?
- How to filter relevant contexts to hazards to avoid unneccessary scenarios?

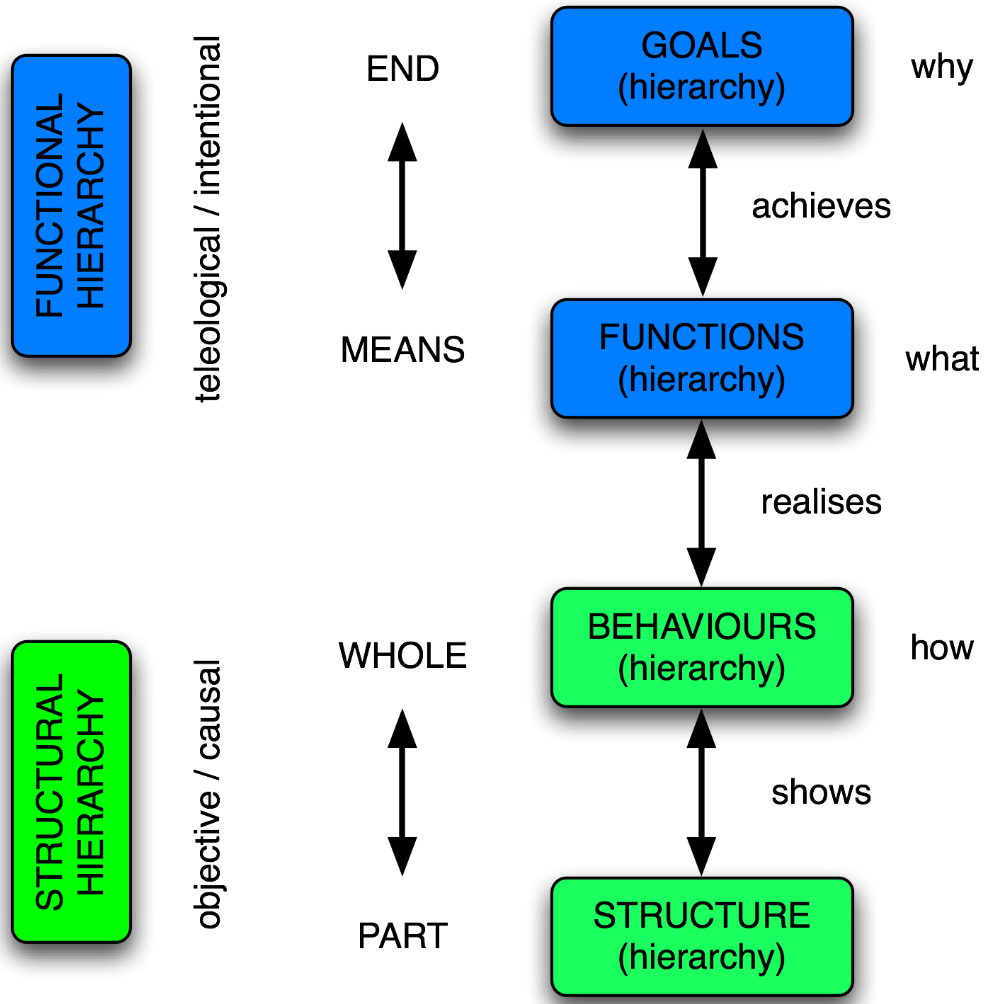
3. Functional modeling & STPA

But there's more, if you buy STPA you get …..

A functional modeling tool FOR FREE!

Functional Modeling

Methodology used to model any man made system by identifying the overall goal and the functions needed to achieve it. It uses qualitative reasoning.



Why Functional Modeling?

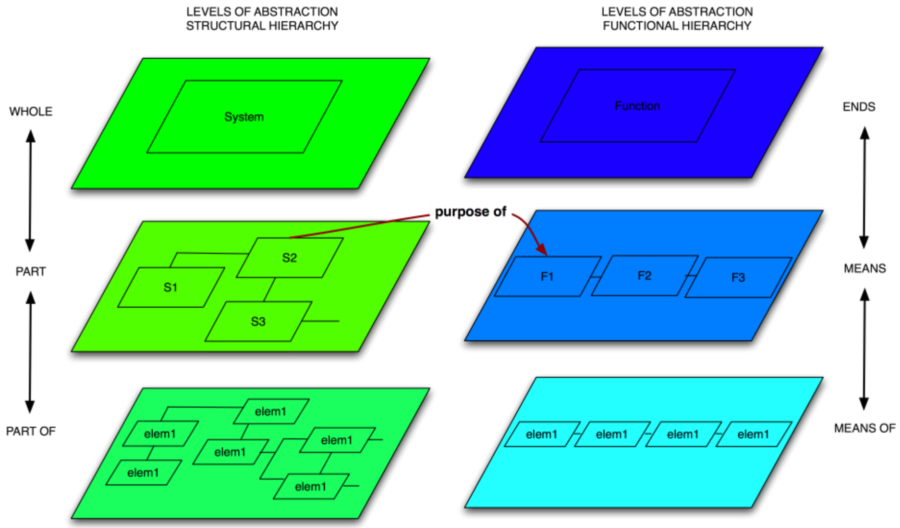
Integrated Process Design & Operation & Automation

