STPA For Internet of Things (IoT) and Mobile Software

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

Gregory Pope, CSQE

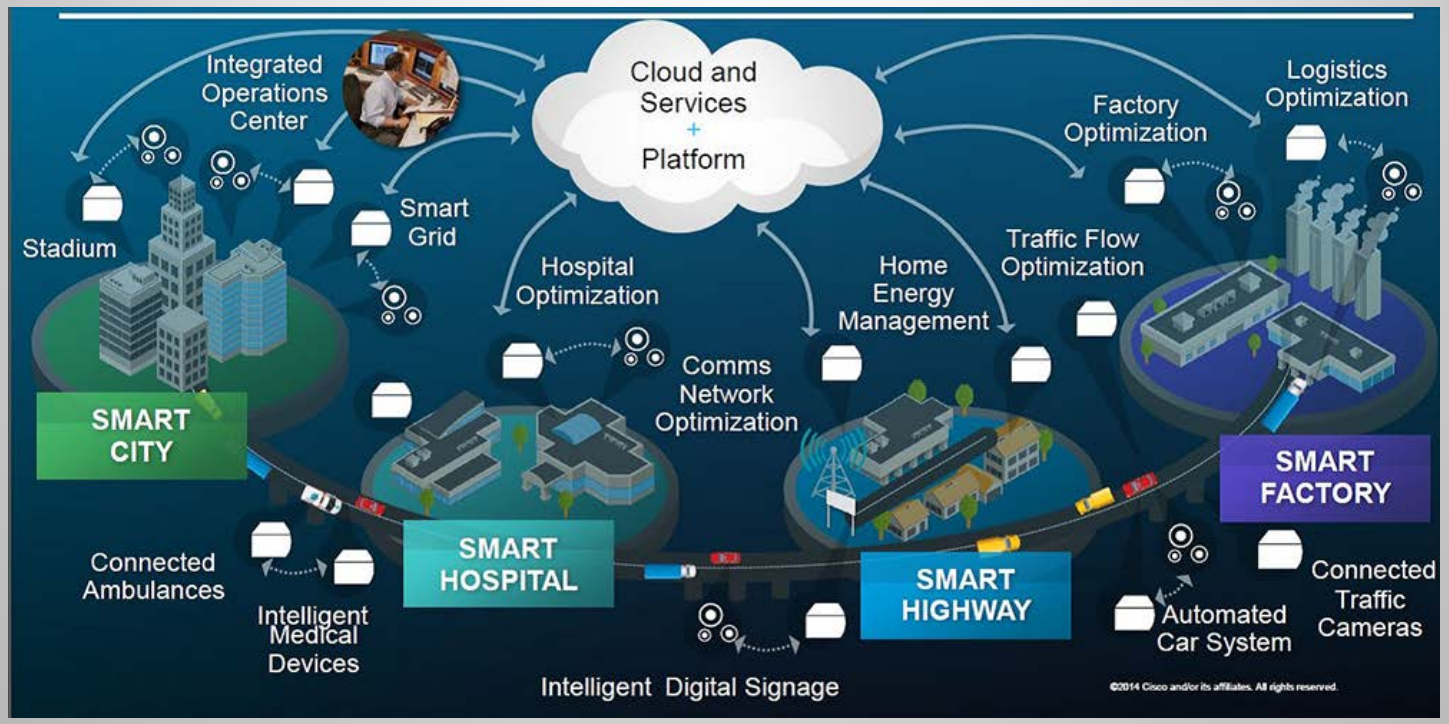
Lawrence Livermore National Laboratory



LLNL-PRES-722772

This work was performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under contract DE-AC52-07NA27344. Lawrence Livermore National Security, LLC

IoT Definition



Source: Cisco (Smart Cities)

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]

1 Brown, Eric (13 September 2016). "Who Needs the Internet of Things?". Linux.com. Retrieved 23 October 2016.
2 Eric (20 September 2016). "21 Open Source Projects for IoT". Linux.com. Retrieved 23 October 2016.
3 "Internet of Things Global Standards Initiative". ITU. Retrieved 26 June 2015

