System-Theoretic Process Analysis for Security (STPA-SEC):
Cyber Security and STPA

William Young Jr, PhD
Reed Porada

2018 STAMP Conference
Boston, MA

March 26, 2018

© Copyright William Young, Jr, 2018
Disclaimer:

The views expressed in this presentation are those of the presenters and do not reflect the official policy or position of the United States Air Force, Department of Defense, Air Combat Command, MIT Lincoln Laboratory, Syracuse University, or the U.S. Government.
To Maximize the Available Time, I Will Assume Basic Familiarity With STPA an Will Leverage John Thomas’s Example from this Morning
Introduction
Before We Start, Please Tell Me

• Name

• Industry

• Experience level with STAMP/STPA/STPA-Sec

• What you hope to gain
Introduction (1/2)

• Losses are growing and current approaches to securing complex, software intense, designed physical systems do not appear to be working as well as desired

• Origins of losses fall into at least one of two categories:
  • Disruption prevents engineered system from fulfilling its designed purpose
  • Disruption does not necessarily prevent the engineered system from fulfilling its primary purpose, but it produces an unacceptable “by-product”

• The side with individuals best able to conceptualize the most creative ways to exploit device/design system functionality has competitive advantage (tactics)
Introduction (2/2)

• Security engineering and underlying systems thinking offers an alternative to address the challenge and bring strategy to bear

• Growing realization that security engineering must begin before architecture development...but we need a Security Engineering Analysis methodology
  • All analysis is based on models, so we require a model of how losses occur
  • Default model today is “threats cause our security-related losses” (but we don’t generally get to control the threats)

• STPA-Sec applies the STAMP model to provide a methodology to place security within a systems engineering context
  • Define “secure” functionality
  • Guide the development of an architecture to realize the functionality
  • We DO get to control our systems engineering

We Must Ensure That We Are Defining and Solving the Right (Engineering) Problem

© Copyright William Young, Jr, 2018
Definitions (1/3)

Security (US Gov’t, CNSSI 4009)-- A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise’s risk management approach.

Cybersecurity (US Gov’t & DoD)-- Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

Cyber Security is an Overarching Term that Covers Nearly Everything

© Copyright William Young, Jr, 2018
• **Security Engineering**—“An interdisciplinary approach and means to enable the realization of secure systems. It focuses on defining customer needs, security protection requirements, and required functionality early in the systems development lifecycle, documenting requirements, and then proceeding with design, synthesis, and system validation while considering the complete problem” (US Federal Gov’t)

• **Systems Security Engineering**—”a specialty discipline of systems engineering. It provides considerations for the security-oriented activities and tasks that produce security-oriented outcomes as part of every systems engineering process *activity* with focus given to the appropriate level of fidelity and rigor in analyses to achieve assurance and trustworthiness objectives. “ (NIST SP 800-160)
Definitions (3/3)

• Mission (US Military Doctrine) – “The task, together with the purpose, that clearly indicates the action to be taken and the reason therefore.”

• Business / Mission Analysis (INCOSE) – “defining the problem domain, identifying major stakeholders, identifying environmental conditions and constraints that bound the solution domain...and developing the business requirements and validation criteria”

• Hazard (US Military Doctrine) --“A condition with the potential to cause injury, illness, or death of personnel; damage to or loss of equipment or property; or mission degradation.”

• Security Control (NIST)-- A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.

• Mission Activity System- “A notional purposive system which expresses some purposeful human activity (a mission)” (Adapted from Checkland, 1984)
Defining the Security Problem in Terms of Threats Limits Our Thinking (and Solutions)

Based on Threat

Build This to be Secure

Function

Form

Problem Space - Abstract

Solution Space - Physical
Observations on Cybersecurity Today
The Cybersecurity Pen-Testing Challenge

Current Emphasis on Blue and Red Teaming is a Difficult Security Strategy
(Expensive, Too little, Too Late)

References: Boehm; Leveson; Frola & Miller; Fleming

© Copyright William Young, Jr, 2018
Schneier’s Attack Tree Model is the Intellectual Foundation of Most Thinking on Cybersecurity

“Clearly, what we need is a way to model threats against computer systems. If we can understand all the different ways in which a system can be attacked, we can likely design countermeasures to thwart those attacks...Security is not a product - it's a process. Attack trees form the basis of understanding that process.”