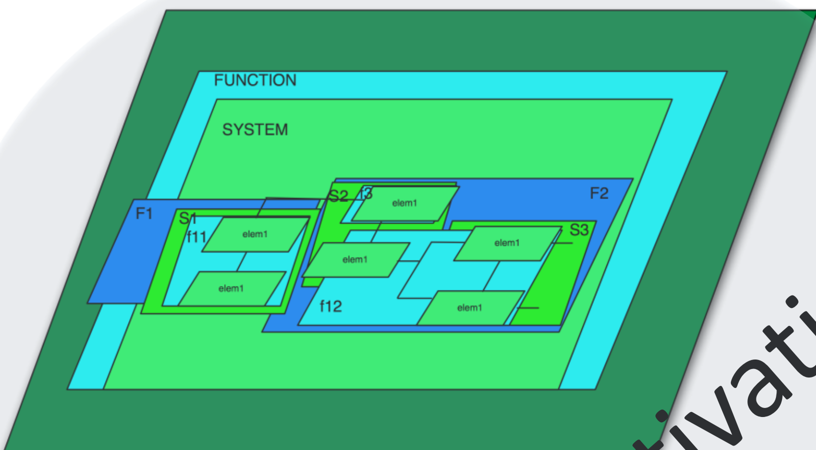
Provide a systematic framework for formalizing inter subjective common sense knowledge which is shared among participants in design and operation of complex systems i.e. engineers and operators.

Functional modeling is a systematic approach to applying different perspectives and degree of abstraction in the description of a system and to represent shifts in contexts of purpose. This aspect of FM is crucial for its use in handling complexity in systems design and operation.

Support integrated process and control system design by providing abstractions by which high level decision opportunities and constraints in process and control system design can be made explicit. FM can be used to reason about control strategies, diagnosis and planning problems.

M. Lind.Nuclear Safety and Simulation, Vol. 4, Number 3, September 2013

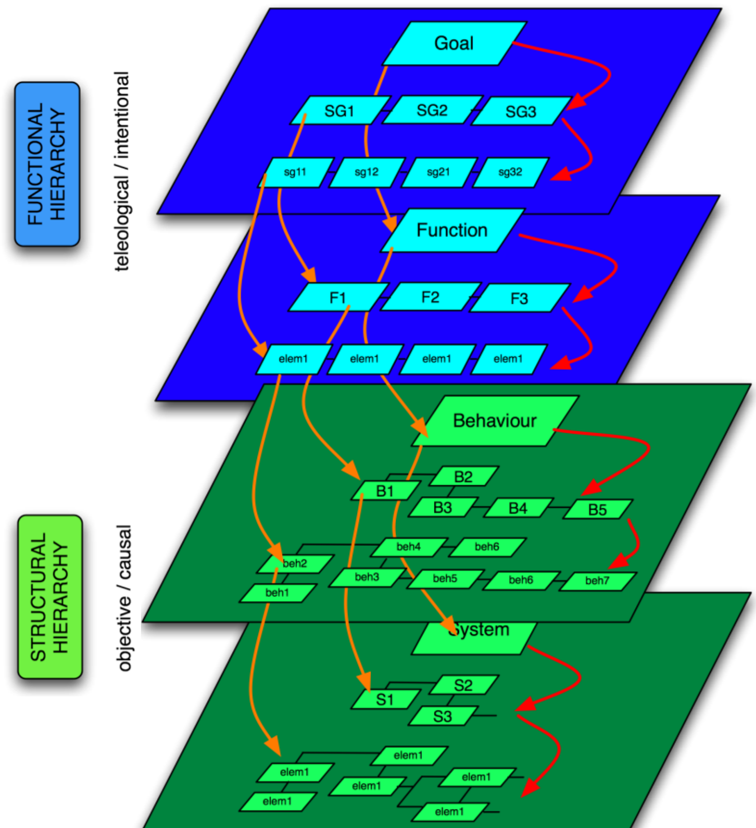




motivation

ALLTOGETHER:

FUNCTION / STRUCTURE



ORTHOGONAL :

MEANS-ENDS / PART-WHOLE

Science of Computer Programming 8 (1987) 231–274
North-Holland

HIGRAPHS / STATECHARTS

inspiration

STATECHARTS: A VISUAL FORMALISM FOR COMPLEX SYSTEMS*

David HAREL
Department of Applied Mathematics, The Weizmann Institute of Science, Rehovot, Israel

