STPA Intro
Dr. John Thomas

Any questions? Email me! JThomas4@mit.edu
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 Model
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

Can capture software errors, human errors, flawed requirements,...
Example
Safety Control Structure

SYSTEM DEVELOPMENT

Congress and Legislatures
Legislation
Government Reports
Lobbying
Hearings and open meetings
Accidents

Government Regulatory Agencies
Industry Associations, User Associations, Unions, Insurance Companies, Courts

Regulations
Standards
Certification
Legal penalties
Case Law

Company Management
Safety Policy
Standards
Resources

Policy, stds.

Project Management
Safety Standards
Hazard Analyses
Progress Reports

Operational Analyses
Safety-Related Changes
Progress Reports

Design, Documentation
Safety Constraints
Standards
Test Requirements

Test reports
Hazard Analyses
Review Results

Implementation and assurance
Hazard Analyses
Documentation
Design Rationale

Manufacturing Management

Work Procedures
Safety reports
Audits
Work logs
Inspections

Manufacturing

Maintenance and Evolution
Problem Reports
Incidents
Change Requests
Performance Audits

SYSTEM OPERATIONS

Congress and Legislatures
Legislation
Government Reports
Lobbying
Hearings and open meetings
Accidents

Government Regulatory Agencies
Industry Associations, User Associations, Unions, Insurance Companies, Courts

Regulations
Standards
Certification
Legal penalties
Case Law

Company Management
Safety Policy
Standards
Resources

Operations Management
Work Instructions

Operating Process
Human Controller(s)
Automated Controller
Actuator(s)
Sensor(s)
Physical Process

Change requests
Audit reports
Problem reports

(Leveson, 2012)
STAMP and STPA

Accidents are caused by inadequate control

(Leveson, 2012)
Accidents are caused by inadequate control.

How do we find inadequate control that caused the accident?

Accidents are caused by inadequate control.

CAST
Accident Analysis

STAMP Model

(Leveson, 2012)
Accidents are caused by inadequate control

How do we find inadequate control in a design?

Accidents are caused by inadequate control

CAST Accident Analysis

STPA Hazard Analysis

STAMP Model

(Leveson, 2012)
STPA: Systems Theoretic Process Analysis
STPA
(System-Theoretic Process Analysis)

- System engineering foundation
  - Define accidents, system hazards
  - Control structure

- Step 1: Identify unsafe control actions

- Step 2: Identify accident causal scenarios
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 from Engineering a Safer World
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.
  – May involve environmental factors outside our control

• 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>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>
# 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>
Aviation Examples

• Accidents
  – A-1: Two aircraft collide
  – A-2: Aircraft crashes into terrain / ocean

• System-level Hazards
  – H-1: Two aircraft violate minimum separation
  – H-2: Aircraft enters unsafe atmospheric region
  – H-3: Aircraft enters uncontrolled state
  – H-4: Aircraft enters unsafe attitude
  – H-5: Aircraft enters prohibited area
STPA
(System-Theoretic Process Analysis)

• System engineering foundation
  – Define accidents, system hazards
  – Control structure
• Step 1: Identify unsafe control actions
• Step 2: Identify accident causal scenarios
Control Structure Examples
Example Control Structure

(System Development)

Congress and Legislatures
Legislation

Government Regulatory Agencies
Industry Associations, User Associations, Unions, Insurance Companies, Courts

Company Management
Safety Policy
Standards
Resources

Policy, stds.

Project Management
Safety Standards

Design, Documentation
Safety Constraints
Standards
Test Requirements

Implementation and assurance
Safety Reports

Manufacturing Management
Work Procedures

Maintenance and Evolution

(System Operations)

Congress and Legislatures
Legislation

Government Reports
Lobbying
Hearings and open meetings
Accidents

Company Management
Safety Policy
Standards
Resources

Policy, stds.