Schneier Based His Security Attack Trees on Fault Trees He Saw Used for Safety

© Copyright William Young, Jr, 2018
Current Security Analysis

“When you ask an engineer to make your boat go faster, you get the trade-space. You can get a bigger engine but give up some space in the bunk next to the engine room. You can change the hull shape, but that will affect your draw. You can give up some weight, but that will affect your stability. When you ask an engineer to make your system more secure, they pull out a pad and pencil and start making lists of bolt-on technology, then they tell you how much it is going to cost.”

- Prof Barry Horowitz, UVA
SYSTEM THINKING & SECURITY
The System Vulnerabilities are Driven by Threat Capability
Threat Based Approach to Developing a Secure Architecture

Current Security Analysis Depends on Identifying the Right Threat (Tactics), But Does Not Help Address the Larger Mission Assurance Goal (Strategy)

Ref: (Anderson, 2010; Shostack, 2014; Swiderski & Snyder, 2004)
Cyber Security Through Different Analytic Lenses

Vulnerability Analysis

Business/Mission System Vulnerability

Mission or Business Operations

Threat Analysis

Threat To System and Business/Mission

Impact Analysis

Alternative Approach based on Systems Engineering

In Systems Engineering, Threats are Just One of Many Trades

© Copyright William Young, Jr, 2018
New Approach: Secure Form Simply Realizes Secure Function

• “Form follows function” is a central tenant of system engineering and architecture

• Generate secure Business & Mission Systems by first defining the secure functionality to be realized

• Get to security via
  • Identify functionality required to solve the problem at hand (But we must understand problem)
  • Implement all required functionality securely based on understanding problem and context

• Architecture Defined (Crawley)
  • The embodiment of concept, and the allocation of physical/informational function to elements of form, and definition of interfaces among the elements and with the surrounding context

New Approach: Secure Form Simply Realizes Secure Function

• “Form follows function” is a central tenant of system engineering and architecture

• Generate secure Business & Mission Systems by first defining the secure functionality to be realized

• Get to security via
  • Identify functionality required to solve the problem at hand (But we must understand problem)
  • Implement all required functionality securely based on understanding problem and context

• Architecture Defined (Crawley)
  • The embodiment of concept, and the allocation of physical/informational function to elements of form, and definition of interfaces among the elements and with the surrounding context

© Copyright William Young, Jr, 2018
STAMP Model & Security

• Focuses on function, not threat to guide realization (form)
  • Separates problem space from solution
  • Allows us to reason about function (and critique a proposed functional decomposition based on security related concerns)
• Provides a means to define and specify secure function clearly, unambiguously, and in context of the mission
• Functional Control Structure is simply a means to help envision how the necessary functionality can be implemented in a way that prevents losses identified
STPA-Sec

• STAMP model allows us to create an analysis process to generate a security concept

• We want to examine a functional process for security to gain insights and craft a novel artifact or set of artifacts to realize our goal

• Threats are just another environmental hindrance to function
  • In fact, the threats themselves don’t really matter…it’s the functional disruption they can deliver
  • We can engineer our systems to handle the most important functional disruptions
STPA-Sec For Security Engineering Analysis

Chemical Reactor Example Based on John Thomas Example Used in Earlier STPA Tutorial. Example is Used With Dr Thomas’ Permission.
Chemical Reactor Design Through a Security Lens

From John Thomas’ Example this Morning

• Toxic catalyst flows into reactor
• Chemical reaction creates heat, pressure
• Water and condenser provide cooling

Additional Factors

• Plant is expected to be the primary source of local jobs
• Company is expected to employ proprietary technology
• Plant is expected to be the company’s crown jewel and has received a great deal of press attention

Adapted from Dr. Thomas’ STPA Tutorial
STPA-Sec Extends STPA

- Synthesize (frame) the security problem
- Define purpose of the analysis
- Model the Control Structure
- Identify unsafe/unsecure control actions
- Step 2: Identify loss scenarios
- Wargame
Synthesize (Frame) the Security Problem: Answering the “Why” Question
Big Picture: Synthesize (Frame) Security Problem