Communicated by A. Pnueli
Received December 1984
Revised July 1986

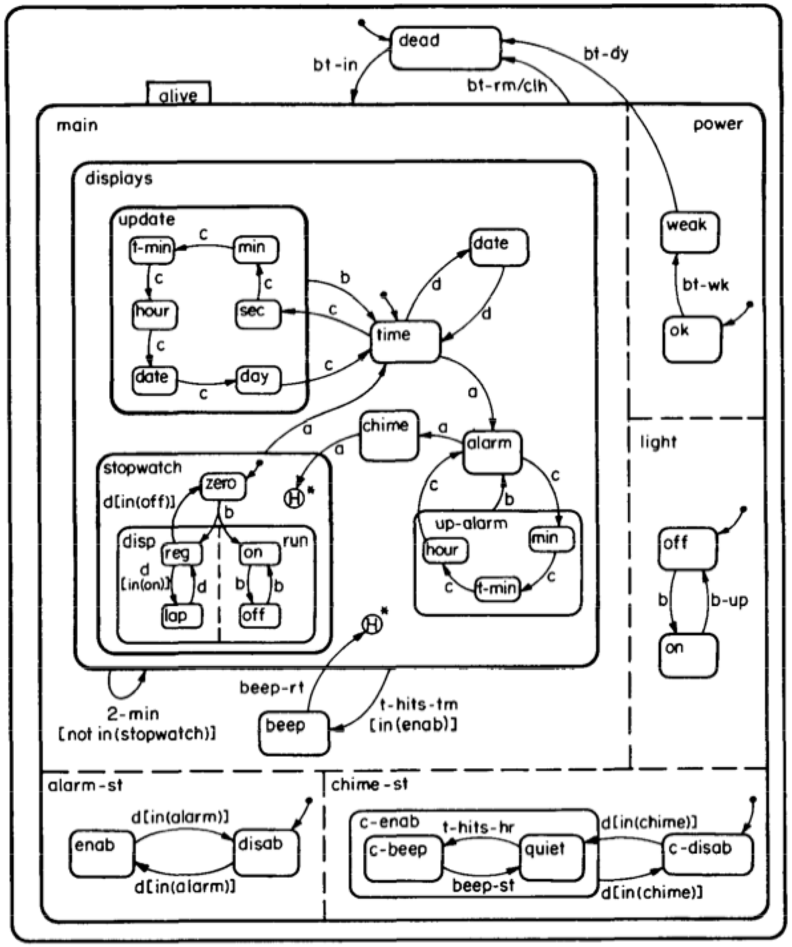
Abstract. We present a broad extension of the conventional formalism of state machines and state diagrams, that is relevant to the specification and design of complex discrete-event systems, such as multi-computer real-time systems, communication protocols and digital control units. Our diagrams, which we call *statecharts*, extend conventional state-transition diagrams with essentially three elements, dealing, respectively, with the notions of hierarchy, concurrency and communication. These transform the language of state diagrams into a highly structured and economical description language. Statecharts are thus compact and expressive—small diagrams can express complex behavior—as well as compositional and modular. When coupled with the capabilities of computerized graphics, statecharts enable viewing the description at different levels of detail, and make even very large specifications manageable and comprehensible. In fact, we intend to demonstrate here that statecharts counter many of the objections raised against conventional state diagrams, and thus appear to render specification by diagrams an attractive and plausible approach. Statecharts can be used either as a stand-alone behavioral description or as part of a more general design methodology that deals also with the system's other aspects, such as functional decomposition and data-flow specification. We also discuss some practical experience that was gained over the last three years in applying the statechart formalism to the specification of a particularly complex system.

1. Introduction

The literature on software and systems engineering is almost unanimous in recognizing the existence of a major problem in the specification and design of large and complex *reactive systems*. A reactive system (see [14]), in contrast with a *transformational system*, is characterized by being, to a large extent, event-driven, continuously having to react to external and internal stimuli. Examples include telephones, automobiles, communication networks, computer operating systems, missile and avionics systems, and the man-machine interface of many kinds of ordinary software. The problem is rooted in the difficulty of describing reactive behavior in ways that are clear and realistic, and at the same time formal and

* The initial part of this research was carried out while the author was consulting for the Research and Development Division of the Israel Aircraft Industries (IAI), Lod, Israel. Later stages were supported in part by grants from IAI and AD CAD, Ltd.

