STPA For Internet of Things (IoT) and Mobile Software

STAMP Workshop, MIT Cambridge, MA, March 28, 2017

Gregory Pope, CSQE
The Internet of things (IoT) is the internetworking of physical devices, vehicles (also referred to as "connected devices" and "smart devices"), buildings and other items—embedded with electronics, software, sensors, actuators, and network connectivity that enable these objects to collect and exchange data.[1][2][3]

3 "Internet of Things Global Standards Initiative". ITU. Retrieved 26 June 2015
IoT Doubling by 2022

Figure 1. The IoT market will be massive

Source: IHS © 2016 IHS
IoT Hot Spots Chart  (Courtesy of Forrester Research, Inc.)

FIGURE 6 Heat Map Of Key IoT Opportunities Varies By Industry And Application

IoT Risks

“Internet of Things” security is hilariously broken and getting worse

Shodan search engine is only the latest reminder of why we need to fix IoT security.¹


J.M. Porup
Accident Prevention

- During software development identify:
  - Hazards → Accidents (Death, Injury)
  - Risks → Loss (Time, Money, Trust)
  - Vulnerabilities → Cyber Attack
Root Cause Analysis (RCA or the Five Why’s) Developed by Sakichi Toyoda, RCA was first used during the development of Toyota’s manufacturing processes in 1958.

https://chapters.theiia.org/pittsburgh/Events/Documents/Root%20Cause%20Analysis%20Presentation.ppt
Hazard Analysis Techniques - FMEA

Failure Modes and Effect Analysis (FMEA) was developed by reliability engineers in the late 1950s to study problems that might arise from malfunctions of military systems.

<table>
<thead>
<tr>
<th>Process Step</th>
<th>Potential Failure Mode</th>
<th>Potential Failure Effect</th>
<th>SEV(^1)</th>
<th>Potential Causes</th>
<th>OCC(^2)</th>
<th>Current Process Controls</th>
<th>DET(^3)</th>
<th>RPN(^4)</th>
<th>Action Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is the step?</td>
<td>In what ways can the step go wrong?</td>
<td>What is the impact on the customer if the failure mode is not prevented or corrected?</td>
<td>How severe is the effect on the customer?</td>
<td>How causes the step to go wrong (i.e., how could the failure mode occur?)</td>
<td>How frequently is the cause likely to occur?</td>
<td>How probable is detection of the failure mode or its cause?</td>
<td>Risk priority number calculated as SEV x OCC x DET</td>
<td>What are the actions for reducing the occurrence of the cause? Provide actions on all high RPNs and on severity ratings of 9 or 10.</td>
<td></td>
</tr>
<tr>
<td>ATM Pin Authentication</td>
<td>Unauthorized access</td>
<td>Unauthorized cash withdrawal</td>
<td>8</td>
<td>Lost or stolen ATM card</td>
<td>3</td>
<td>Block ATM card after three failed authentication attempts</td>
<td>3</td>
<td>72</td>
<td></td>
</tr>
<tr>
<td>Authentication failure</td>
<td>Annoyed customer</td>
<td>Network failure</td>
<td>3</td>
<td>Install load balancer to distribute workload across network links</td>
<td>5</td>
<td>75</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dispense Cash</td>
<td>Cash not disbursed</td>
<td>Unsatisfied customer</td>
<td>7</td>
<td>ATM out of cash</td>
<td>7</td>
<td>Internal alert of low cash in ATM</td>
<td>4</td>
<td>196</td>
<td>Increase minimum cash threshold limit of heavily used ATMs to prevent out-of-cash instances</td>
</tr>
<tr>
<td></td>
<td>Account debited but no cash disbursed</td>
<td>Very dissatisfied customer</td>
<td>8</td>
<td>Transaction failure</td>
<td>3</td>
<td>Install load balancer to distribute workload across network links</td>
<td>4</td>
<td>96</td>
<td></td>
</tr>
<tr>
<td>Extra cash dispensed</td>
<td>Bank loses money</td>
<td>Bills stuck to each other</td>
<td>8</td>
<td>Bills stacked incorrectly</td>
<td>2</td>
<td>Verification while loading cash in ATM</td>
<td>3</td>
<td>48</td>
<td></td>
</tr>
</tbody>
</table>

1. Severity: Severity of impact of failure event. It is scored on a scale of 1 to 10. A high score is assigned to high-impact events while a low score is assigned to low-impact events.
2. Occurrence: Frequency of occurrence of failure event. It is scored on a scale of 1 to 10. A high score is assigned to frequently occurring events while events with low occurrence are assigned a low score.
3. Detection: Ability of process control to detect occurrence of failure events. It is scored on a scale of 1 to 10. A failure event that can be easily detected by the process control is assigned a low score while a high score is assigned to an in-detectable event.
4. Risk priority number: The overall risk score of an event. It is calculated by multiplying the scores for severity, occurrence and detection. An event with a high RPN demands immediate attention while events with lower RPNs are less risky.
Fault Tree Analysis (FTA) was originally developed in 1962 at Bell Laboratories by H.A. Watson, under a U.S. Air Force Ballistics Systems Division contract to evaluate the Minuteman I Intercontinental Ballistic Missile (ICBM) Launch Control System.
Computers in 1962

IBM 7094
32,768 words of memory
36 bit word
Floating Point double precision
300MB Disk
Cost: 2.9 Million

Safety Hazard – Dropping the 25 inch disk onto your foot.
Software Proliferating Into Everything

- 100 Million lines of code
- 14 Million lines of code
- 12 Million lines of code
- 2 Billion lines of code

[://wwhttpw.informationisbeautiful.net/visualizations/million-lines-of-code/](://wwhttpw.informationisbeautiful.net/visualizations/million-lines-of-code/)
Software does not fail like hardware single point failures.

One cannot rely solely on hazard analysis methods developed for hardware when performing hazard analysis for software.