• Purpose is to set the foundation for the security analysis

• Must uncover / elicit unknown concerns

• Must ID all relevant stakeholders

• Must understand how product / service fits into organizational strategy

• Surface key assumptions

• Includes key aspects of Business or Mission Analysis (BMA) in ISO/IEEE/IEC 15288
Best Tactics and Tools Cannot Overcome a Flawed Strategy

The Maginot Line Remains an Incredible Engineered System, But Failed Operationally (Perfectly Solved the Wrong Problem)
By now we are all beginning to realize that one of the most intractable problems is that of defining problems (of knowing what distinguishes an observed condition from a desired condition) and of locating problems (finding where in the complex causal networks the trouble really lies). In turn, and equally intractable, is the problem of identifying the actions that might effectively narrow the gap between what-is and what-ought-to-be. "Dilemmas in a General Theory of Planning." Horst Rittel and Melvin Webber
The Security Problem is Not Generally Obvious or Easy to Specify

• Determining life cycle security concepts
• Defining security objectives
• Defining security requirements
• Determining measures of success

“Many systems fail because their designers protect the wrong things, or protect the right things in the wrong way” – Ross Anderson “Security Engineering”
Define Purpose and Goal

“A system to do {What = Purpose}
by means of {How = Method}
in order to contribute to {Why = Goals}
while {constraints, restraints}

Specify a gap between “as is” and “to be”
That will be addressed through a process (e.g. a transformation of some type)

What Might Be an Example from the Plant Example?
Define System Purpose and Goal

From John Thomas’ Example this Morning

• Toxic catalyst flows into reactor
• Chemical reaction creates heat, pressure
• Water and condenser provide cooling

Additional Factors

• Plant is expected to be the primary source of local jobs
• Company is expected to employ proprietary technology
• Plant is expected to be the company’s crown jewel and has received a great deal of press attention

Format

“A system to do {What = Purpose} by means of {How = Method} in order to contribute to {Why = Goals} while {constraints, restraints}”

What Might Be an Example from the Plant Example?
Chemical Reactor – Potential Solution

A system to contain and process chemicals by means of transferring, mixing, and cooling chemicals in order contribute to production of chemicals sold by the company while maintaining and improving the company’s position and branding as a responsible community partner and world leader in technology.

This is one Solution, But are There Others Based Upon Looking at the Plant Through other Stakeholders’ lenses?

Adapted from Dr Thomas’ STPA Tutorial © Copyright William Young, Jr, 2018
Define Purpose of the Analysis
Security Perspective on Defining the Purpose of the Analysis

• The purpose of the analysis draws upon the insights generated through the problem framing
• Need to include security related losses and hazards
• Need to examine other required functionality from a security perspective
Adding Security Related Losses

• Many of the losses will overlap with safety
• Security perspective may add nuance to a previous safety perspective
• Security perspective may also highlight an important safety / security trade
• Focus on alternative “system” uses
• Focus on security concerns of other stakeholders

Simply Gaining Clarification on Unacceptable Losses May Provide a Significant Gain in Security Effectiveness!
Chemical Reactor - Losses

- Unacceptable Losses (From Earlier Today)
  - L-1: People die or become injured
  - L-2: Production loss

Are there other unacceptable losses Related to Security?

Adapted from Dr Thomas’ STPA Tutorial
Chemical Reactor - Losses

- **Unacceptable Losses**
  - L-1: People die or become injured
  - L-2: Production loss
  - L-3: Loss of Reputation
  - L-4: Loss of Intellectual Property

Are these Distinct, Security-Related Losses?

