Systems Theoretic Process Analysis (STPA)
Systems approach to safety engineering (STAMP)

- Accidents are more than a chain of events, they involve complex dynamic processes.
- Treat accidents as a control problem, not just a failure problem.
- Prevent accidents by enforcing constraints on component behavior and interactions.
- Captures more causes of accidents:
  - Component failure accidents
  - Unsafe interactions among components
  - Complex human, software behavior
  - Design errors
  - Flawed requirements
    - esp. software-related accidents
STAMP: basic control loop

- Controllers use a **process model** to determine control actions
  - Accidents often occur when the process model is incorrect
- A good model of both software and human behavior in accidents
- Four types of **unsafe control actions**:
  1) Control commands required for safety are not given
  2) Unsafe ones are given
  3) Potentially safe commands but given too early, too late
  4) Control action stops too soon or applied too long
Using control theory

Using control theory

Using control theory

Example
Safety
Control
Structure

Accidents are caused by inadequate control
STAMP and STPA

How do we find inadequate control that caused an accident?

Accidents are caused by inadequate control

CAST
Accident Analysis

STAMP Model
STAMP and STPA

How do we find inadequate control in a design?

Accidents are caused by inadequate control.
STPA Hazard Analysis
STPA
(System-Theoretic Process Analysis)

- Identify accidents and hazards
- Draw the control structure
- Step 1: Identify unsafe control actions
- Step 2: Identify causal scenarios

Can capture requirements flaws, software errors, human errors

(Leveson, 2012)
Definitions

- Accident (Loss)
  - An undesired or unplanned event that results in a loss, including loss of human life or human injury, property damage, environmental pollution, mission loss, etc.

- Hazard
  - A system state or set of conditions that, together with a particular set of worst-case environment conditions, will lead to an accident (loss).
Definitions

- **System Accident (Loss)**
  - An undesired or unplanned event that results in a loss, including loss of human life or human injury, property damage, environmental pollution, mission loss, etc.
  - May involve environmental factors *outside our control*

- **System Hazard**
  - A system state or set of conditions that, together with a particular set of worst-case environment conditions, will lead to an accident (loss).
  - Something we can **control** in the design

<table>
<thead>
<tr>
<th>System Accident</th>
<th>System Hazard</th>
</tr>
</thead>
<tbody>
<tr>
<td>People die from exposure to toxic chemicals</td>
<td>Toxic chemicals from the plant are in the atmosphere</td>
</tr>
</tbody>
</table>
Definitions

• System Accident (Loss)
  – An undesired or unplanned event that results in a loss, including loss of human life or human injury, property damage, environmental pollution, mission loss, etc.
  – May involve environmental factors outside our control
• System Hazard
  – A system state or set of conditions that, together with a particular set of worst-case environment conditions, will lead to an accident (loss).
  – Something we can control in the design

<table>
<thead>
<tr>
<th>System Accident</th>
<th>System Hazard</th>
</tr>
</thead>
<tbody>
<tr>
<td>People die from exposure to toxic chemicals</td>
<td>Toxic chemicals from the plant are in the atmosphere</td>
</tr>
<tr>
<td>People die from radiation sickness</td>
<td>Nuclear power plant radioactive materials are not contained</td>
</tr>
<tr>
<td>Vehicle collides with another vehicle</td>
<td>Vehicles do not maintain safe distance from each other</td>
</tr>
<tr>
<td>People die from food poisoning</td>
<td>Food products for sale contain pathogens</td>
</tr>
</tbody>
</table>
Definitions

- System Accident (Loss)
  - An undesired or unplanned event that results in a loss, including loss of human life or human injury, property damage, environmental pollution, mission loss, etc.

- System Hazard
  - A system state or set of conditions that, together with a particular set of worst-case environment conditions, will lead to an accident (loss).
  - Something we can control in the design

<table>
<thead>
<tr>
<th>People die from radiation sickness</th>
<th>Nuclear power plant radioactive materials are not contained</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vehicle collides with another vehicle</td>
<td>Vehicles do not maintain safe distance from each other</td>
</tr>
<tr>
<td>People die from food poisoning</td>
<td>Food products for sale contain pathogens</td>
</tr>
</tbody>
</table>

Broad view of safety

“Accident” is anything that is unacceptable, that must be prevented.