IoT Doubling by 2022

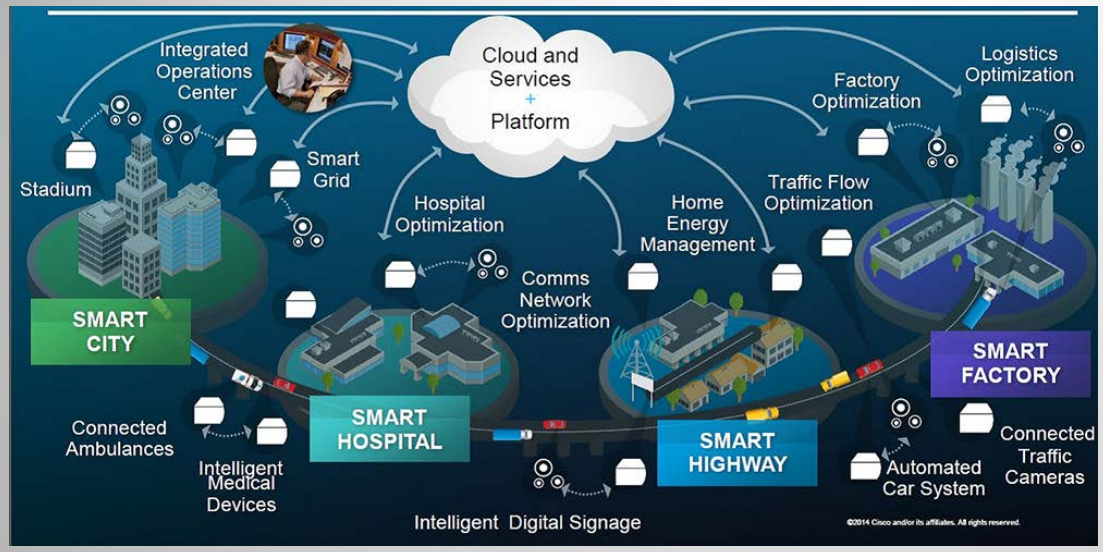