Nancy Leveson, MIT Aeronautics and Aerospace Professor

1995

2011
Hardware versus Software Over Time

Hardware wears out

Software wears in

http://www.onlineclassnotes.com/2013/01/software-doesnt-wear-out-explain-this.html
Accident Studies Involving Software Controlled Systems

1. Three Mile Island
2. Vincennes (Iran Air Flight 655)
3. Cali (American Airlines Flight 965)
4. Ariane 501
5. Mars Climate Orbiter (MCO)
6. Mars Polar Lander (MPL)
7. Titan/Centaur/Milstar
8. SOHO (Solar Heliospheric Observatory)
9. Therac 25
10. ATT Phone System
11. Kegworth British Midlands
12. Asiana Flight 214

In no case did the software fail to execute. Usual problem is requirements and interactions between components.
STPA Steps Overview

Step 1: Identify Potential Accidents

Step 2: Identify Potential Hazards/Risks

Step 3: Model The System

Step 4: Create The Context Tables

Step 5: Plan Hazard/Risk Mitigation Strategies
Simple Example: How Should Automated Train Doors Work?

High Level Requirements:

- Doors shall open at station when train is completely stopped and aligned with platform.
- Doors shall remain closed when train is moving.
- Doors shall remain open when someone is in the doorway.
- Doors shall open in an emergency.
Derived (Detailed) requirements

- Doors shall remain open when **someone** is in the **doorway**.
- Doorway: A volume of space extending from the top edge of the door frame to the floor of the car and 6 inches to either side.
- Someone: A person or object that is detected within the doorway volume.
Step 1: Identify Potential Accidents

- A1 - Passenger falls out of moving train
- A2 - Passengers not able to escape train during emergency
- A3 - Passenger steps off stopped train not at platform
- A4 – Doors close on passenger in doorway
Step 2: Identify Potential Hazards/Risks

- H-1 Doors open when the train is moving (A-1)
- H-2 Doors close while person in the doorway (A-4)
- H-3 Doors stuck closed during emergency (A-2)
- H-4 Doors stuck open (A-1, A-3)
- H-5 Doors open when not aligned to platform (A-3)
STPA Control Structure Model

- Diagram the system as a control structure

Automated Controller

Control Algorithm

Model of Process

Actuator

Sensor

Controlled Process
Step 3: Model the Automated Door Controller System

Control Commands

- Open door, stop opening door
- Close door, stop closing door

Model of Process

Door Actuator

Door Sensor

Physical Door

Control Algorithm

Other Inputs:
- Train motion
- Train position
- Emergency Indicator

Feedback:
- Door position
- Door clear

Commands:
- Open door, stop opening door
- Close door, stop closing door

Mechanical Force

Mechanical Position
Guide Phrases

- Identify Hazards that can cause accidents using guide phrases:

  1. A safety control **action is not provided or is not followed**.
  2. An **unsafe control action is provided**.
  3. A safety control **action is provided too late or out of sequence**.
  4. A safety control **action is stopped too soon or applied too long**.
### Step 4: Create Context Tables: Lack of Open Door Control Action

<table>
<thead>
<tr>
<th>Control Action</th>
<th>Train Motion</th>
<th>Train Position</th>
<th>Emer.</th>
<th>Door State</th>
<th>Hazard/Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open not provided</td>
<td>Stopped</td>
<td>Aligned</td>
<td>No</td>
<td>Person not in doorway</td>
<td>No</td>
</tr>
<tr>
<td>Open not provided</td>
<td>Stopped</td>
<td>Not Aligned No</td>
<td>No</td>
<td>Person not in doorway</td>
<td>No</td>
</tr>
<tr>
<td>Open not provided</td>
<td>Stopped</td>
<td>Aligned</td>
<td>No</td>
<td>Person in doorway</td>
<td>Yes (H-2)</td>
</tr>
<tr>
<td>Open not provided</td>
<td>Stopped</td>
<td>Not Aligned No</td>
<td>No</td>
<td>Person in doorway</td>
<td>No</td>
</tr>
<tr>
<td>Open not provided</td>
<td>Stopped</td>
<td>N/A</td>
<td>Yes</td>
<td>N/A</td>
<td>Yes (H-3)</td>
</tr>
<tr>
<td>Open not provided</td>
<td>Moving</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>No</td>
</tr>
</tbody>
</table>
## Step 4: Create Context Table for Open Door Control Action

<table>
<thead>
<tr>
<th>Control Action</th>
<th>Train Motion</th>
<th>Train Position</th>
<th>Emer.</th>
<th>Hazard/Risk Any</th>
<th>Hazard/Risk Early</th>
<th>Hazard/Risk Late</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open Moving</td>
<td>N/A</td>
<td>No</td>
<td>Yes</td>
<td>Yes (H-1)</td>
<td>Yes (H-1)</td>
<td>Yes (H-1)</td>
</tr>
<tr>
<td>Open Stopped</td>
<td>Not Aligned</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Open Stopped</td>
<td>Aligned</td>
<td>No</td>
<td>No</td>
<td>Yes (H-5)</td>
<td>Yes (H-5)</td>
<td>Yes (H-5)</td>
</tr>
</tbody>
</table>
## Step 5: Plan Hazard/Risk Mitigation Strategies

<table>
<thead>
<tr>
<th>Open Door Control</th>
<th>Don't Provide</th>
<th>Provide</th>
<th>Wrong Time/Order</th>
<th>Too Short/Long</th>
<th>Impact</th>
<th>Likelihood</th>
<th>Mitigation Strategy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Door open command not provided when train is stopped at platform and person in doorway (H-1)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>Injury</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Door open command not provided when train is stopped and emergency exists (H-3)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>Injury</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Door open command provided when train is moving and there is no emergency (H-2)</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td>Death Injury</td>
<td>Injury</td>
<td></td>
</tr>
<tr>
<td>Door open command provided when train is moving and there is an emergency (H-2)</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td>Death Injury</td>
<td>Injury</td>
<td></td>
</tr>
<tr>
<td>Door open command provided when train is stopped and not aligned with platform and is an emergency</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td>Injury</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Door open command provided when train is stopped and not aligned with platform and is an emergency</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Door open command is provided more than X seconds after train stops during an emergency (H-3)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>Injury</td>
<td></td>
</tr>
</tbody>
</table>