Not limited to loss of life or human injury!
# System Safety Constraints

<table>
<thead>
<tr>
<th>System Hazard</th>
<th>System Safety Constraint</th>
</tr>
</thead>
<tbody>
<tr>
<td>Toxic chemicals from the plant are in the atmosphere</td>
<td>Toxic plant chemicals must not be released into the atmosphere</td>
</tr>
<tr>
<td>Nuclear power plant radioactive materials are not contained</td>
<td>Radioactive materials must not be released</td>
</tr>
<tr>
<td>Vehicles do not maintain safe distance from each other</td>
<td>Vehicles must always maintain safe distances from each other</td>
</tr>
<tr>
<td>Food products for sale contain pathogens</td>
<td>Food products with pathogens must not be sold</td>
</tr>
</tbody>
</table>

Additional hazards / constraints can be found in ESW p355
STPA
(System-Theoretic Process Analysis)

• Identify accidents and hazards
• Draw the control structure
• Step 1: Identify unsafe control actions
• Step 2: Identify causal scenarios

(Leveson, 2012)
Control Structure Examples
Proton Therapy Machine
High-level Control Structure

Gantry

Beam path and control elements
Proton Therapy Machine
High-level Control Structure
Proton Therapy Machine Control Structure

Figure 13 - Zooming into the Treatment Delivery group (D1)

Courtesy of MIT. Used with permission.
Adaptive Cruise Control
Example: ACC – BCM Control Loop

Courtesy of Qi D. Van Eikema Hommes. Used with permission.
An image of the explosion at the Bayer chemical plant in Institute, West Virginia removed due to copyright restrictions.
An image of the explosion at the Bayer chemical plant in Institute, West Virginia removed due to copyright restrictions.
U.S. pharmaceutical safety control structure

An image of the prescription drug Vioxx removed due to copyright restrictions.

Ballistic Missile Defense System

An image of the ballistic missile defense system removed due to copyright restrictions.

Image from:

Safeware Corporation
STPA
(System-Theoretic Process Analysis)

- Identify accidents and hazards
- Draw the control structure
- Step 1: Identify unsafe control actions
- Step 2: Identify causal factors and create scenarios

(Leveson, 2012)
STPA Step 1: Unsafe Control Actions (UCA)

Controller

Control Actions

Controlled process

Feedback

Control Action A

Table:

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
STPA Step 1: Unsafe Control Actions (UCA)

<table>
<thead>
<tr>
<th>(Control Action)</th>
<th>Not providing causes hazard</th>
<th>Providing causes hazard</th>
<th>Incorrect Timing/Order</th>
<th>Stopped Too Soon / Applied too long</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controller</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Controlled process</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Feedback
Step 1: Identify Unsafe Control Actions
(a more rigorous approach)

<table>
<thead>
<tr>
<th>Control Action</th>
<th>Process Model Variable 1</th>
<th>Process Model Variable 2</th>
<th>Process Model Variable 3</th>
<th>Hazardous?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
STPA
(System-Theoretic Process Analysis)

- Identify accidents and hazards
- Draw the control structure
- **Step 1**: Identify unsafe control actions
- **Step 2**: Identify causal scenarios

(Leveson, 2012)
STPA Step 2: Identify Control Flaws

- **Controller**
  - Inadequate Control Algorithm
    - (Flaws in creation, process changes, incorrect modification or adaptation)
  - Process Model
    - (inconsistent, incomplete, or incorrect)

- **Actuator**
  - Inadequate operation

- **Sensor**
  - Inadequate operation

- **Controlled Process**
  - Component failures
  - Changes over time
  - Unidentified or out-of-range disturbance
  - Process output contributes to system hazard

- **Missed Communication**
- **Controller**

- **Controller**

- **Controller**
  - Inadequate or missing feedback
  - Feedback delays

- **Controller**
  - Incorrect or no information provided
  - Measurement inaccuracies
  - Feedback delays

- **Controller**
  - Process input missing or wrong
  - Conflicting control actions

- **Controller**
  - Inadequate operation
  - Delayed operation

- **Controller**
  - Inappropriate, ineffective, or missing control action

- **Controller**

- **Controller**
  - Component failures
  - Changes over time
  - Unidentified or out-of-range disturbance
  - Process output contributes to system hazard