A DIGITAL WATCH



D-higraphs: The origin

DUALIZATION

Higraphs

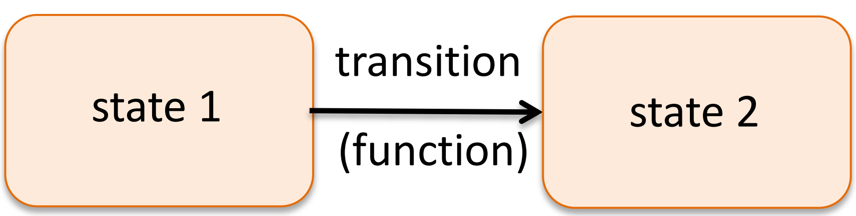
STATE CENTERED

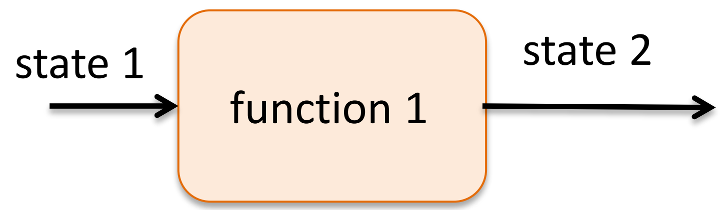
- Blobs: states
- Edges: transitions
- Exclusion: OR
- Orthogonality: AND

Required conditions

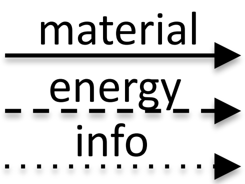
FUNCTION CENTERED

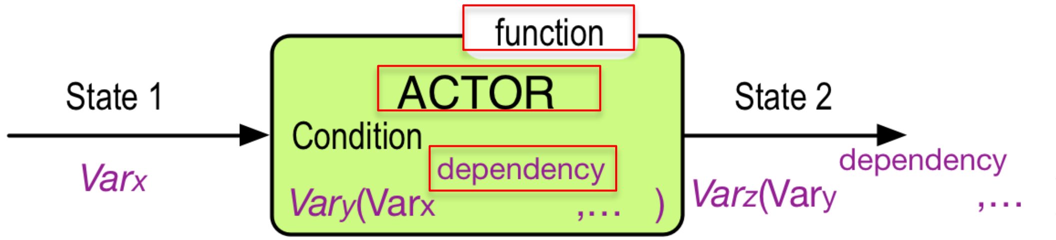
- Blobs: functions
- Edges: states
- Exclusion: AND
- Orthogonality: OR





D-higraphs: Elements & Properties



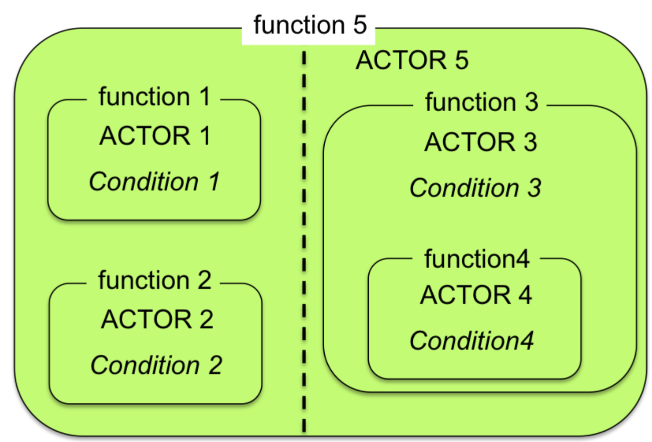


SYSTEMS' VIEW DESCRIPTION

Structural description: variables that characterize the system. Flow(F), temperature (T), Level (L),etc. Used by D-higraphs

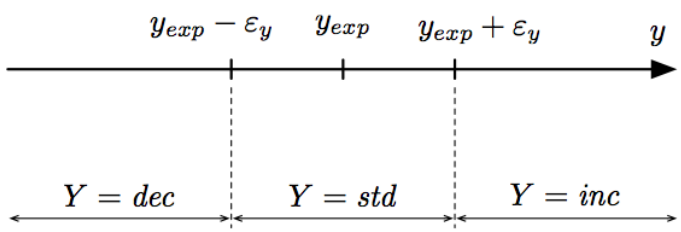
Behavioral description: Potential behavior of the system as a network.

