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
AS REQUESTED, I DID A "RISK MANAGEMENT" ASSESSMENT.

I CONCLUDED THAT THERE WAS NO RISK OF ANY MANAGEMENT.

DO YOU HAVE ANYTHING TO ADD?

I'LL GET BACK TO YOU.
OF COURSE WE WERE AWARE OF THE RISK.

THAT IS WHY WE DID A VERY CAREFUL ANALYSIS OF WHO WOULD GET THE BLAME.
Hey listen... I sell STPAs
It’s good for your business

Sorry!, We’ve already got HAZOPs...
I know.... But look!
Eight workers mill explosion
Ghaziabad | March 14, 2014

Fertiliser plant EXPLODES in Sarawak town, 8 workers rescued

Summary
The explosion at the mill carried out in the early hours of 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

The eight have been identified as Sahil, Chandradev Yadav, Ravindra, impact on fulfilling existing Ram Nivas, Jamaluddin, Tilakram, Sunil and Gurwinder Singh.

*y compruébalo ahora

EL ÁRTICO SE DERRITE
Firma y pide que el Polo Norte sea declarado Santuario Global.

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

The eight have been identified as Sahil, Chandradev Yadav, Ravindra, impact on fulfilling existing Ram Nivas, Jamaluddin, Tilakram, Sunil and Gurwinder Singh.

*y compruébalo ahora

EL ÁRTICO SE DERRITE
Firma y pide que el Polo Norte sea declarado Santuario Global.
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

1. Conceptual Stage
2. Basic Engineering
3. FEED (Front End Engineering Design)
4. EPC
   - Engineering (detailed)
   - Procurement
   - Construction
5. (Commissioning & Startup)
The Safety Process

1. Establish context & Process Info
   - Stakeholders

2. Identify Hazards
   - Risk Classes

3. Risk analysis & assessment
   - Analysis methods
   - Likelihood & Consequences

4. 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

ANALYSIS
- Hazard and Risk Assessment
- Allocation of Safety Functions to Protection Layers
- Safety Requirements Specifications for the SIS

IMPLEMENTATION
- Design and Engineering of Safety Instrumented System
- Design and Development of Other Means of Risk Reduction
- Installation, Commissioning and Validation

OPERATION
- Operation and Maintenance
- Modification
- Decommissioning
Safety Lifecycle Closed Loop
Hazards studies

1. Hazards types identification
2. Preliminary Hazard Analysis
3. Analysis Methods & Evaluation
# Preliminary PHA example

<table>
<thead>
<tr>
<th>Hazardous Event/Situation</th>
<th>Prompts</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>External fire</strong></td>
<td></td>
</tr>
<tr>
<td>Fuel</td>
<td>Flammable gas, vapour, solid, metal, wood, waste material, pyrophoric material</td>
</tr>
<tr>
<td>Release mechanism</td>
<td>LOC, poor housekeeping</td>
</tr>
<tr>
<td>Ignition</td>
<td>Sparks, flares, static, friction, vehicles, hot spots, welding, lightning, auto-ignition, furnaces</td>
</tr>
<tr>
<td><strong>Internal fire</strong></td>
<td></td>
</tr>
<tr>
<td>(in equipment)</td>
<td></td>
</tr>
<tr>
<td>Flammable mixture</td>
<td>Flammable gas, vapour, liquid, solid, metal, dust, residue, pyrophoric material, oxygen, halogen</td>
</tr>
<tr>
<td>Ignition</td>
<td>Sparks, static, friction, welding, decomposition</td>
</tr>
<tr>
<td><strong>Internal explosion</strong></td>
<td></td>
</tr>
<tr>
<td>(in equipment)</td>
<td></td>
</tr>
<tr>
<td>Physical over pressure</td>
<td>LOC (Burst-Physical overpressure), head pressure, liquid filling, testing, purging</td>
</tr>
<tr>
<td>Uncontrolled reaction</td>
<td>Runaway reaction, decomposition, polymerization, contamination</td>
</tr>
<tr>
<td>Flammable mixture</td>
<td>Flammable gas, vapour, liquid, solid, dust, mist, oxygen, halogen, NC$_{13}$ explosive/ unstable compound, polymerization, loss of ignition/re-ignition</td>
</tr>
<tr>
<td>Ignition</td>
<td>Sparks, static, friction, hot spots, welding, decomposition</td>
</tr>
</tbody>
</table>