Operations Management
Work Instructions

Operating Process
Hazard Analyses
Safety-Related Changes
Progress Reports

Operating Assumptions
Operating Procedures

Revised operating procedures

Problem Reports
Incidents
Change Requests
Performance Audits

Human Controller(s)

Automated Controller

Actuator(s)

Sensor(s)

Physical Process

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

Gantry
Beam path and control elements

Cyclotron
Proton Therapy Machine
High-level Control Structure

Figure 11 - High-level functional description of the PROSCAN facility (D0)
Proton Therapy Machine Control Structure

Figure 13 - Zooming into the Treatment Delivery group (D1)
Proton Therapy Machine Detailed Control Structure

Ballistic Missile Defense System


Safeware Corporation
Adaptive Cruise Control
U.S. pharmaceutical safety control structure

(a purely human/organizational system)


Leveson, Couturier, Thomas, Dierks, Wierz, Psaty, Finkelstein, Applying System Engineering to Pharmaceutical Safety
Automotive Shift By Wire

• The shift-by-wire concept replaces mechanical cables between the shifter and the transmission with an electronic lever, a computer, and electronic actuators. The computer senses the shift lever position and commands the actuator to achieve the appropriate transmission range.

Your turn: Control structure?
Control structure: Initial Concept

*Similar for both mechanical/electrical implementations*
Control Structure: Refined

Application of STPA to a Shift by Wire System, STPA workshop 2014
STPA
(System-Theoretic Process Analysis)

- System engineering foundation
  - Define accidents, hazards, constraints
  - Control structure

- Step 1: Identify unsafe control actions
- Step 2: Identify accident causal scenarios
STPA Step 1: Unsafe Control Actions (UCA)

4 ways unsafe control may occur:
- A control action required for safety is not provided or is not followed
- An unsafe control action is provided that leads to a hazard
- A potentially safe control action provided too late, too early, or out of sequence
- A safe control action is stopped too soon or applied too long (for a continuous or non-discrete control action)

<table>
<thead>
<tr>
<th>Shifter Command</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></td>
<td>?</td>
<td>?</td>
<td>?</td>
<td>?</td>
</tr>
</tbody>
</table>
Structure of an Unsafe Control Action

Example:
“Driver provides Park cmd while driving at speed (propulsion needed)”

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)
### UCAs → Safety Constraints

<table>
<thead>
<tr>
<th>Unsafe Control Action</th>
<th>Safety Constraint</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
STPA
(System-Theoretic Process Analysis)

- System engineering foundation
  - Define accidents, hazards, constraints
  - Control structure

- Step 1: Identify unsafe control actions
- Step 2: Identify accident causal scenarios
STPA Step 2: Identify Causal Scenarios

• Select an Unsafe Control Action
  A. Identify what might cause it to happen
     – Develop accident scenarios
     – Identify controls and mitigations
  B. Identify how control actions may not be followed or executed properly
     – Develop causal accident scenarios
     – Identify controls and mitigations
Step 2A: Potential causes of UCAs

- **UCA: Shift Control Module provides range command without driver new range selection**

  **Controller**
  - Inadequate Procedures (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

  **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

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

©
STPA Step 2: Identify Causal Scenarios

- Select an Unsafe Control Action
  
  A. Identify what might cause it to happen
     - Develop accident scenarios
     - Identify controls and mitigations
  
  B. Identify how control actions may not be followed or executed properly
     - Develop causal accident scenarios
     - Identify controls and mitigations
Step 2B: Potential control actions not followed

**Controller**
- Inadequate Procedures
  - (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

**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

**Controller**
- Step 2B: Potential control actions not followed

**Shift Control Module provides range command**

**Range is not engaged**
How does STPA compare?

- **MIT: TCAS**
  - Existing high quality fault tree done by MITRE for FAA
  - MIT comparison: STPA captured everything in fault tree, plus more
- **JAXA: HTV**
  - Existing fault tree reviewed by NASA
  - JAXA comparison: STPA captured everything in fault tree, plus more
- **EPRI: HPCI/RCIC**
  - Existing fault tree & FMEA overlooked causes of real accident
  - EPRI comparison: Blind study, only STPA found actual accident scenario
- **NRC: Power plant safety systems**
  - Proposed design that successfully completed Final Safety Analysis Report
  - STPA found additional issues that had not been considered
- **Safeware: U.S. Missile Defense Agency BMDS**
  - Existing hazard analysis per U.S. military standards
  - Safeware comparison: STPA captured existing causes plus more
  - STPA took 2 people 3 months, MDA took 6 months to fix problems
- **Automotive: EPS**
  - Compare STPA results to FMECA using SAE J1739
- **MIT: NextGen ITP**
  - Existing fault tree & event tree analysis by RTCA
  - MIT comparison: STPA captured everything in fault tree, plus more
- **MIT: Blood gas analyzer**
  - Existing FMEA found 75 accident causes
  - STPA by S.M. student found 175 accident causes
  - STPA took less effort, found 9 scenarios that led to FDA Class 1 recall