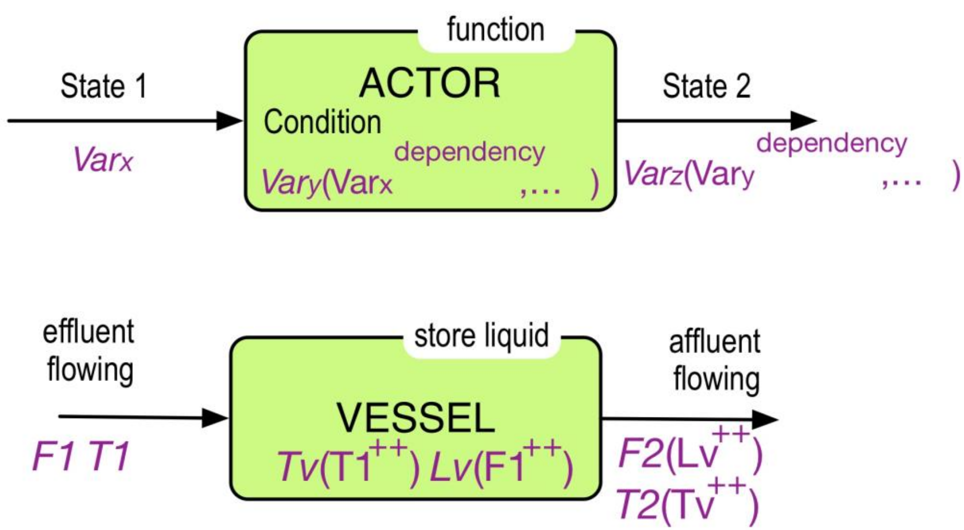
Functional description: Purpose of a structural component of connections. Provided by the D-higraph layout.

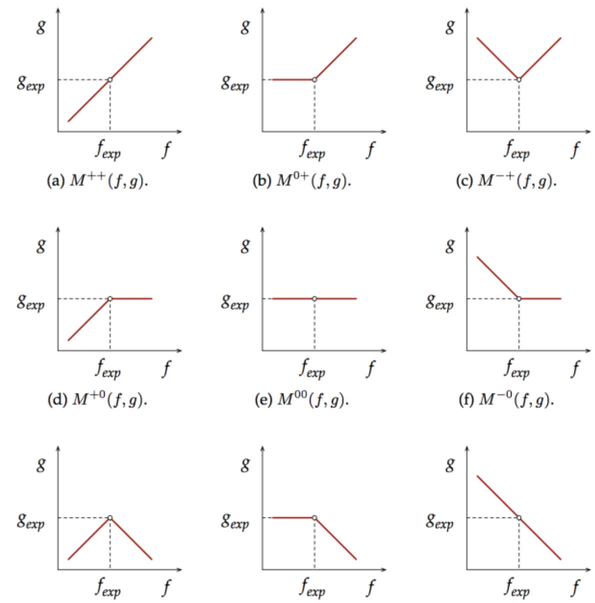


Properties: Inclusion, exclusion and cartesian product

D-higraphs: Qualitative simulation





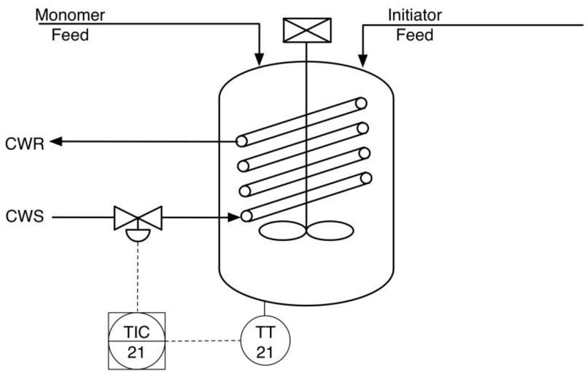


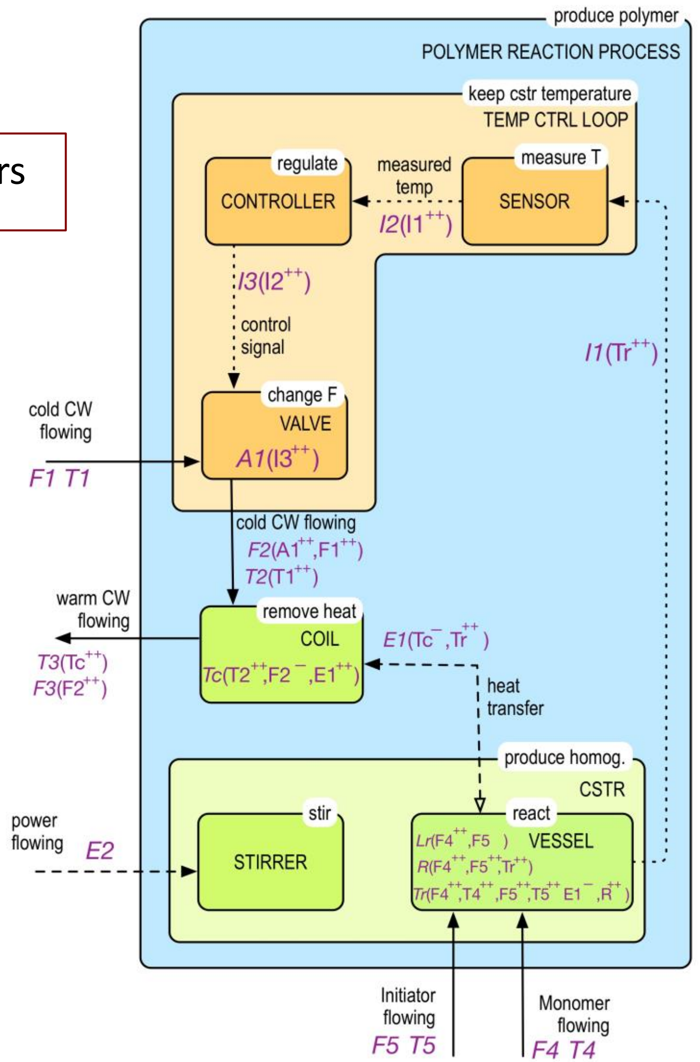
(a) $M^{++}(f,g)$. (b) $M^{0+}(f,g)$. (c) $M^{-+}(f,g)$.
(d) $M^{+0}(f,g)$. (e) $M^{00}(f,g)$. (f) $M^{-0}(f,g)$.
(g) $M^{+-}(f,g)$. (h) $M^{0-}(f,g)$. (i) $M^{--}(f,g)$.