- **Controller**
  - Inadequate operation

- **Controller**
  - Inadequate operation

- **Controller**
  - Inadequate operation

- **Controller**
  - Inadequate operation

- **Controller**
  - Inadequate operation

- **Controller**
  - Inadequate operation

- **Controller**
  - Inadequate operation
STPA Examples
Chemical Reactor
Chemical Reactor Design

- Catalyst flows into reactor
- Chemical reaction generates heat
- Water and condenser provide cooling

What are the accidents, system hazards, system safety constraints?
STPA
(System-Theoretic Process Analysis)

- Identify accidents and hazards
- Draw the control structure
- Step 1: Identify unsafe control actions
- Step 2: Identify causal scenarios

(Leveson, 2012)
Chemical Reactor Design

• Catalyst flows into reactor
• Chemical reaction generates heat
• Water and condenser provide cooling

Create Control Structure
STPA Analysis

- High-level (simple) Control Structure
  - What are the main parts?
STPA Analysis

• High-level (simple) Control Structure
  – What commands are sent?
STPA Analysis

• High-level (simple) Control Structure
  – What feedback is received?

![Diagram showing STPA analysis process](chart.png)
Chemical Reactor Design

Control Structure:
STPA
(System-Theoretic Process Analysis)

- Identify accidents and hazards
- Draw the control structure
- Step 1: Identify unsafe control actions
- Step 2: Identify causal scenarios

(Leveson, 2012)
Chemical Reactor: Unsafe Control Actions

Control Structure:
### Chemical Reactor: Unsafe Control Actions

#### Control Structure:

<table>
<thead>
<tr>
<th></th>
<th>Not providing causes hazard</th>
<th>Providing causes hazard</th>
<th>Incorrect Timing/Order</th>
<th>Stopped Too Soon / Applied too long</th>
</tr>
</thead>
<tbody>
<tr>
<td>Close Water Valve</td>
<td>?</td>
<td>Computer closes water valve while catalyst open</td>
<td>?</td>
<td>?</td>
</tr>
</tbody>
</table>
Structure of an Unsafe Control Action

Example:
“Computer provides close water valve command when catalyst open”

Four parts of an unsafe control action
– Source Controller: the controller that can provide the control action
– Type: whether the control action was provided or not provided
– Control Action: the controller’s command that was provided / missing
– Context: conditions for the hazard to occur
  • (system or environmental state in which command is provided)
# Chemical Reactor: Unsafe Control Actions (UCA)

<table>
<thead>
<tr>
<th></th>
<th>Not providing causes hazard</th>
<th>Providing causes hazard</th>
<th>Incorrect Timing/Order</th>
<th>Stopped Too Soon / Applied too long</th>
</tr>
</thead>
<tbody>
<tr>
<td>Close Water Valve</td>
<td></td>
<td>Computer closes water valve while catalyst open</td>
<td>Computer closes water valve before catalyst closes</td>
<td></td>
</tr>
<tr>
<td>Open Water Valve</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Open Catalyst Valve</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Close Catalyst Valve</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Chemical Reactor: Unsafe Control Actions (UCA)

<table>
<thead>
<tr>
<th></th>
<th>Not providing causes hazard</th>
<th>Providing causes hazard</th>
<th>Incorrect Timing/Order</th>
<th>Stopped Too Soon / Applied too long</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Close Water Valve</strong></td>
<td></td>
<td>Computer closes water valve while catalyst open</td>
<td>Computer closes water valve before catalyst closes</td>
<td></td>
</tr>
<tr>
<td><strong>Open Water Valve</strong></td>
<td>Computer does not open water valve when catalyst open</td>
<td>Computer opens water valve more than X seconds after open catalyst</td>
<td>Computer stops opening water valve before it is fully opened</td>
<td></td>
</tr>
<tr>
<td><strong>Open Catalyst Valve</strong></td>
<td>Computer opens catalyst valve when water valve not open</td>
<td>Computer opens catalyst more than X seconds before open water</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Close Catalyst Valve</strong></td>
<td>Computer does not close catalyst when water closed</td>
<td>Computer closes catalyst more than X seconds after close water</td>
<td>Computer stops closing catalyst before it is fully closed</td>
<td></td>
</tr>
</tbody>
</table>
# Safety Constraints