**Hazardous event/situation**

<table>
<thead>
<tr>
<th><strong>Immediate consequences</strong></th>
<th><strong>Ultimate consequences</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Chronic harmful/noxious exposure</td>
<td>B, D, M</td>
</tr>
<tr>
<td>Pollution</td>
<td>H, I, J, K, L</td>
</tr>
<tr>
<td>Violent release of energy</td>
<td>A, E, F, G, J, K, M</td>
</tr>
<tr>
<td>Noise</td>
<td>J, K</td>
</tr>
<tr>
<td>Visual impact</td>
<td>J, K</td>
</tr>
<tr>
<td>Nuisance/annoyance to public</td>
<td>F, G</td>
</tr>
<tr>
<td>Direct damage, consequential loss</td>
<td></td>
</tr>
</tbody>
</table>

**Code**

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

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

DESIGN INTENTION

DEVIAION

ELEMENT + GUIDEWORD (PARAMETER/CHELAKTERISTIC)

MIXING
PHASE
LEVEL
TEMP.
PRESSURE
COMPOSITION
FLOW
REACTION
COMM

[NOT ALL DEVIATIONS FEASIBLE]
DIRECT CAUSALITY

CAUSES

CONSEQUENCES

SAFEGUARDS

RECOMMENDATIONS/ACTIONS

ALARMS/SIS

NO / NONE
MORE
LESS
AS WELL AS
PART OF
REVERSE
OTHER THAN
------------------
WHERE ELSE
BEFORE / AFTER
EARLY / LATE
FASTER / SLOWER
The Result: Layers of Protection

- Emergency Plans
- Fire & gas
- Flare & Scrubber
- SIS
- Alarm
- BPCS
- Processes

Prevention

Mitigation
Nice!. Let me show you something....
Accidents causes

Causes of Process Upsets
- Human error: 40%
- Equipment failure: 20%
- Other: 40%

Source: ASM Consortium

Causes of Equipment Failure
- Operating out of range: 76%
- Improper design: 5%
- Improper maintenance: 5%
- No defect found: 10%
- Improper installation: 2%
- Improper material: 2%

Presented by N Kosaric at 2005 Defect Elimination Conference
Accidents causes
(SIS layer)

- 44% Specifications
- 15% Design and implementations
- 15% Installations and commissioning
- 15% Operations and maintenance
- 20% Changes after commissioning
“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!
1. ESTABLISH SYSTEM ENGINEERING FOUNDATION

FUNCTIONAL CONTROL STRUCTURE

2. IDENTIFY UNSAFE CONTROL ACTIONS (UCAs)

HAZARDS TYPES
HAZID

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

<table>
<thead>
<tr>
<th>Process Variables: Context</th>
<th>System state</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fmonomer</td>
<td>Finitiator</td>
</tr>
<tr>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>+</td>
<td>D</td>
</tr>
<tr>
<td>+</td>
<td>N</td>
</tr>
<tr>
<td>N</td>
<td>+</td>
</tr>
<tr>
<td>D</td>
<td>+</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Accident</th>
<th>Hazard</th>
<th>Safety Constraint</th>
</tr>
</thead>
<tbody>
<tr>
<td>Explosion</td>
<td>H1: Temperature too high</td>
<td>Temperature must never violate maximum value</td>
</tr>
<tr>
<td></td>
<td>H2: Pressure too high</td>
<td>Pressure must never violate maximum value</td>
</tr>
<tr>
<td>Leakage</td>
<td>H3: Level too high</td>
<td>Level must never violate maximum value</td>
</tr>
</tbody>
</table>
**Source Controller:** Open level control valve. **Type:** Not Provided