Adapted from Dr Thomas’ STPA Tutorial
Chemical Reactor - Losses

- **Unacceptable Losses**
- L-1: People die or become injured
- L-2: Production loss
- L-3: Loss of Reputation
- L-4: Loss of Intellectual Property

Are There Strategic Actions We Might Want to Take that Could Improve Our Ability to Prevent These Losses?
## Thinking Broadly About Loss Mechanisms

<table>
<thead>
<tr>
<th>Stakeholders</th>
<th>Stake or Value</th>
<th>Associated Loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>S&amp;T Division</td>
<td>Developed proprietary algorithm implementing new chemical mixing scheme.</td>
<td>Financial loss if competitors become aware of the new mixing scheme and apply it before patent issued or apply it undetected after patent is issued</td>
</tr>
</tbody>
</table>

How Might We Think Differently About How We Implement the “Mixing” Function in the Plant to Prevent the Associated Loss?
## Thinking Broadly About Loss Mechanisms

<table>
<thead>
<tr>
<th>Stakeholders</th>
<th>Stake or Value</th>
<th>Associated Loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>S&amp;T Division</td>
<td>Developed proprietary algorithm implementing new chemical mixing scheme.</td>
<td>Financial loss if competitors become aware of the new mixing scheme and apply it before patent issued or apply it undetected after patent is issued</td>
</tr>
</tbody>
</table>

We are Beginning to Define our Business/Mission Related Tactical Context for Confidentiality but Effective Security Strategy Extends Beyond IT Security Professionals

© Copyright William Young, Jr, 2018
# Chemical Reactor - Hazards

<table>
<thead>
<tr>
<th>Hazard</th>
<th>Description</th>
<th>Worst Case Environment</th>
<th>Associated Losses</th>
</tr>
</thead>
<tbody>
<tr>
<td>H1:</td>
<td>Plant releases toxic chemicals</td>
<td></td>
<td></td>
</tr>
<tr>
<td>H2:</td>
<td>Plant is unable to produce chemical</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

What system state or set of conditions together with a set of worst-case environmental conditions will lead to a loss?

Adapted from Dr Thomas’ STPA Tutorial

© Copyright William Young, Jr, 2018
# Using Verbs to Help Identify System Level Hazards

<table>
<thead>
<tr>
<th>Loss</th>
<th>Transfer</th>
<th>Cool</th>
<th>Mix</th>
</tr>
</thead>
<tbody>
<tr>
<td>L1: Death or Injury</td>
<td>Transferring lethal chemicals into the environment inadvertently</td>
<td>Cooling insufficient to maintain safe operating conditions</td>
<td>Mixing the wrong chemicals</td>
</tr>
<tr>
<td>L2: Production Loss</td>
<td></td>
<td>Cooling insufficient to maintain operating limits for equipment</td>
<td>Exceeding operating conditions in the mixer might lead to equipment damage</td>
</tr>
</tbody>
</table>

© Copyright William Young, Jr, 2018
Chemical Reactor - Constraints

<table>
<thead>
<tr>
<th>Hazard</th>
<th>Safety Constraint</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>H1</strong>: Chemicals inadvertently released</td>
<td><strong>C1</strong>:</td>
</tr>
<tr>
<td><strong>H2</strong>: ??</td>
<td></td>
</tr>
</tbody>
</table>

What system state or set of conditions together with a set of worst-case environmental conditions will lead to a loss?

Adapted from Dr Thomas’ STPA Tutorial
### Chemical Reactor - Constraints

<table>
<thead>
<tr>
<th>Hazard</th>
<th>Safety Constraint</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>H1:</strong> Chemicals in air or ground after release from plant</td>
<td>Chemicals must never be released inadvertently from plant</td>
</tr>
<tr>
<td><strong>H2:</strong> ??</td>
<td></td>
</tr>
</tbody>
</table>

**Hazard**
- **H1:** Chemicals in air or ground after release from plant
- **H2:** ??

**Safety Constraint**
- Chemicals must never be released inadvertently from plant

---

**Diagram**

What are the system constraints?

Adapted from Dr Thomas’ STPA Tutorial

© Copyright William Young, Jr, 2018
Model the Control Structure
Chemical Reactor – Control Structure

A system to contain and process chemicals by means of transferring, mixing, and cooling chemicals in order contribute to production of chemicals sold by the company.

