A Different Look at the Entire Accident / Disaster Cycle affecting Safety of Complex Sociotechnical Systems by Using STAMP

Daniel Hartmann, PhD
Management & Safety Engineering Unit, Ben-Gurion University, Israel
Outline

• Motivation

• Harmonizing...

• Accident / Disaster Cycle

• Some thoughts about Sociotechnical Systems,

Accident / Disaster Cycle & STAMP
<table>
<thead>
<tr>
<th>S-T System Levels</th>
<th>Loop Number</th>
<th>Official Results</th>
<th>CAST Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>State – Regulation</td>
<td>1, 2, 3</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>State – Professional</td>
<td>4, 5, 6, 7, 8, 9</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>Regulation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>External Institutions</td>
<td>10, 11, 12</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>Management &amp; Operation</td>
<td>13</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Physical Level</td>
<td>2</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td><strong>Total Results</strong></td>
<td>7</td>
<td>21</td>
<td></td>
</tr>
<tr>
<td><strong>Total in %</strong></td>
<td>100%</td>
<td>300%</td>
<td></td>
</tr>
</tbody>
</table>
## Anacortes Accident: CSB & CAST Investigations Results

<table>
<thead>
<tr>
<th>S-T System Levels</th>
<th>Loop Number</th>
<th>CSB Results</th>
<th>CAST Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Federal – Regulation</td>
<td>1</td>
<td>6</td>
<td>8</td>
</tr>
<tr>
<td>State – Regulation</td>
<td>2, 3, 4, 5</td>
<td>5</td>
<td>8</td>
</tr>
<tr>
<td>External Institutions</td>
<td>6, 7</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>External Experts</td>
<td>8, 9</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>Management &amp; Operation</td>
<td>10, 11</td>
<td>10</td>
<td>14</td>
</tr>
<tr>
<td>Physical Level</td>
<td></td>
<td>9</td>
<td>14</td>
</tr>
<tr>
<td>Total Results</td>
<td></td>
<td>32</td>
<td>50</td>
</tr>
<tr>
<td>Total in %</td>
<td></td>
<td>100%</td>
<td>156%</td>
</tr>
</tbody>
</table>
A very crude and bold Assumption

<table>
<thead>
<tr>
<th>New Socio-technological Systems</th>
<th>Old, well established Socio-technological Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt; 0.1 %</td>
<td>&gt; 99.9%</td>
</tr>
<tr>
<td>STPA needed, but...</td>
<td>STAMP not wanted as long as...</td>
</tr>
</tbody>
</table>
Outline

• Motivation

• Harmonizing...

• Accident / Disaster Cycle

• Some thoughts about Sociotechnical Systems,

Accident / Disaster Cycle & STAMP
A Normal Variability of Viewpoints...

So many thinkers with different views of the world.
Systems Engineering & DoD AF Viewpoint Structure

Dr. Daniel Hartmann 2016 © Fifth MIT STAMP/STPA Workshop
Definitions of Accident

• An undesired and unplanned event that results in a loss (including loss of human life or injury, property damage, environmental pollution, and so on).

• Loss [event] that is unacceptable to the stakeholders.

• An unexpected and undesirable event, especially one resulting in damage or harm.

• anything that occurs unintentionally or by chance

• a misfortune or mishap, esp. one causing injury or death.

• any event that happens unexpectedly, without a deliberate plan or cause
“Accidents”  Fragmented Worlds

Systems Engineering  STAMP / CAST

Validation & Verification  Design for Safety

Accidents [Investigation]
## STAMP & Systems Lifecycle

### Safety & Accidents

<table>
<thead>
<tr>
<th>System Development</th>
<th>Value Chain: From Cradle to Grave</th>
</tr>
</thead>
<tbody>
<tr>
<td>Concept</td>
<td>Build</td>
</tr>
<tr>
<td>Requirements</td>
<td>Design</td>
</tr>
</tbody>
</table>

**Accidents**

**System Operation**

**End of System**

Dr. Daniel Hartmann 2016 © Fifth MIT STAMP/STPA Workshop
Why do Accident* Analysis along the entire Value Chain?