<table>
<thead>
<tr>
<th>Unsafe Control Action</th>
<th>Safety Constraint</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer does not open water valve when catalyst valve open</td>
<td>Computer must open water valve whenever catalyst valve is open</td>
</tr>
<tr>
<td>Computer opens water valve more than X seconds after catalyst valve open</td>
<td>?</td>
</tr>
<tr>
<td>Computer closes water valve while catalyst valve open</td>
<td>?</td>
</tr>
<tr>
<td>Computer closes water valve before catalyst valve closes</td>
<td>?</td>
</tr>
<tr>
<td>Computer opens catalyst valve when water valve not open</td>
<td>?</td>
</tr>
<tr>
<td>Etc.</td>
<td>Etc.</td>
</tr>
</tbody>
</table>
## Safety Constraints

<table>
<thead>
<tr>
<th>Unsafe Control Action</th>
<th>Safety Constraint</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer does not open water valve when catalyst valve open</td>
<td>Computer must open water valve whenever catalyst valve is open</td>
</tr>
<tr>
<td>Computer opens water valve more than X seconds after catalyst valve open</td>
<td>Computer must open water valve within X seconds of catalyst valve open</td>
</tr>
<tr>
<td>Computer closes water valve while catalyst valve open</td>
<td>Computer must not close water valve while catalyst valve open</td>
</tr>
<tr>
<td>Computer closes water valve before catalyst valve closes</td>
<td>Computer must not close water valve before catalyst valve closes</td>
</tr>
<tr>
<td>Computer opens catalyst valve when water valve not open</td>
<td>Computer must not open catalyst valve when water valve not open</td>
</tr>
<tr>
<td>Etc.</td>
<td>Etc.</td>
</tr>
</tbody>
</table>
Traceability

• Always provide traceability information between UCAs and the hazards they cause.
  – Same for Safety Constraints and the hazards that result if violated.

• Two ways:
  – Create one UCA table (or safety constraint list) per hazard, label each table with the hazard
  – Create one UCA table for all hazards, include traceability info at the end of each UCA
    • E.g. Computer closes water valve while catalyst open [H-1]
STPA
(System-Theoretic Process Analysis)

- Identify accidents and hazards
- Draw the control structure
- Step 1: Identify unsafe control actions
- Step 2: Identify causal scenarios

(Leveson, 2012)
Step 2: Potential causes of UCAs

UCA: Computer opens catalyst valve when water valve not open

Inadequate Control Algorithm (Flaws in creation, process changes, incorrect modification or adaptation)

Process Model (inconsistent, incomplete, or incorrect)

Control input or external information wrong or missing

Missing or wrong communication with another controller

Inadequate or missing feedback

Feedback Delays

Inadequate operation

Inadequate operation

Incorrect or no information provided

Measurement inaccuracies

Feedback delays

Component failures

Changes over time

Unidentified or out-of-range disturbance

Process output contributes to system hazard

Controller

Actuator

Sensor

Controller

Controlled Process

Controller

Process input missing or wrong

Conflicting control actions

Delayed operation

Inadequate operation

Process output contributes to system hazard
Step 2: Potential control actions not followed

- **Controller**
  - Inadequate Control Algorithm (Flaws in creation, process changes, incorrect modification or adaptation)
  - Control input or external information wrong or missing
  - Missing or wrong communication with another controller

- **Actuator**
  - Inadequate operation
  - Delayed operation

- **Sensor**
  - Inadequate operation
  - Incorrect or no information provided
  - Measurement inaccuracies
  - Feedback delays

- **Controlled Process**
  - Component failures
  - Changes over time
  - Unidentified or out-of-range disturbance
  - Process output contributes to system hazard

- **Open water valve**

- **Controller**
  - Process input missing or wrong
  - Conflicting control actions

- **Controller**
  - Inadequate operation
  - Feedback Delays

- **Controller**
  - Inadequate operation
  - Feedback Delays
Chemical Reactor: Real accident
16.63J / ESD.03J System Safety
Spring 2016

For information about citing these materials or our Terms of Use, visit: https://ocw.mit.edu/terms.