- What Processes Must Be Controlled in Order to Accomplish Business or Mission Objective
  - Transfer and mixing catalyst
  - Cooling reflux
- Use Insights to understand Controller requirements

Adapted from Dr Thomas’ STPA Tutorial

© Copyright William Young, Jr, 2018
Chemical Reactor – Control Structure

Need Functional Equivalent

Adapted from Dr Thomas’ STPA Tutorial

© Copyright William Young, Jr, 2018
Functional Control Structure

1. Identify Model Elements
2. Identify each Model Element’s responsibilities in carrying out each of the key activities necessary to conduct the mission
3. Identify Control Relationships
4. Identify the Control Actions necessary for each element to execute their responsibilities
5. Develop Process Model Description
6. Identify Process Model Variables
7. Identify Process Model Variable Values
8. Identify Feedback providing PMV Values
9. Check Functional Control Structure Model for completeness
Chemical Reactor – Control Structure

A system to **contain and process chemicals** by means of **transferring, mixing, and cooling chemicals** in order contribute to **production of chemicals sold by the company**.
Chemical Reactor – Control Structure

A system to **contain and process chemicals**
by means of **transferring, mixing, and cooling chemicals**
in order contribute to **production of chemicals sold by the company**.

<table>
<thead>
<tr>
<th>High-Level Functional Activity</th>
<th>Model Elements</th>
<th>Description</th>
</tr>
</thead>
</table>

Adapted from Dr Thomas’ STPA Tutorial © Copyright William Young, Jr, 2018
### Chemical Reactor – Control Structure

<table>
<thead>
<tr>
<th>High-Level Functional Activity</th>
<th>Model Elements</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Transfer</strong></td>
<td>Operator, Computer, Valves</td>
<td></td>
</tr>
<tr>
<td><strong>Mix</strong></td>
<td>Operator, Computer, Valves, Reactor</td>
<td></td>
</tr>
<tr>
<td><strong>Cool</strong></td>
<td>Operator, Computer, Valves, Condenser</td>
<td></td>
</tr>
</tbody>
</table>
### Key Activity: Transfer

<table>
<thead>
<tr>
<th>Element</th>
<th>Responsibility Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operator</td>
<td>• Initiate process</td>
</tr>
<tr>
<td></td>
<td>• Monitor progress</td>
</tr>
<tr>
<td></td>
<td>• Manually Intervene</td>
</tr>
<tr>
<td>Computer</td>
<td>• Control valves</td>
</tr>
<tr>
<td></td>
<td>• Report status</td>
</tr>
<tr>
<td>Valves</td>
<td>• Open/close on command</td>
</tr>
<tr>
<td></td>
<td>• Fail open? / Fail closed?</td>
</tr>
</tbody>
</table>

Adapted from Dr Thomas’ STPA Tutorial

© Copyright William Young, Jr, 2018
Chemical Reactor – Control Structure

Operator

Start Process
Stop Process

Status info
Plant state alarm

Computer

Open/close water valve
Open/close catalyst valve

Plant status

Physical Plant

Valves

Adapted from Dr Thomas’ STPA Tutorial

© Copyright William Young, Jr, 2018
Chemical Reactor – Control Structure

Operator
Start Process
Stop Process

Computer
Status info
Plant state alarm

Open/close water valve
Open/close catalyst valve

Valves

Physical Plant

What are the unacceptable losses?

Adapted from Dr Thomas’ STPA Tutorial
© Copyright William Young, Jr, 2018
Chemical Reactor – HCAs (Unsafe / Unsecure)

What are the unacceptable losses?

HCA - Hazardous Control Action

Adapted from Dr Thomas’ STPA Tutorial

© Copyright William Young, Jr, 2018
Identify Hazardous Control Actions
# Chemical Reactor – HCAs (Unsafe / Unsecure)

<table>
<thead>
<tr>
<th>Control Action</th>
<th>Not providing causes hazard</th>
<th>Providing causes hazard</th>
<th>Incorrect Timing or Order</th>
<th>Stopped too soon or applied too long</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA1: Start Process</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CA2: Open Water Valve</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Chemical Reactor: Hazardous Control Actions (HCA)