- Loss that is unacceptable to the stakeholders
- Non accomplishment of the mission

Sociotechnical System as A Learning Organization

Incidents → Learning Curve

System → System Changes → Analysis → Accident → System

Dr. Daniel Hartmann 2016 © Fifth MIT STAMP/STPA Workshop
“Hidden” / Latent Accidents in Criminal Justice*

• The **Hidden Accidents principle** refers to reality in which accidents in **criminal law** — **false convictions** — tend to remain **concealed**. In contrast to aeronautics, for example, where an airplane crash is an open fact, **no one** — except the person accused, who is almost never believed — **ever knows or can know** that a defendant **has been wrongly convicted**. This enables legal decision-makers to optimistically **assume** the system is close to perfect, and makes it virtually impossible to prove otherwise.

• the Hidden Accidents Principle is what facilitates many optimists about the criminal justice system to compellingly claim that **false convictions never occur**, or else understate their frequency.

• Due to the Hidden Accidents Principle in criminal law, many people continue to have great faith in the system and are confident that the rate of false convictions is low. ... this is hardly the case.

* Boaz Sangero, Safety from False Convictions
This inability to detect wrongful decision is a highly significant feature of sociotechnical system, which we call the “Hidden Accident Principle.” This principle can be formulated as follows:

• A sociotechnical system is characterized by accidents (wrongful decision) that typically remain undetected. The inability to detect these accidents translates into optimism on the part of policymakers that false decision only occur at a negligible rate.

• In a reality in which wrongful decision go undetected, the sociotechnical system in fact receives no immediate feedback or a delayed feedback once the wrongful decision materializes and the hidden accident become visible as a tangible accident.

The higher we are in the Hierarchical Safety Control Structure, the more prominent the problem of wrongful decision is!
Another view of **Accidents Classification**

<table>
<thead>
<tr>
<th>Tangible</th>
<th>Nontangible</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>“Real” Accidents</strong></td>
<td><strong>“Hidden” Accidents</strong></td>
</tr>
<tr>
<td>Feedback loop accomplished</td>
<td>Feedback loop Not accomplished</td>
</tr>
</tbody>
</table>

Proximal Event

Systemic Event

Dr. Daniel Hartmann 2016 © Fifth MIT STAMP/STPA Workshop
“Rumsfeld’s Dilemma”

Information, knowledge is everything

The most important thing is what we don’t know

“BROCHURE VIEW”

KNOWN TO SELF & OTHERS

KNOWN ONLY TO OTHERS

NOT KNOWN to OTHERS

NOT KNOWN TO ANYONE

“BLIND SPOT”

“PROMISE OF INVENTION”

Dr. Daniel Hartmann 2016 © Fifth MIT STAMP/STPA Workshop
Learning Curve & “Knowledge”

Mistakes - Accidents

<table>
<thead>
<tr>
<th>Time</th>
<th>Known - Unknowns</th>
<th>Unknown - Knowns</th>
<th>Known - Knowns</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bonen 0-1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bonen 1-2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bonen 3-4</td>
<td>Modern / Immature Systems</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Traditional / Mature Systems

Dr. Daniel Hartmann 2016 © Fifth MIT STAMP/STPA Workshop
Performance = speed, availability, quality, productivity, profit, technology, reliability, safety, etc.
The “Real System” and a Socio-technical System

As a Learning System

Social - Cultural

Technical - Scientific

Learning

Survival

Learning

Survival

Environmental

Dr. Daniel Hartmann 2016 © Fifth MIT STAMP/STPA Workshop
Learning Socio-technical Systems, Safety & Survival Gap

Economic

Cultural & Paradigms

Survival Gap

Technical-Scientific

Human Yields

Environmental Negative Yields

Dr. Daniel Hartmann 2016 © Fifth MIT STAMP/STPA Workshop
STAMP, Sociotechnical Systems Lifecycle