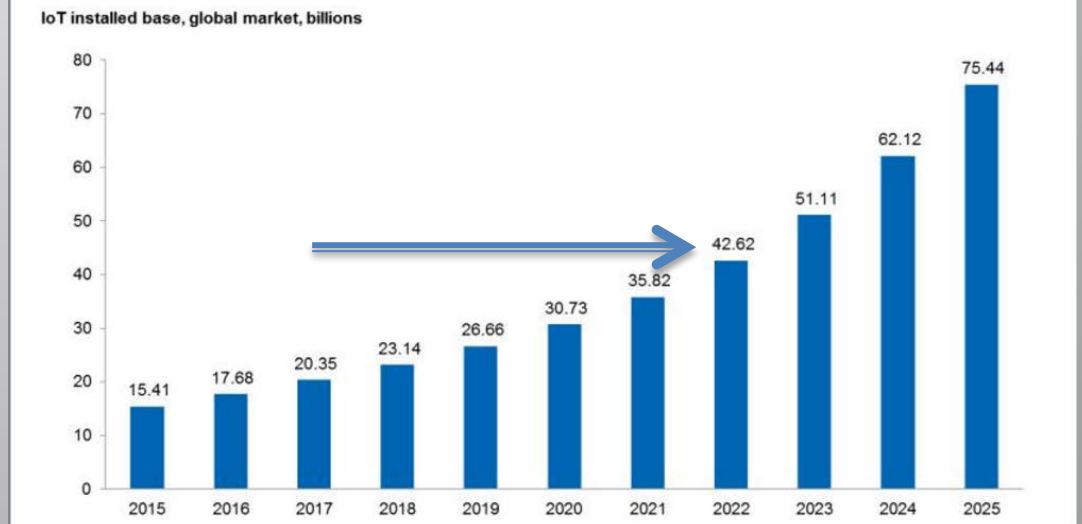
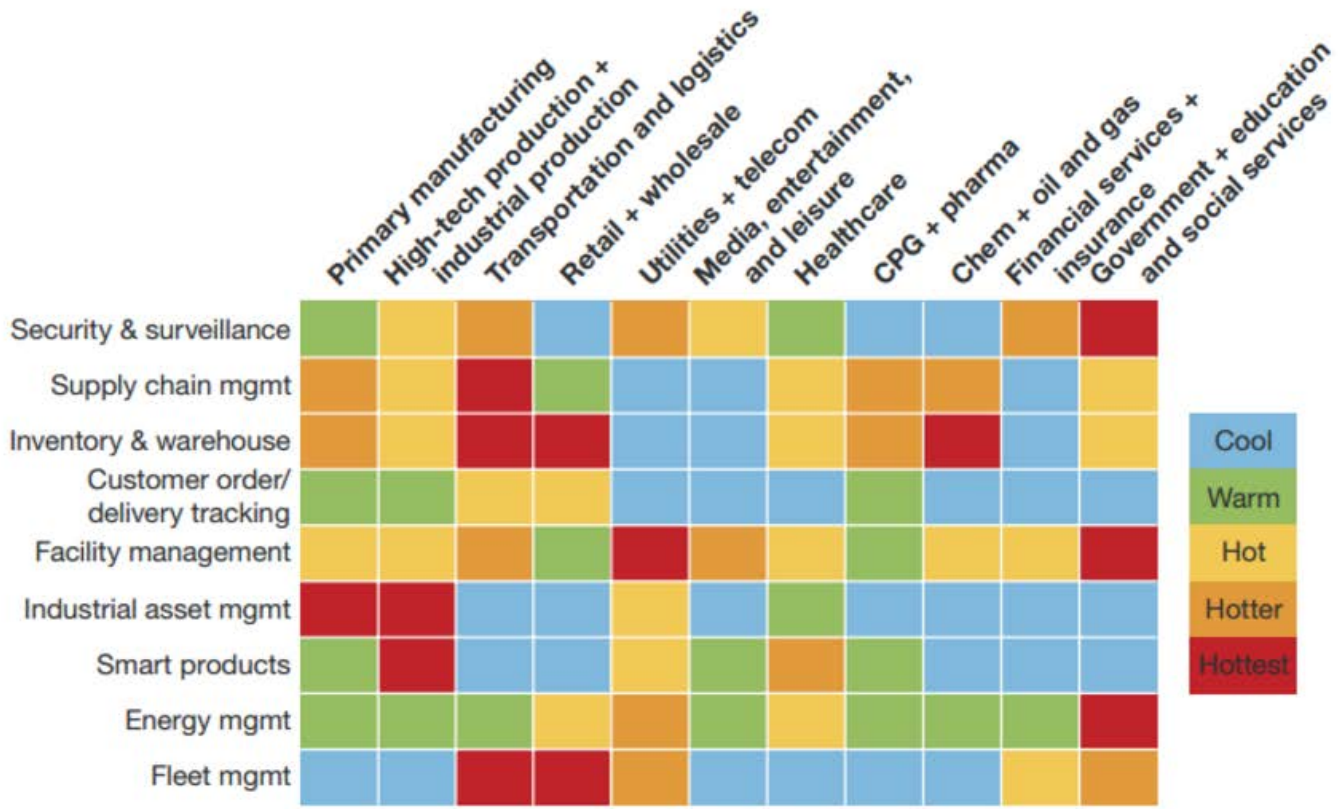