<table>
<thead>
<tr>
<th>ID</th>
<th>Fcw</th>
<th>Fgas</th>
<th>F1</th>
<th>F2</th>
<th>Hazard</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>H1, H2, H3</td>
</tr>
<tr>
<td>2</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>-</td>
<td>H2, H3</td>
</tr>
<tr>
<td>3</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>N</td>
<td>H2</td>
</tr>
<tr>
<td>4</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>D</td>
<td>H2, H3</td>
</tr>
<tr>
<td>5</td>
<td>+</td>
<td>+</td>
<td>-</td>
<td>+</td>
<td>H3</td>
</tr>
<tr>
<td>6</td>
<td>+</td>
<td>+</td>
<td>-</td>
<td>-</td>
<td>H3</td>
</tr>
<tr>
<td>7</td>
<td>+</td>
<td>+</td>
<td>-</td>
<td>N</td>
<td>--</td>
</tr>
<tr>
<td>8</td>
<td>+</td>
<td>+</td>
<td>-</td>
<td>D</td>
<td>H3</td>
</tr>
<tr>
<td>9</td>
<td>+</td>
<td>+</td>
<td>N</td>
<td>+</td>
<td>H3</td>
</tr>
<tr>
<td>10</td>
<td>+</td>
<td>+</td>
<td>N</td>
<td>-</td>
<td>H3</td>
</tr>
<tr>
<td>11</td>
<td>+</td>
<td>+</td>
<td>N</td>
<td>N</td>
<td>--</td>
</tr>
<tr>
<td>12</td>
<td>+</td>
<td>+</td>
<td>N</td>
<td>D</td>
<td>H3</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>252</td>
<td>D</td>
<td>D</td>
<td>N</td>
<td>D</td>
<td>H3</td>
</tr>
<tr>
<td>253</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>+</td>
<td>H3</td>
</tr>
<tr>
<td>254</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>-</td>
<td>H3</td>
</tr>
<tr>
<td>255</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>N</td>
<td>--</td>
</tr>
<tr>
<td>256</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>H3</td>
</tr>
</tbody>
</table>

**States considered:**
- Desired (D)
- More (+)
- Less (-)
- No / none (N)

Long tables
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 unnecessary 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
ORTHOGNONAL:

MEANS-ENDS / PART-WHOLE

ALLTOGETHER:

FUNCTION / STRUCTURE

motivation
STATECHARTS: A VISUAL FORMALISM FOR COMPLEX SYSTEMS*

David HAREL

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.
D-higraphs: The origin

Higraphs

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

DUALIZATION

Required conditions

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

STATE CENTERED

function 1

state 1  transition  function 1  state 2
(State)

FUNCTION CENTERED

state 1  state 2
(Function)
**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

\[ y_{exp} - \varepsilon_y \quad y_{exp} \quad y_{exp} + \varepsilon_y \quad y \]

\[ Y = \text{dec} \quad Y = \text{std} \quad Y = \text{inc} \]

**Actor**
- Condition: \( \text{Var}_{x} \)
- Function: \( \text{Var}(\text{Var}_{x}, \ldots) \)

**Vessel**
- State 1: \( \text{State 1} \) \( \text{Var}_{x} \)
- State 2: \( \text{State 2} \) \( \text{Var}(\text{Var}_{x}, \ldots) \)
- Flow: \( \text{Effluent flowing} \)
- Store liquid: \( \text{F1 T1} \)
- Affluent flowing: \( \text{F2 (Lv)} \text{ (Tv)} \)

\( \text{Var}_{x} \) \( \text{Var}(\text{Var}_{x}, \ldots) \)
D-higraphs & STPA

STPA generates huge tables:

Controllers x UCAs x states

D-higraphs exploits the model to reduce the analysis
D-higraphs & STPA

### STEPS:

1. Associate every hazard with a variable $Hi(\text{var}_x)$

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

3. Identify which of the variables is a CA ($\text{var}_j$)

4. Apply UCAs scenarios
   - CA: $\text{var}_j$
   - Context $\text{var}_i, \text{var}_k$

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 occur.

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)
Conclusion

You have a very promising future...
But you’re still young.
Come back in a few years
aslab.org

manuel.rodriguezh@upm.es