D-higraphs & STPA

STPA generates huge tables:

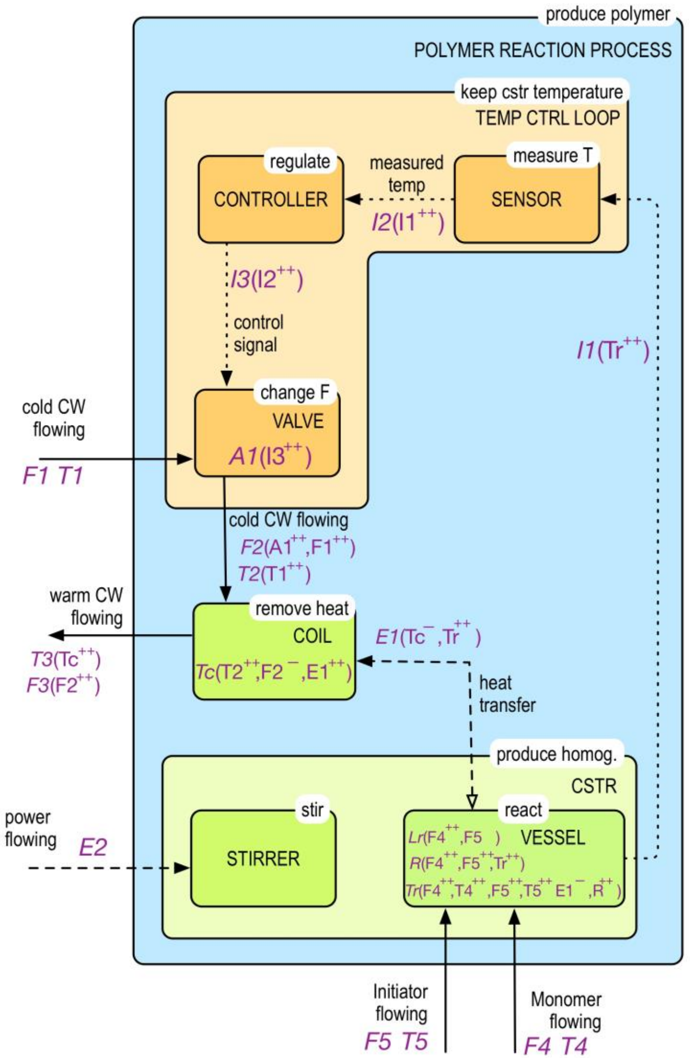
Controllers x UCAs x states^{ContextVars}





D-higraphs exploits the model to reduce the analysis

D-higraphs & STPA



STEPS:

1. Associate every hazard with a variable
   Hi(var_x)

1. See var_x dependencies in D-higraphs
   $var\_x(var\_i^{++},var\_j^{-+},var\_k^{++})$

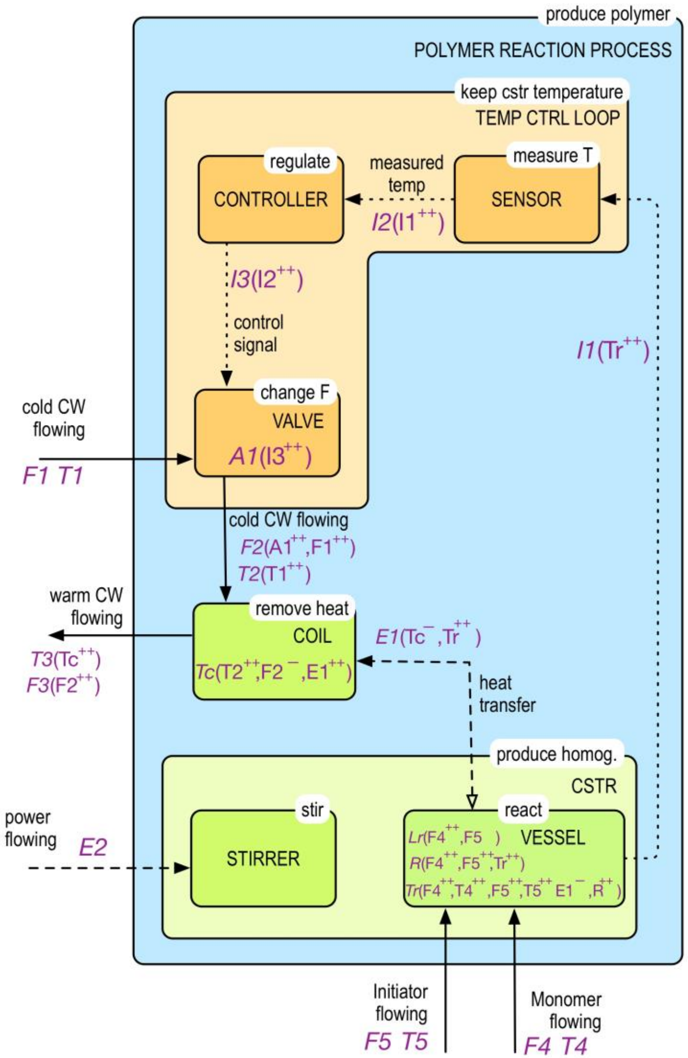
3. Identify which of the variables is a CA (var_j)

4. Apply UCAs scenarios
   CA: var_j
   Context var_i, var_k

5. Identify non hazardous contexts →
   → potential solutions

6. Rank safe contexts

D-higraphs & STPA



D-higraphs can also help in STPA step 4:

Determine how each hazardous control action could occurr.

D-higraphs allows for

root cause & consequence analysis.