Figure 1. The IoT market will be massive



IoT Hot Spots Chart (Courtesy of Forrester Research, Inc.)

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



The Internet Of Things Heat Map, 2016 Where IoT Will Have The Biggest Impact On Digital Business by Michele Pelino and Frank E. Gillett January 14, 2016

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

1 J. M. Porup, https://arstechnica.com/security/2016/01/how-to-search-the-internet-of-things-for-photos-of-sleeping-babies/

Accident Prevention

- During software development identify:
  - Hazards → Accidents (Death, Injury)
  - Risks → Loss (Time, Money, Trust)
  - Vulnerabilities → Cyber Attack







Hazard Analysis Techniques - RCA

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

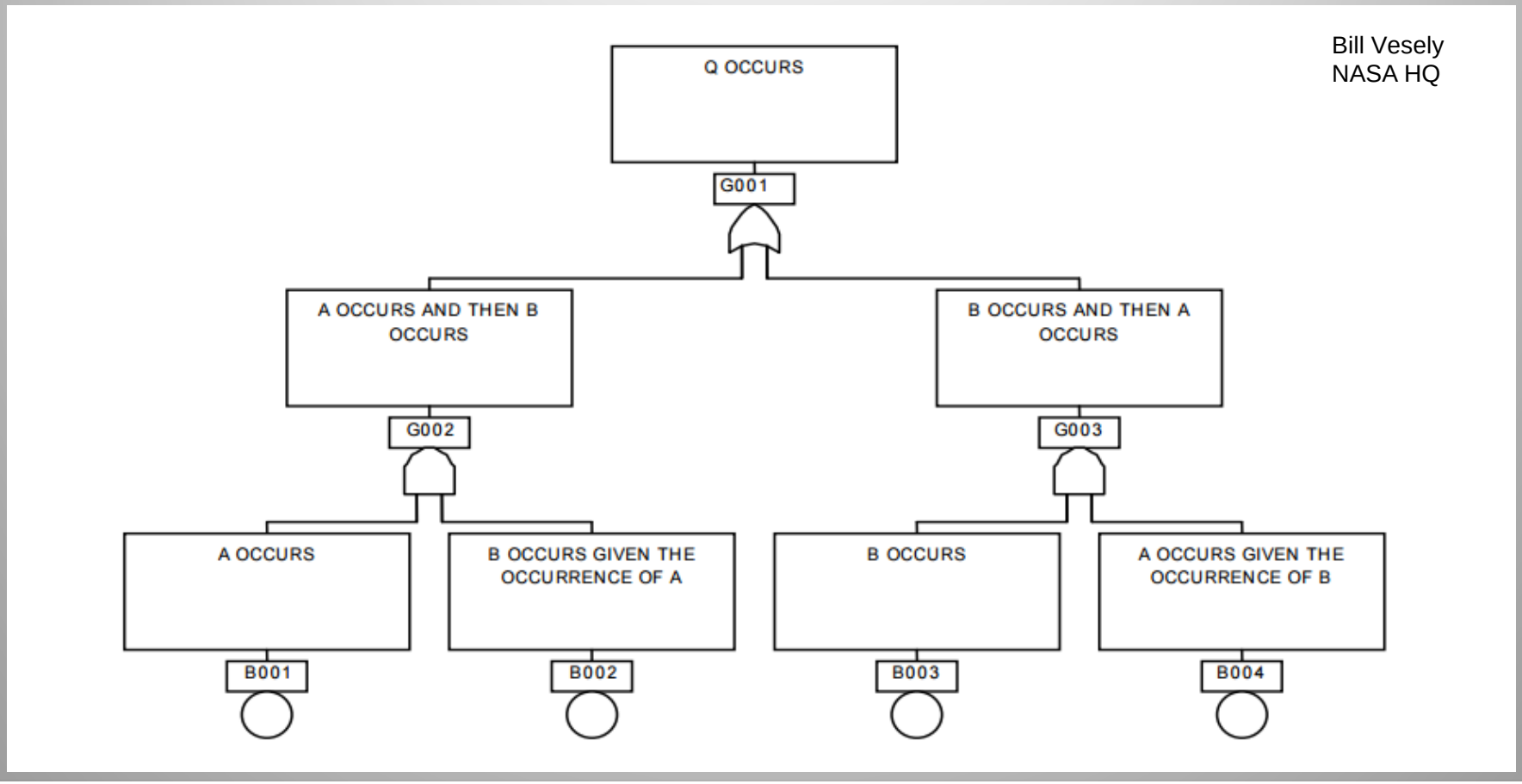
Failure Modes and Effect Analysis (FMEA) was developed by reliability engineers in the late 1950s to study problems that might arise from malfunctions of military systems.

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

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 the 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 inconspicuous 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.