Prefatory STPA Analysis of context tables
## Context Tables Using Spreadsheet, Exhaustive STPA Approach

| Case | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 |
|------|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| Stopped: | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | F | F | F | F | F | F | F | F | F | F | F | F | F | F | F |
| Aligned: | T | T | T | T | T | T | F | F | F | F | F | F | F | F | F | F | F | T | T | T | T | T | T | F | F | F | F | F | F | F | F | F | F |
| Emergency: | F | F | F | F | T | T | T | T | T | T | T | T | T | F | F | F | F | T | T | T | T | T | F | F | F | F | F | F | T | T | T | T | T |
| Doorway Obstructed: | F | F | T | T | F | F | F | F | F | F | F | F | F | F | F | F | F | F | F | T | T | T | F | T | T | T | T | T | T | T | T | T | T |
| Doorway Closed: | T | F | T | T | F | T | T | T | T | F | F | F | F | F | F | F | F | F | F | F | F | F | F | F | F | F | F | F | F | F | F | F | F |
| Hazard (Me): | N | N | N | N | N | N | N | N | Y | Y | Y | Y | N | N | N | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |
| Hazard (Chart): | N | N | N | N | N | N | N | Y | Y | Y | Y | N | N | N | N | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |
| Hazard (Equation): | N | N | N | N | N | N | N | N | Y | Y | Y | Y | N | N | N | N | N | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |
### Context Table Per Guide Phrase

| Case | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 |
|------|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| Open Provided | T | F | T | F | T | F | T | F | T | F | T | F | T | F | T | F | T | F | T | F | T | F | T | F | T | F | T | F | T | F | T | F | T | F | T | F | T |
| Open Not Provided | F | F | T | T | F | F | T | T | F | F | T | T | F | F | T | T | F | F | T | T | F | F | T | T | F | F | T | T | F | F | T | T | F | F | T | T | F |
| Open Provided Too Late or Out of Sequence | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T | T |
| Open Stopped Too Soon or Applied Too Long | T | F | T | F | T | F | T | F | T | F | T | F | T | F | T | F | T | F | T | F | T | F | T | F | T | F | T | F | T | F | T | F | T | F | T | F | T |
## Automation of Context Table Analysis

### Open Provided When:

(Stopped = "T" And Aligned = "T") Or (Stopped = "T" And Aligned = "T" And Obstructed = "T") Or (Stopped = "T" And Alarm = "T")

<table>
<thead>
<tr>
<th>And</th>
<th>/ Or Chart</th>
<th>Or</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Stopped</td>
<td>T</td>
</tr>
<tr>
<td></td>
<td>Aligned</td>
<td>F</td>
</tr>
<tr>
<td></td>
<td>Emergency</td>
<td>F</td>
</tr>
<tr>
<td></td>
<td>Obstructed</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Closed</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Use null (del) or blank for d</td>
<td></td>
</tr>
</tbody>
</table>

### Open Not Provided When:

Stopped = "F" Or (Stopped = "T" And Aligned = "F" And Alarm = "F")

Or (Stopped = "T" And Closed = "F")

<table>
<thead>
<tr>
<th>And</th>
<th>/ Or Chart</th>
<th>Or</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Stopped</td>
<td>T</td>
</tr>
<tr>
<td></td>
<td>Aligned</td>
<td>F</td>
</tr>
<tr>
<td></td>
<td>Alarm</td>
<td>T</td>
</tr>
<tr>
<td></td>
<td>Obstructed</td>
<td>T</td>
</tr>
<tr>
<td></td>
<td>Closed</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Use null (del) or blank for d</td>
<td></td>
</tr>
</tbody>
</table>

Use null (del) or blank for don
Automation of Context Table Analysis

Open Provided Too Late of Out of Sequence:
Stopped = "F" Or (Stopped = "T" And Aligned = "F" And Alarm = "F")

<table>
<thead>
<tr>
<th>And / Or Chart</th>
<th>Or</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stopped</td>
<td>T</td>
</tr>
<tr>
<td>Aligned</td>
<td>T</td>
</tr>
<tr>
<td>Alarm</td>
<td>T</td>
</tr>
<tr>
<td>Obstructed</td>
<td>T</td>
</tr>
<tr>
<td>Closed</td>
<td></td>
</tr>
</tbody>
</table>

Use null (del) or blank for don't care

Open Stopped Too Soon or Applied Too Long:
Stopped = "F" Or (Stopped = "T" And Aligned = "F" And Alarm = "F")

<table>
<thead>
<tr>
<th>And / Or Chart</th>
<th>Or</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stopped</td>
<td>F</td>
</tr>
<tr>
<td>Aligned</td>
<td>F</td>
</tr>
<tr>
<td>Alarm</td>
<td></td>
</tr>
<tr>
<td>Obstructed</td>
<td></td>
</tr>
<tr>
<td>Closed</td>
<td></td>
</tr>
</tbody>
</table>
# The Hazomatic

Automated Context Table with And/Or Charts

| Case | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 |
|------|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| Stopped: | T | T | T | T | T | T | T | T | T | T | T | F | F | F | F | F | F | F | F | F | F | F | F | F | F | F | F | F | F | F |
| Aligned: | T | T | T | T | T | T | T | F | F | F | F | F | F | F | F | T | T | T | T | T | T | T | F | F | F | F | F | F | F | F |
| Emergency: | F | F | F | F | T | T | T | F | F | F | F | T | T | T | F | F | F | T | T | T | F | F | F | F | F | F | F | F | F | F |
| Doorway Obstructed | F | F | T | T | T | F | F | T | T | F | F | T | T | F | F | T | T | F | F | T | T | F | F | T | T | F | T | F | T | T |
| Doorway Closed | T | F | T | F | T | T | F | F | T | F | T | F | F | T | F | T | F | T | F | F | T | F | F | T | F | T | F | T | F | T |
| Hazard (Me) | N | N | N | N | N | N | N | N | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |
| Hazard (Chart) | N | N | N | N | N | N | N | N | N | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |
| Hazard (Equation) | N | N | N | N | N | N | N | N | N | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |

And / Or Chart

<table>
<thead>
<tr>
<th>And / Or Chart</th>
<th>30</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stopped</td>
<td>F</td>
</tr>
<tr>
<td>Aligned</td>
<td>F</td>
</tr>
<tr>
<td>Emergency</td>
<td>F</td>
</tr>
</tbody>
</table>

Obstructed

Closed

Use null (del) or blank for d

Hazards

<table>
<thead>
<tr>
<th>Hazomatic</th>
<th>20</th>
</tr>
</thead>
</table>

Clear

20
Exhaustive Context Tables Analysis

- Number of Combinations = 128
  - \( s = \) number of binary states
  - \( g = \) number of guide phrases
  - Combinations = \( 2^s \times g = 2^5 \times 4 = 128 \)

- Number of Potential Hazards Combinations:

<table>
<thead>
<tr>
<th>Condition</th>
<th>me</th>
<th>and/or</th>
<th>equation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open Provided =</td>
<td>20</td>
<td>20</td>
<td>20</td>
</tr>
<tr>
<td>Open Not Provided =</td>
<td>12</td>
<td>12</td>
<td>12</td>
</tr>
<tr>
<td>Open Too Late or Out of Sequence =</td>
<td>12</td>
<td>12</td>
<td>12</td>
</tr>
<tr>
<td>Open Stopped Too Soon Applied Too Long =</td>
<td>32</td>
<td>32</td>
<td>32</td>
</tr>
<tr>
<td>Total</td>
<td>76</td>
<td>76</td>
<td>76</td>
</tr>
</tbody>
</table>

- Resulting Revised Requirements = 4
- Manual was 7 hazards and 0 Revised Requirements
STPA Can Point Out Requirement Problems

Revised High Level Requirements:

- Doors shall open at station when train is completely stopped and aligned with platform.
- Doors shall remain closed when train is moving.
- Doors shall remain open when someone is in the doorway, the train shall not move until the doors close.
- The train shall remain stopped and a door open command issued if an object is detected in the doorway when doors are closed.
- An emergency shall stop the train, Doors shall open in an emergency after the train has stopped.
IoT Benefits

- CO Detector
- Thermostat
- Internet Service Provider
- Dash Button
- Home Wi-Fi Router
- Alarm System
- Cell Tower
- Smart Phone
- Vehicles
- Camera Front Door
- Camera Driveway
- Motion Detection
Turn Down The Air Conditioning When No One is Home

Cell Tower

Internet Service Provider

Home Wi-Fi Router

Thermostat

Lower Utility Bills
Energy Preservation
Turn Down Air Conditioning If No Motion for an Hour

Cell Tower

Internet Service Provider

Lower Utility Bills
Energy Preservation

Home Wi-Fi Router

Thermostat

Motion Detection
Turn Down Air Conditioning if Burglar Alarm Set To Away

- Cell Tower
- Internet Service Provider
- Home Wi-Fi Router
- Thermostat

Lower Utility Bills
Energy Preservation

Alarm System
Is Teen Driver Home Yet?

Cell Tower → Internet Service Provider → Home Wi-Fi Router → Camera Driveway

Safety
Win Arguments With Teens

Motion Detection
Turn Off Gas Source If CO Detected

Cell Tower

Internet Service Provider

Home Wi-Fi Router

Thermostat

Safety

CO Detector
On Vacation

Cell Tower

Internet Service Provider

Home Wi-Fi Router

Security

Smart TV

House Sounds

Home Lighting
Do I Recognize My Visitor?

- Cell Tower
- Internet Service Provider
- Home Wi-Fi Router
- Camera Front Door

Safety Security
Just In Time Supply Ordering Dash Buttons

https://www.amazon.com/Dash-Buttons/b?ie=UTF8&node=10667898011

Energy Preservation
Is STPA Useful for IoT Vulnerability Analysis?

- Literature searches cite 6-10 concerns about vulnerabilities.
- Have not found a formal hazard or vulnerability analysis on the IoT.
- Can STPA identify the same 6-10 Hazards and Vulnerabilities?
- Can STPA find additional Hazards and Vulnerabilities?
IoT Basic Logical Model
IoT Basic Device Physical Model

Development Subsystem

Requirement Elicitation -> Software Requirements -> Software Design

Editor <-> Compiler <-> Build Tools <-> Libraries <-> Debuggers <-> Software Testing

Cellular Network <-> Smart Phones O/S

Other Smart Phone Applications <-> Browsers

Electronic Design <-> Mechanical Design

IoT Code Developed <-> IoT Device

External Communications Subsystem

IoT Device

Device HMI <-> Peripherals <-> Other Software Applications <-> Utilities <-> Operating System(s)

I/O Cable or Wi-Fi <-> LAN Routers <-> Firewalls <-> Internet <-> Updates Patches

Lawrence Livermore National Laboratory
Development Sub-Subsystem Analysis

STPA Guide Phrases

A resource or action required for correct operation is not provided or is not followed.

An incorrect resource or action is provided that leads to a hazard/risk.

A potentially correct resource or action is provided too late, or out of sequence.

A correct resource or control action is stopped too soon or applied too long.
### Combinations of Things That Could Go Wrong in IoT

<table>
<thead>
<tr>
<th>Physical Model</th>
<th>Risks</th>
<th>Comb.</th>
<th>Average</th>
</tr>
</thead>
<tbody>
<tr>
<td>Development Risks</td>
<td>110</td>
<td>94592</td>
<td>9.2</td>
</tr>
<tr>
<td>Communications Risk</td>
<td>64</td>
<td>6080</td>
<td>6.4</td>
</tr>
<tr>
<td>Mobile Risks</td>
<td>27</td>
<td>1424</td>
<td>5.4</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>201</strong></td>
<td><strong>102096</strong></td>
<td><strong>7.0</strong></td>
</tr>
</tbody>
</table>

\[ \text{s = number of binary states} \]
\[ \text{g = number of guide phrases} \]
\[ \text{Combinations} = 2^s \times g = 2^4 \times 4 = \text{###} \]

Assume “or” of all three

Assume “and” of all

---

Estimated number of electrons in the universe = \(10^{E+88}\)