Safety, Accidents & Disasters

Value Chain: From Cradle to Grave

System Development

Concept

Requirements

Design

Build

System Operation

Operation

End of System

Disposal

Accidents

Disasters

Dr. Daniel Hartmann 2016 © Fifth MIT STAMP/STPA Workshop
Definitions of Disaster

- a sudden event, such as an accident or a natural catastrophe, that causes great damage or loss of life.
- an event or fact that has unfortunate consequences.
- a serious disruption of the functioning of a community or a society involving widespread human, material, economic or environmental losses and impacts...
- A disaster is a sudden, calamitous event that seriously disrupts the functioning of a community or society and causes human, material, and economic or environmental losses that exceed the community’s or society’s ability to cope using its own resources.
Harmonizing “Different” Worlds

Accident = Disaster
Relationship between Accidents and Disasters

Dr. Daniel Hartmann 2016 © Fifth MIT STAMP/STPA Workshop
And another view of Classification of Accidents and Disasters

- Simple Disasters
  - Simple Accidents
  - Complex Accidents
- Complex Disasters

Time:
- Seconds
- Minutes
- Hours
- Days
- Weeks
- Months
- Years

Space:
- Simple
- Complex

Severity:
- Simple
- Complex

Dr. Daniel Hartmann 2016 © Fifth MIT STAMP/STPA Workshop
Hierarchical Sociotechnical Systems with Levels connected by Control Flows

System development stage

Regulators

Company management

Project management

Design

Implementation Construction

Maintenance

System operations stage

Regulators

Company management

Operations management

Operating process

Human controller

Automated controller

Sensor

Actuator

Physical process

Dr. Daniel Hartmann 2016 © Fifth MIT STAMP/STPA Workshop
Outline

• Motivation

• Harmonizing...

• Accident / Disaster Cycle

• Some thoughts about Sociotechnical Systems,

Accident / Disaster Cycle & STAMP
# Relationship between Accidents and Disasters

<table>
<thead>
<tr>
<th>Accidents</th>
<th>Disasters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Limited</td>
<td>Time Limited - Unlimited</td>
</tr>
<tr>
<td>Space Limited</td>
<td>Space Limited - Unlimited</td>
</tr>
<tr>
<td>Complexity Limited</td>
<td>Complexity Limited - Unlimited</td>
</tr>
<tr>
<td>Severity Limited</td>
<td>Severity Limited - Unlimited</td>
</tr>
</tbody>
</table>

**Simple Response** | **Complex Response**

---

Dr. Daniel Hartmann 2016 © Fifth MIT STAMP/STPA Workshop
Outline

• Motivation
• Harmonizing...
• Accident / Disaster Cycle
• Some thoughts about Sociotechnical Systems,

Accident / Disaster Cycle & STAMP
Sociotechnical Systems and Full Lifecycle [Development, Operation & Response]

- Process Facilities
- Airplanes
- Trains
- Cars
- Buildings

- Bridges
- Dames
- Technologies
- Pipelines
- Power Supply
<table>
<thead>
<tr>
<th>S-T System Development</th>
<th>S-T System Operation</th>
<th>S-T System Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legislation</td>
<td>Legislation</td>
<td>Legislation</td>
</tr>
<tr>
<td>Regulation</td>
<td>Regulation</td>
<td>Regulation</td>
</tr>
<tr>
<td>Corporate Management</td>
<td>Corporate Management</td>
<td>“Corporate” Management</td>
</tr>
<tr>
<td>Company Management</td>
<td>Company Management</td>
<td>“Company” Management</td>
</tr>
<tr>
<td>Project Management</td>
<td>Project Management</td>
<td>Project Management</td>
</tr>
<tr>
<td>Manufacturing Management</td>
<td>Operation Management</td>
<td>Operation Management</td>
</tr>
</tbody>
</table>

Dr. Daniel Hartmann 2016 © Fifth MIT STAMP/STPA Workshop
Theoretical Safety of Sociotechnical Systems

Pro-Active Approach

Hazard & Risk Mgmt.

STPA

Existing Rigid, Hardwired Systems

Existing Rigid long-lasting Regulations

Existing Rigid long-lasting Policies

DIKC Levels, Issues, Problems

Real Engineered Safety of Sociotechnical Systems

Re-Active Approach

Accident Investigation

CAST

Databases

Research

Case Studies

Dr. Daniel Hartmann 2016 © Fifth MIT STAMP/STPA Workshop