Hazard Analysis Techniques - FTA

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



Google

2 Billion lines of code



12 Million
lines of code

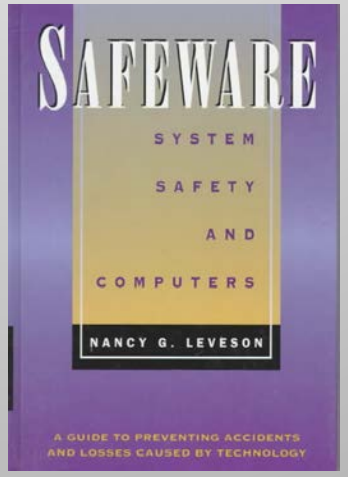
://wwhttpw.informationisbeautiful.net/visualizations/million-lines-of-code/

Software does not fail like hardware single point failures.

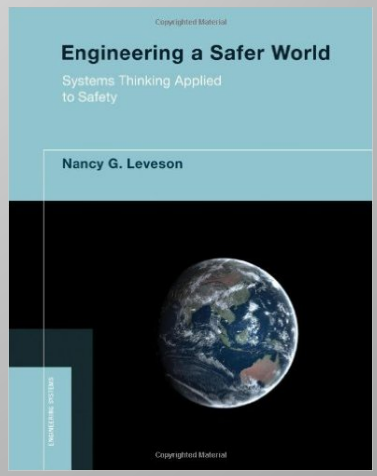


Nancy Leveson, MIT Aeronautics and Aerospace Professor

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



1995



2011

Hardware versus Software Over Time

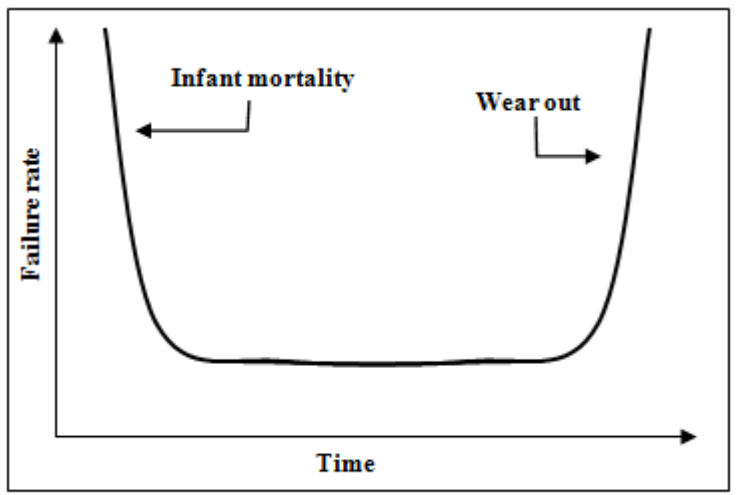


Figure 01: Failure curve for hardware

Hardware wears out

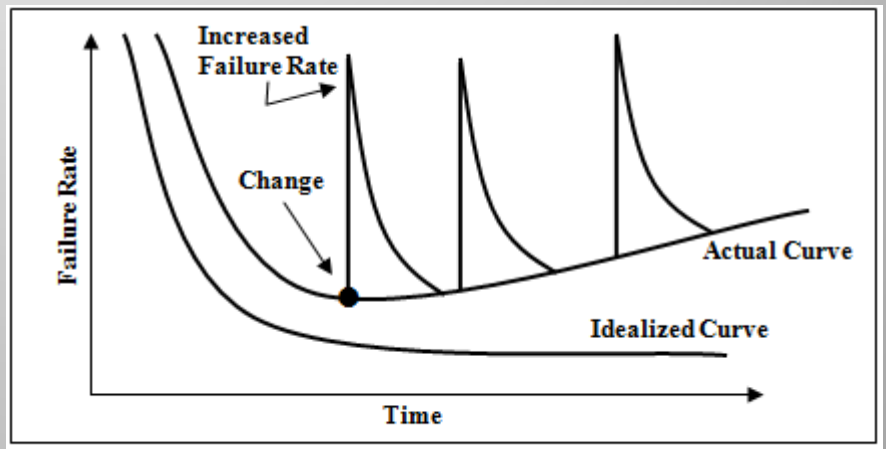


Figure 02: Failure Curves for software

http://www.onlineclassnotes.com/2013/01/software-doesnt-wear-out-explain-this.html