Age of the Universe in Plank time = \(8 \times 10^{E+60}\)

Plank time = \(10^{E-43}\) seconds
Using Surrogates for STPA of IoT

- Representative STPA which represents all the analyzed components of the physical model:

  - Requirements Incorrect
  - Weak Security Design
  - Difficult User Interface
  - Software Defects
  - Software Vulnerabilities
  - Tainted Input Possible
  - Logic Bomb in Code
  - Back Door in Code
  - Inadequate Testing
  - Untrusted Supply Chain
  - Updates Not Used
Using Surrogates for STPA of IoT

- Representative STPA which represents all the analyzed components of the physical model:
  - Internet for IoT
  - Acuator
  - Sensor
  - Physical Device
  - Unclear Error Messages
  - Confusing Documentation
  - Weak Encryption
  - Open Ports
  - Insufficient Platform Testing
  - Weak Negative Testing
  - Inadequate Security Testing
  - Updates No Longer Supported
  - Updates Contain Malware
  - Browser Vulnerabilities
Using Surrogates for STPA of IoT

- Representative STPA which represents all the analyzed components of the physical model:
  - Inadequate Encryption
  - Backbone Vulnerabilities
  - O/S Vulnerabilities
  - Faux Cell Tower
  - Juice Jacking
  - Directed Phishing
  - Unsecured Hot Spots
  - Browser Vulnerabilities
  - Smart Phone Not Updated
IoT What Could Possibly Go Wrong?
User Interface (UI) Big Challenge

1985

Home IT Engineer 2022

Good News:
“Apple Home Kit”
“Works With Nest”

Emerging Standards

https://workswith.nest.com/products
http://www.apple.com/shop/accessories/all-accessories/homekit
http://www.digitaltrends.com/home/everything-that-works-with-apple-homekit/

Home Sweet Home

- Oven
- Washer
- Climate Control
- Surveillance Cameras
- Alarm System
- Vacuum Cleaner
- Toaster
- Dryer
- Lights
- Entertainment Center
- Door Controller
- Hot Tub
- Refrigerator
- Door Bell
- Utilities
- Game Center
- Pet Door Controller
- Children Monitors
- Freezer
- Phone System
- Pet Feeding
- Outdoor Sprinkler System
- Fire/Smoke Alarms
- Vehicle Monitors
Obsolesce Update Story

Vehicles As Weapons, e-Jacking

http://www.express.co.uk/news/world/600771/ISIS-Islamic-State-remote-controlled-cars-bomb-attacks-Syria-Iraq-drones-Britain

Wireless Carjacking

DDoS Attacks – Bots Gone Wild

Video Cameras → Wide Spread Internet Outages

In January a fully booked four-star hotel in Austria, Romantik Seehotel Jaegerwirt, had its locks hacked.

The hackers demanded the equivalent of 1,500 Euros in bitcoin in exchange for restoring the keys’ functionality

http://www.welivesecurity.com/2017/01/30/austrian-hotel-experiences-ransomware-things-attack/
But There’s More
IoT Power Surge (Toaster Attack)

166,667 ovens x 3,000 watts per oven = 500 Megawatts

OR

454,545 toasters x 1,100 watts per toaster = Wide Spread Power Disruption
IoT Click and Enter Burglary

- Disable Alarms
- Open Doors
- Assure No One Home
- Self Parking Get Away Car
IoT Medical Race Condition

Tell-tale heart: Pacemaker data leads to arson, fraud charges
IoT Inconvenient Subscription Renewals

![Image of a car's infotainment system with a message indicating a subscription expiration and options to renew or enter a product key.]
IoT New Risks In Toilet Training
IoT Incremental Surgical Billing Adds Motivation to Pay Quickly

…and how did you want to pay for your anesthesia today Martha?
Driving Violations for April 2017

- Speeding: 23
- Stop Signs: 12
- Traffic Lights: 3
- Acceleration: 8
- Turn G Force: 3

Rate Increase = 15%
IoT Car Pricing

31,984

25,984
With Ads
IoT New Meaning for Blue Screen of Death

![Blue Screen of Death Image]
## Telecommunications and Web Software yet to be Mission Critical Level

<table>
<thead>
<tr>
<th>Application Domain</th>
<th>Number Projects</th>
<th>Error Range (Errors/KESLOC)</th>
<th>Normative Error Rate (Errors/KESLOC)</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automation</td>
<td>55</td>
<td>2 to 8</td>
<td>5</td>
<td>Factory automation</td>
</tr>
<tr>
<td>Banking</td>
<td>30</td>
<td>3 to 10</td>
<td>6</td>
<td>Loan processing, ATM</td>
</tr>
<tr>
<td>Command &amp; Control</td>
<td>45</td>
<td>0.5 to 5</td>
<td>1</td>
<td>Command centers</td>
</tr>
<tr>
<td>Data Processing</td>
<td>35</td>
<td>2 to 14</td>
<td>8</td>
<td>DB-intensive systems</td>
</tr>
<tr>
<td>Environment/Tools</td>
<td>75</td>
<td>5 to 12</td>
<td>8</td>
<td>CASE, compilers, etc.</td>
</tr>
<tr>
<td>Military -All</td>
<td>125</td>
<td>0.2 to 3</td>
<td>&lt; 1.0</td>
<td>See subcategories</td>
</tr>
<tr>
<td>Airborne</td>
<td>40</td>
<td>0.2 to 1.3</td>
<td>0.5</td>
<td>Embedded sensors</td>
</tr>
<tr>
<td>Ground</td>
<td>52</td>
<td>0.5 to 4</td>
<td>0.8</td>
<td>Combat center</td>
</tr>
<tr>
<td>Missile</td>
<td>15</td>
<td>0.3 to 1.5</td>
<td>0.5</td>
<td>GNC system</td>
</tr>
<tr>
<td>Space</td>
<td>18</td>
<td>0.2 to 0.8</td>
<td>0.4</td>
<td>Attitude control system</td>
</tr>
<tr>
<td>Scientific</td>
<td>35</td>
<td>0.9 to 5</td>
<td>2</td>
<td>Seismic processing</td>
</tr>
<tr>
<td>Telecommunications</td>
<td>50</td>
<td>3 to 12</td>
<td>6</td>
<td>Digital switches</td>
</tr>
<tr>
<td>Test</td>
<td>35</td>
<td>3 to 15</td>
<td>7</td>
<td>Test equipment, devices</td>
</tr>
<tr>
<td>Trainers/Simulations</td>
<td>25</td>
<td>2 to 11</td>
<td>6</td>
<td>Virtual reality simulator</td>
</tr>
<tr>
<td>Web Business</td>
<td>65</td>
<td>4 to 18</td>
<td>11</td>
<td>Client/server sites</td>
</tr>
<tr>
<td>Other</td>
<td>25</td>
<td>2 to 15</td>
<td>7</td>
<td>All others</td>
</tr>
</tbody>
</table>