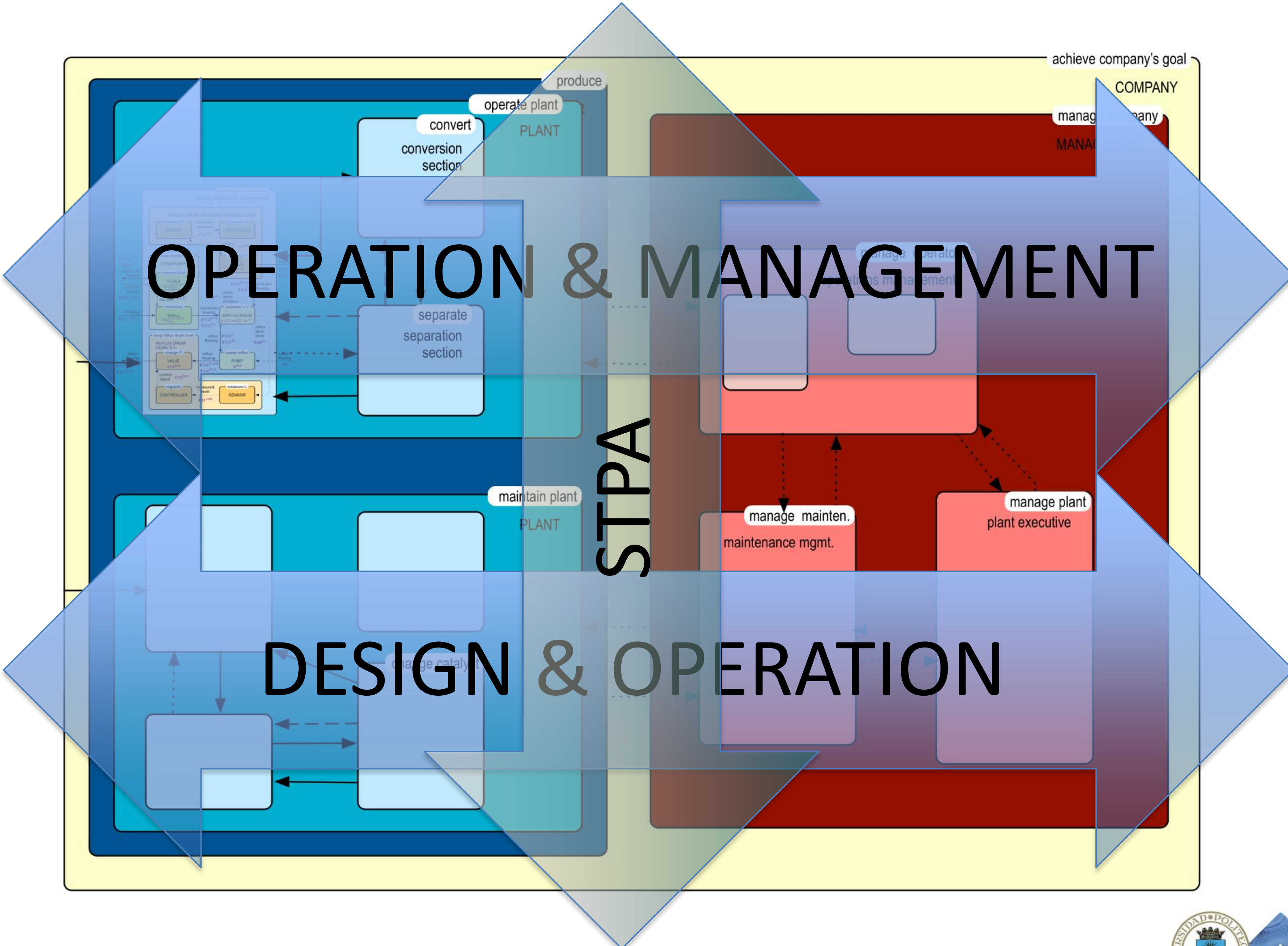
Remarks

- Presentation focused on the low level of the architecture

  Upper levels are similar to other domains
  Functional modeling can represent the architecture (abstraction & hierarchy)

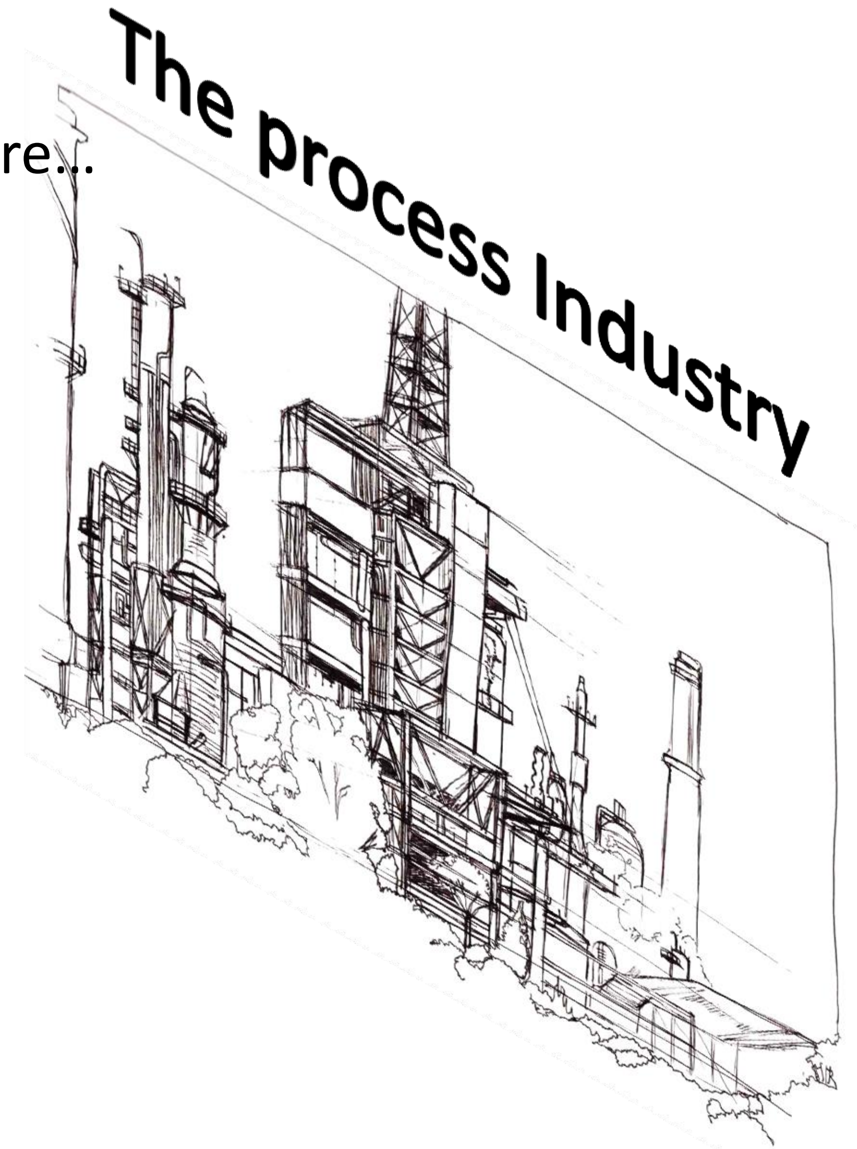
- STPA for the process industry needs knowledge to avoid huge tables

- D-higraphs (easy) extension to include humans (as controllers)


OPERATION & MANAGEMENT
STPA
DESIGN & OPERATION
achieve company's goal
COMPANY
produce
operate plant
PLANT
convert
conversion section
separate
separation section
maintain plant
PLANT
manage mainten.
maintenance mgmt.
manage plant
plant executive

Conclusion

You have a very promising future…
But you're still young.
Come back in a few years



aslab.org

manuel.rodriguezh@upm.es