<table>
<thead>
<tr>
<th>Control Action</th>
<th>Not providing causes hazard</th>
<th>Providing causes hazard</th>
<th>Incorrect Timing or Order</th>
<th>Stopped too soon or applied too long</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA1: Start Process</td>
<td></td>
<td>Operator provides command when condenser water valve not functioning</td>
<td>Operator manually overrides valves and computer misses signal</td>
<td></td>
</tr>
<tr>
<td>CA2: Open Water Valve</td>
<td>Computer does not provide open water valve cmd when catalyst open</td>
<td>Computer provides open water valve cmd more than X seconds after open catalyst</td>
<td>Computer stops providing open water valve cmd too soon when catalyst open</td>
<td></td>
</tr>
<tr>
<td>CA3: Close Water Valve</td>
<td></td>
<td>Computer provides close water valve cmd while catalyst open</td>
<td>Computer provides close water valve cmd before catalyst closes</td>
<td></td>
</tr>
<tr>
<td>CA4: Open Catalyst Valve</td>
<td></td>
<td>Computer provides open catalyst valve cmd when water valve not open</td>
<td>Computer provides open catalyst valve cmd more than X seconds before open water</td>
<td></td>
</tr>
<tr>
<td>CA5: Close Catalyst Valve</td>
<td>Computer does not provide close catalyst valve cmd when water closed</td>
<td>Computer provides close catalyst valve cmd more than X seconds after close water</td>
<td>Computer stops providing close catalyst valve cmd too soon when water closed</td>
<td></td>
</tr>
</tbody>
</table>

Adapted from Dr Thomas’ STPA Tutorial
Identify Loss Scenarios
Inadequate Control Algorithm (Flaws in creation, process changes, incorrect modification or adaptation)

Controller (?)

Process Model (inconsistent, incomplete, or incorrect)

Controller

Control input or external information wrong or missing or malformed

Sensor

Inappropriate, ineffective, malformed, or missing control action

Actuator

Inadequate operation

Sensor

Feedback Delays

Inadequate, malformed or missing feedback

Controller

Feedback Delays

Sensor

Inadequate operation

Incorrect, partial or no information provided

Actuator

Measurement inaccuracies

Controller

Component failures

Changes over time

Controller

Unidentified or out-of-range disturbance

Process output contributes to system hazard

Controller (?)

Controller

Process input missing or wrong

Controller (?)

Controller

© Copyright William Young, Jr, 2017
Identifying Scenarios that Lead to Unsecure Control Actions

- Scenarios should be used to facilitate deeper insights and understanding, they are not a checklist
- Scenarios provide an opportunity to engage technical experts and ask key questions necessary to support improved requirements
- Scenarios form a connected narrative to understand and explain interactions across the system (and set appropriate requirements)
- Scenarios should provide useful insight or generate additional questions for deeper debate and discussion
  - Scenarios such as “denial of service attack prevents controller from issuing close valve command” aren’t really as useful as “controller issues command to initiate the process because it received inputs from sensor X indicating that valve is closed when the valve was only partially closed due to sensor logic declaring the valve closed when XXXX”
Step 2: Potential causes of UCAs

UCA: Computer opens catalyst valve when water valve not open

Controller

Sensor

Actuator

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

Controller

Process Model (inconsistent, incomplete, or incorrect)

Controller

Control input or external information wrong or missing or malformed

Actuator

Inadequate operation

Sensor

Inadequate operation

Controller (?

Controller

Sensor

Actuator

Incorrect, partial or no information provided

Measurement inaccuracies

Feedback delays

Inadequate, malformed or missing feedback

Feedback Delays

Component failures

Changes over time

Controller

Process output contributes to system hazard

Unidentified or out-of-range disturbance

Process input missing or wrong

Controller

Conflicting control actions

Controller

Delayed, partial, or malformed operation

Controller

Missing or wrong or unauthorized communication with another controller

Adapted from Dr Thomas’ STPA Tutorial

© Copyright William Young, Jr, 2017
## Scenario

**UCA: Computer does not provide close catalyst valve cmd when water closed**

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Associated Causal Factors</th>
<th>Rationale/Notes</th>
</tr>
</thead>
</table>
| Water valve status signal is incorrectly processed by computer. | •Malformed signal from valve  
•Partial signal from valve  
•Missing signal from valve  
•Inconsistent process model | Malicious logic on water valve system reports false/delayed/malformed information.  
Malicious logic on computer modifies process model variable to indicate that water valve is open. |
Step 2: Potential control actions not followed

Missing or wrong or unauthorized communication with another controller

Controller

Sensor

Actuator

Controller (?)