2016 Benchmark for Telecommunications and Web Getting Better – Donald Reifer

- Assumption is defect rate after one year, not at release as in 2004 table.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Defects/KESLOC</td>
<td>4.0</td>
<td>3.4</td>
<td>2.9</td>
<td>2.3</td>
<td>1.6</td>
</tr>
</tbody>
</table>

Average Defects/KESLOC for Commercial - Telecommunications

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Defects/KESLOC</td>
<td>7.0</td>
<td>6.4</td>
<td>5.8</td>
<td>5.3</td>
<td>4.8</td>
</tr>
</tbody>
</table>

Average Defects/KESLOC for Commercial - Web Business

- .55 defects per ksloc for Mission Critical codes
- What should defect rate be for IoT and Mobile software then?

Reifer Consultants
http://reifer.com/
IoT Software Reaching Mission Critical Level

![IoT Software Error Rates graph](image)

Defect Rates will approach but never reach zero.

- Web Business 2026
- Telecommunications 2021
Over 175 Tools to Support IoT

Numbers Linked to IoT Tools for each component

Development Subsystem

Software Requirements
Software Design
Editor
Compiler
Build Tools
Libraries
Debuggers
Software Testing
Cellular Network
Smart Phones O/S
Browsers
Electronic Design
Mechanical Design
IoT Code Developed
IoT Device

Mobile Phone Subsystem

Other Smart Phone Applications

External Communications Subsystem

Device HMI
Peripherals
Other Software Applications
Utilities
Operating System(s)

I/O Cable or Wi-Fi
Routers
Firewalls
Internet
Updates Patches
IoT and Mobile Mitigations

1. Do not use inexpensive household routers for IoT applications as the software is buggy.
2. Use strong (AES or better) encryption everywhere.
3. Replace default factory user names and passwords with strong passwords, change periodically. [Link](http://www.howtogeek.com/195430/how-to-create-a-strong-password-and-remember-it/)
4. Assure firmware and software updated to latest versions.
5. Assure media and updates are from trusted sources
6. Don’t use public recharge stations
IoT and Mobile Mitigations

7. Alarm on IoT devices disabled
8. Wait until IoT industry matures
9. Don’t allow remote help desks without confirming source.
10. Static and Dynamic code analysis on Source and Binary codes
11. Assure IoT applications are security tested and support security with updates
12. Segment networks (IoT, Personal, Business)
13. Purchase new device every three year
Comparison Test

- Literature search found 6-10 security vulnerabilities
- STPA found 101 security vulnerabilities, hazards, and risk types.
- Surrogate STPA rolled up to 30 issues
STPA Lessons Learned

1. STPA facilitated me to think of hazards and risks I could not think of intuitively
2. STPA identified risks and hazards not identified in the literature search
3. STPA helped me research further important topics
4. STPA helped me ask better questions and enroll experts
Prefatory Versus Exhaustive STPA

- Prefatory STPA requires human analysis to identify hazards or vulnerabilities when requirements are stated.

- Exhaustive STPA (examining all combinations) can be useful for small numbers of variables or when requirements are not stated.

- Exhaustive STPA may not be practical for analysis of a larger number if variables, decomposition and a surrogate approach may be helpful.
Conclusion – STPA Useful

- STPA useful addition to other techniques, literature search, and expert consultation, for IoT and Mobile hazard, risk, and security analysis
Back Up Slides Tools
Requirement and Design Tools

- Requirements
  - Rational Requisite Pro
  - Objectiver
  - CaseComplete
  - RMTrac
  - Optimal Trace
  - Analyst Pro
  - DOORS
  - GMARC
  - Jira

- Design
  - IBM Architect Designer
  - Structure Chart
  - Data Flow Diagram
  - Doxygen
  - Visustin
  - McCabe IQ
  - Design By Contract
  - Assertions
Editors and Compilers

- Editors
  - Sublime Text
  - Notepad ++
  - Vim
  - Atom
  - Emacs
  - Eclipse
  - Code::Blocks
  - GNAT Programming Studio
  - Code Lite
  - NetBeans
  - Qt Creator

- Compilers
  - Intel
  - Gnu
  - Microsoft
  - Visual C++
  - Clang
  - CUDA
  - ROSE Custom Tool
Build Tools and Libraries

- **Build Tools**
  - Cmake
  - Autoconf
  - Jenkins
  - Bamboo
  - Ant
  - CruiseControl
  - Git
  - Subversion
  - Mecurial
  - Perforce
  - *and many more*

- **Libraries**
  - Boost
  - OpenMP
  - OpenGL
  - VTK
  - *and many more*
Debuggers and Software Testing

**Debuggers**
- Code View
- Valgrind
- MS Visual Studio
- Intel Debugger
- Parasoft Insure++
- IDAPro
- ROSE Custom Tool
- and many more

**Software Testing**
- Cppunit
- Junit
- Google Test
- Test Complete
- HP Functional Tester
- Selenium
- Squish
- ATS
- and many more
Developed Code and IoT Device

- Developed Code
  - Purify
  - Intel Inspector XE
  - Insure++
  - Lcov, Gcov
  - Cobertura
  - Klocworks
  - Parasoft
  - Coverity
  - ROSE Custom Tool

- IoT Device
  - Vector Software
  - HiTex
  - eggPlant
  - Xilinx SDK
  - Peta Linux Tools
  - IDAPro
  - ROSE Custom Tool
Electronic and Mechanical Design

- **Electronic**
  - Spark
  - PulseForge 3300
  - Project Wire
  - TDK4PE
  - PCB Web Designer
  - NanoTech AMD 3D
  - *and many more*

- **Mechanical**
  - AutoCad
  - Autodesk CAM
  - IronCAD
  - SolidWorks
  - *and many more*
Device HMI and Peripherals

- **HMI**
  - Active X
  - Lab Windows
  - Tk/Tcl
  - Motif
  - Visual Basic/C++
  - PowerBuilder
  - and many more

- **Peripherals**
  - LabView
  - FastSend
  - PacketCheck
  - Intel Admin Tools
  - NDT
Software Aps and Utilities

- **Software Aps**
  - Norton
  - McAfee
  - TrendMicro
  - Malwarebytes
  - Bitdefender
  - MS Office
  - ROSE Custom Tool

- **Utilities**
  - CrashPlan
  - COMODO Back Up
  - AOMEI Backupper
  - Cobian Backup
  - and many more
Operating Systems, I/O Cable of Wi-Fi

- Operating Systems
  - Windows
  - Linux
    - Embedded Linux
    - Android
  - Unix BSD
  - Mac OS X
    - iOS
  - Commercial Unix
  - Solaris/OpenSolaris
  - Custom OS

- Cable or Wi-Fi
  - Vastar
  - Fluke
  - Ideal Networks
  - AirCheck G2
  - Wi-Fi Pineapple
  - Wi-Spy DBx
  - Wi-Fi Analyzer
  - Yellowjacket-BANG
Routers and Firewalls

- **Routers**
  - Angry IP Scanner
  - Ping Plotter
  - Blast
  - TCP View
  - PRTG Network Monitor
  - HP Load Runner
  - and many more

- **Firewalls**
  - Nessus
  - Nmap
  - Netcat
  - Tcpdump
  - Wireshark
  - CommView
  - and many more
Internet and Update Patches

- Internet
  - ZenMap
  - Ipplan
  - Tcpdump
  - Nmap NSE Scripts
  - Dig
  - Acunetix
  - John the Ripper
  - and many more

- Update Patches
  - Tripwire CCM
  - CodeDx
  - Corporate Software Inspector
  - Open VAS
  - Retina CS
  - MBSA
  - Nexpose
  - and many more
Cellular Network Smart Phone O/S

- Cellular Network
  - Speedtest
  - Network Signal Info Pro
  - wiggle.net

- Smart Phone O/S
  - iOS
  - Android
  - Windows Mobile
  - BlackBerry OS
  - LG webOS
Smart Phone Aps and Browser

- **Smart Phone Aps**
  - McAfee
  - Norton
  - Trend
  - Panda
  - Webroot
  - iPhone N/A

- **Browsers**
  - Chrome
  - Firefox
  - Safari
  - Opera
  - Skyfire
  - UC Browser
  - BeFE
Backup Slides STPA Analysis
Requirements Elicitation/Software Requirements

- Stakeholder Sample Wrong
- Requirement Not Specific
- Requirement Not Measurable
- Requirement Not Attainable
- Requirement Not Realizable
- Requirement Not Time Bounded
- Requirement Not Complete
- Requirement Not Concise
- Approved Before Understood
- Jumping to Design

https://www.linkedin.com/pulse/top-8-mistakes-requirements-elicitation-aaron-whittenberger-cbap
Development Sub-Subsystem Risks

Software Requirements/Software Design
- Missing Functional Requirements
- Missing Non-Functional Requirements
- Missing Security Requirements
- Missing Safety Requirements
- Exception Cases Not Handled
- Unclear
- Unprioritized
- Incomplete
- Unconsumable
- Unreflective of business goals

http://www.seilevel.com/requirements/5-reasons-software-projects-fail-hint-its-often-due-to-incomplete-incorrect-requirements
Development Sub-Subsystem Risks

Software Design/Editor
- Lacks Intuitiveness
- Weak Exception Handling
- Human Machine Interface not well Defined
- Requirement Creep
- Weak Scalability
- Weak Coupling
- Weak Cohesion
- Sparse Commenting
- Lack of Meaningful Naming

http://www.pcworld.com/article/146282/article.html
Development Sub-Subsystem Risks

- Uninitialized Variable
- UnReleased Memory
- Array overflow
- Buffer Overflow
- Tainted Input
- Null pointer
- Stale Pointer
- Unreachable Code
- Back Door
- Logic Bomb
- Missing Requirements
- Misunderstood Requirements
- Syntax Error
Development Sub-Subsystem Risks

Compiler/Build Tools

- Compiler Warnings Ignored
- Wrong Test Baseline
- Inadequate Resources
- Missing or Wrong Includes
- Wrong Options Set
- Non-Standard Features Used
- Exceptions Not Caught
- Unclear Error Messages
- Errors Ignored
- Warnings Ignored
- Compiler Not Updated
Development Sub-Subsystem Risks

- **Build Tools/Libraries**
  - Wrong Library Version
  - Misnamed Library
  - Library Vulnerability
  - Library Not Updated
  - Library Back Door
  - Untrusted Supply Chain
  - Library Not Updated

Development Sub-Subsystem Risks

- Actuator
- Sensor
- Libraries (Built Code)
- Debuggers

Libraries/Debuggers
- Heisenberg Effect
- Diagnostics Residual
- Intermittent Problem
- Residual Debug Code
- Unrealistic Simulators
Development Sub-Subsystem Risks

- Actuator
- Sensor
- Debuggers (Debugged Code)

Debuggers/Software Testing
- Low Coverage
- No/Few Security Tests
- Rushed Testing
- No/Few Requirements Traceability
- Redundant Testing
- No/Few Performance Tests
- Weak Platform Testing
Development Sub-Subsystem Risks

Software Testing/IoT Code Developed
- Residual Bugs
- Slow Performance
- Race Condition
- Weak Error Recovery
- Weak On Line Help
- Weak Documentation
Development Sub-Subsystem Risks