Inadequate, malformed or missing feedback

Feedback Delays

Inadequate operation

Incorrect, partial or no information provided

Measurement inaccuracies

Feedback delays

Component failures

Changes over time

Controller

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

Control input or external information wrong or missing or malformed

Controller

Computer opens water valve

Inappropriate, ineffective, malformed, or missing control action

Controller

Sensor

Actuator

Controller

Inadequate operation

Delayed, partial, or malformed operation

Controller

Sensor

Actuator

Controller

Controlled Process

Unidentified or out-of-range disturbance

Process output contributes to system hazard

Conflicting control actions

Process input input missing or wrong

Controller (?)

Adapted from Dr Thomas’ STPA Tutorial

© Copyright William Young, Jr, 2017
## Causal Scenarios

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Associated Causal Factors</th>
<th>Rationale/Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Code on the computer processes asynchronously. Assumptions about the</td>
<td>• Inadequate control algorithm</td>
<td>Test and operational environment were low latency and timing errors were not</td>
</tr>
<tr>
<td>latency of commands violated causing a delayed send to water valve.</td>
<td>• Delayed partial operation</td>
<td>tested. Malicious logic on computer or other system causes delay in the sending or</td>
</tr>
<tr>
<td></td>
<td></td>
<td>receiving of command.</td>
</tr>
</tbody>
</table>

Adapted from Dr Thomas’ STPA Tutorial © Copyright William Young, Jr, 2018
### UCA: Operator provides command when condenser water valve not functioning

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Associated Causal Factors</th>
<th>Rationale/Notes</th>
</tr>
</thead>
</table>
| Operator believes that systems are fully functioning, and commands the start of the reaction process. | • Inadequate feedback from computer on water valve status  
• Malformed sensor data incorrectly indicates green  
• Partial data coming from sensor causes computer to indicate wrong state  
• Missing status feedback from valve | Unaccounted for error state in software used by malicious logic in valve and/or computer. |
War Gaming
Blue focus on Enforcing Constraint, Red focus on violating constraint...
Goal is to “Fix” Problem Through Elimination or Mitigation Above Component Level
Summary and Conclusions
Lessons Learned Applying STPA-Sec

• Often heard comments:
  • “You’re starting at a much higher level of abstraction…”
  • “We try to do something like that, but STPA-Sec is much more rigorous…”
  • “This requires a great deal of thought…from more than just security experts”

• Difficult or impossible to implement if system owner is unable cannot specify what system is supposed to do

• Initial expert guess on what is most important to assure tends to be too broad to be actionable
  • E.g. “Power grid”

STPA-Sec is NOT a silver bullet, but appears to enable increased rigor “Left of Design”
Recent Self-Reported Assessment Results

Before Training: Ability to Develop Mitigation Strategy

- Somewhat Capable: 2
- Capable: 4
- Very Capable: 14
- Absolutely Capable: 4

After Training: Ability to Develop Mitigation Strategy

- Somewhat Capable: 1
- Capable: 10
- Very Capable: 13
- Absolutely Capable: 1

© Copyright William Young, Jr, 2017
Safety and Security

• Goal is loss prevention and risk management

• Source is probably irrelevant and may be unknowable

• Method is the development and engineering of controls

• Focus on what we have the ability to address, not the environment

• STPA/STPA-Sec provide opportunity for a unified and integrated effort through shared control structure!
Conclusion

• Must think carefully about defining the security problem

• Perfectly solving the wrong security problem doesn’t really help

• STPA-Sec provides a means to clearly link security to the broader mission or business objectives

• STPA-Sec does not replace existing security engineering methods, but enhances their effectiveness
Concluding Thoughts from Sun Tzu

The opportunity to secure ourselves against defeat lies in our own hands.

The supreme art of war is to subdue the enemy without fighting.

Strategy without tactics is the slowest route to victory. Tactics without strategy is the noise before defeat.
QUESTIONS ??
QUESTIONS ??