IoT Code Developed/IoT Device
- HW/SW Compatibility
- Operating System Vulnerability
- Unsupported Operating System Version
- Slow Performance
- Race Conditions
- Confusing Install Procedure
- Missing Resources
- Tainted Install Media
Development Sub-Subsystem Risks

- Insufficient Air Flow
- Confusing Labeling
- Harness Rub
- Poor Serviceability
- Fan Cooling Needed
- EMI/EMC Shielding
- Insufficient Vibration Resistance
- Insufficient Shock Resistance
- Insufficient Environmental Resistance
- Manufacturing Defect
- Supply Chain Defect
IoT Device/ Electrical Design

- Inadequate Power Supply
- Inadequate Component Reliability
- Inadequate Surge Protection
- Inadequate Noise Suppression
- Counterfeit Parts
- Slow Processing
- Lack of Fault Detection
- Inadequate Shock Protection
- Inadequate Static Discharge Protection
- Version Control Issues
- Weak Serviceability
- Weak or No Upgrade Ability
External Communications Sub-Subsystem Risks

IoT/Device HMI

- Confusing User Interface
- Weak Exception Handling
- Unclear Error Messages
- Unlike Incumbent
- Lack of Documentation
- Confusing Documentation
- Secret Codes Remain
- Unix Jan 19, 2038 Bug /32 bit

https://en.wikipedia.org/wiki/Year_2038_problem
External Communications Sub-Subsystem Risks

IoT/Peripherals
- Current Drivers Not Available
- Encryption Not Available
- Inadequate Installation Guide
- No Guest Device Controls
- Open Unused I/O Ports
- Driver Not Updated
- No Longer Supported
- Buggy Software
External Communications Sub-Subsystem Risks

- Actuator
- Sensor
- IoT Device
- Other Software Applications
- IoT/Other SW Apps
  - File Names Not Unique
  - Versions Not Compatible
  - Supply Chain Not Secure
  - Trojans Present
  - Back Door Present
  - Not Enough Memory
  - Rogue Applications
External Communications Sub-Subsystem Risks

IoT/Utilities
- Wrong Version
- Known Vulnerabilities in Version
- Version Not Updated
- Wrong Numerical Precision
- Wrong Data Format
- Counterfeit Item
- No Upgrade Path
- Browser Vulnerabilities
External Communications Sub-Subsystem Risks

- Operating Systems
- Sensor
- Actuator
- IoT Device

IoT/Utilities
- Wrong Version
- Known Vulnerabilities in Version
- Version Not Updated
- Wrong Numerical Precision
- Wrong Data Format
- Counterfeit Item
- No Upgrade Path
- Browser Vulnerabilities
External Communications Sub-Subsystem Risks

Peripheral/ IO Cable or Wi-Fi
- Not Encrypted
- Weak Encryption
- Network Not Password Protected
- Open I/O Ports
- Driver Not Updated
- Trap Door in Driver
I/O Cable or Wi-Fi / LAN Routers

- No / Weak Encryption
- Buggy Router Software
- Router Firmware Not Updated
- Router Updates No Longer Available
- Back Door Left In Router
- Updates Contain Virus
- Default User and Password
- Ports Left Open (7547)
- Services Exposed TR-64 -69
External Communications Sub-Subsystem Risks

- LAN Routers
- Firewalls
- Actuator
- Sensor
- Firewalls

<table>
<thead>
<tr>
<th>LAN Routers/Firewall</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ports Left Open</td>
</tr>
<tr>
<td>Wrong Security Policy</td>
</tr>
<tr>
<td>Firewall No Longer Supported</td>
</tr>
<tr>
<td>Firewall Contains Back Door</td>
</tr>
<tr>
<td>Capacity Insufficient</td>
</tr>
<tr>
<td>VPN Not Available</td>
</tr>
<tr>
<td>Not Updated</td>
</tr>
</tbody>
</table>

- I/O Cable or Wi-Fi
- LAN Routers
- Internet
- Updates Patches
- Operating System(s)
- Utilities
- Other Software Applications
- Peripherals
- Device HMI
- IoT Device
External Communications Sub-Subsystem Risks

- Firewall
- Internet
- Actuator
- Sensor

Firewall/Internet
- Capacity Insufficient
- VPN Not Available
- No Port Scanning Detectors
- Required Port Blocked
External Communications Sub-Subsystem Risks

Internet/Update Patched
- Patch Infected With Virus
- Patch Has Vulnerability
- Device No Longer Supported
- Updates Not Done

Update Patches

Actuator

Sensor

Internet
I/O Connection Cable or Wi-Fi/Cellular Network

- Not Encrypted
- Inadequate Encryption A5/1, A5/2
- Backbone Vulnerabilities SS7
- Backdoors
- Public Unsecured Wi-Fi
- Operating System Vulnerabilities
- O/S Not Upgraded
Mobile Phone and Update Sub-Subsystem Risks

Cellular/Smart Phones

- Juice Jacking
- Faux Cell Tower
Mobile Phone and Update Sub-Subsystem Risks

Smart Phones/Browser
- Lack of Frame Busting, Tap Jacking
- Vulnerable Mobile Site
- Phishing
- Counterfeit Address Bar
- Unsecured Hot Spots
- Unintelligible Error Message

Actuator
Sensor

---

Lawrence Livermore National Laboratory
Mobile Phone and Update Sub-Subsystem Risks

**Browsers/Other Apps**

- Not Downloaded From Trusted Source
- Malicious Apps
- Apps Not Updated
- App No Longer Supported
- Apps Not Updated
Mobile Phone and Update Sub-Subsystem Risks

- Cellular Network
- Smart Phones O/S
- Other Smart Phone Applications
- Browsers
- IoT Code Developed
- IoT Device
- I/O Cable or Wi-Fi
- LAN Routers
- Firewalls
- Internet
- Updates Patches
- Peripherals

Smart Phone/Updates
- Counterfeit Updates
- Trap Door in Update
- Discontinued Updates
- Slow Updates
- Unencrypted Updates
- Out Of Date Firmware
- Device Not Updated

Actuator

Sensor

IoT Code Developed

Smart Phones