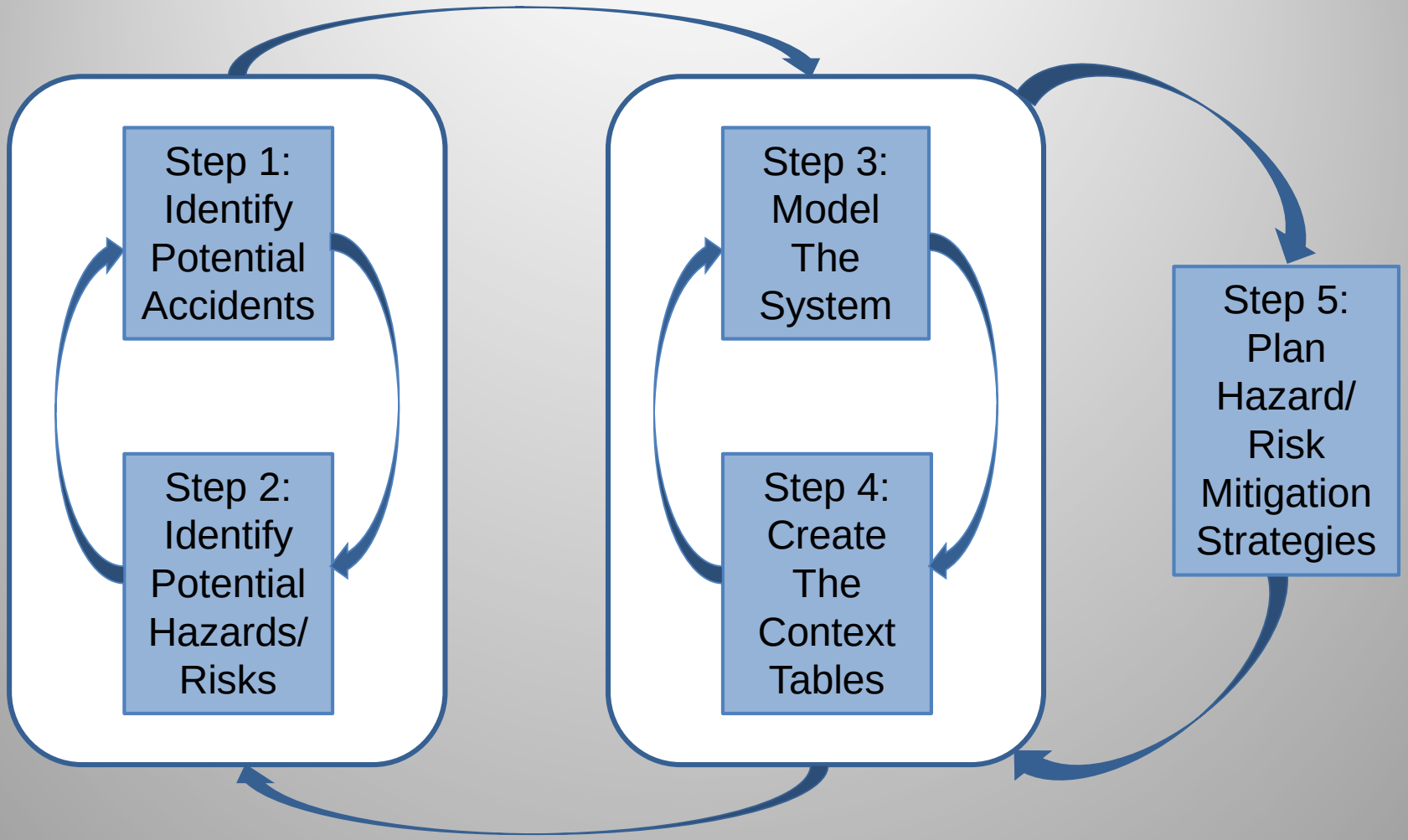
Software wears in

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



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



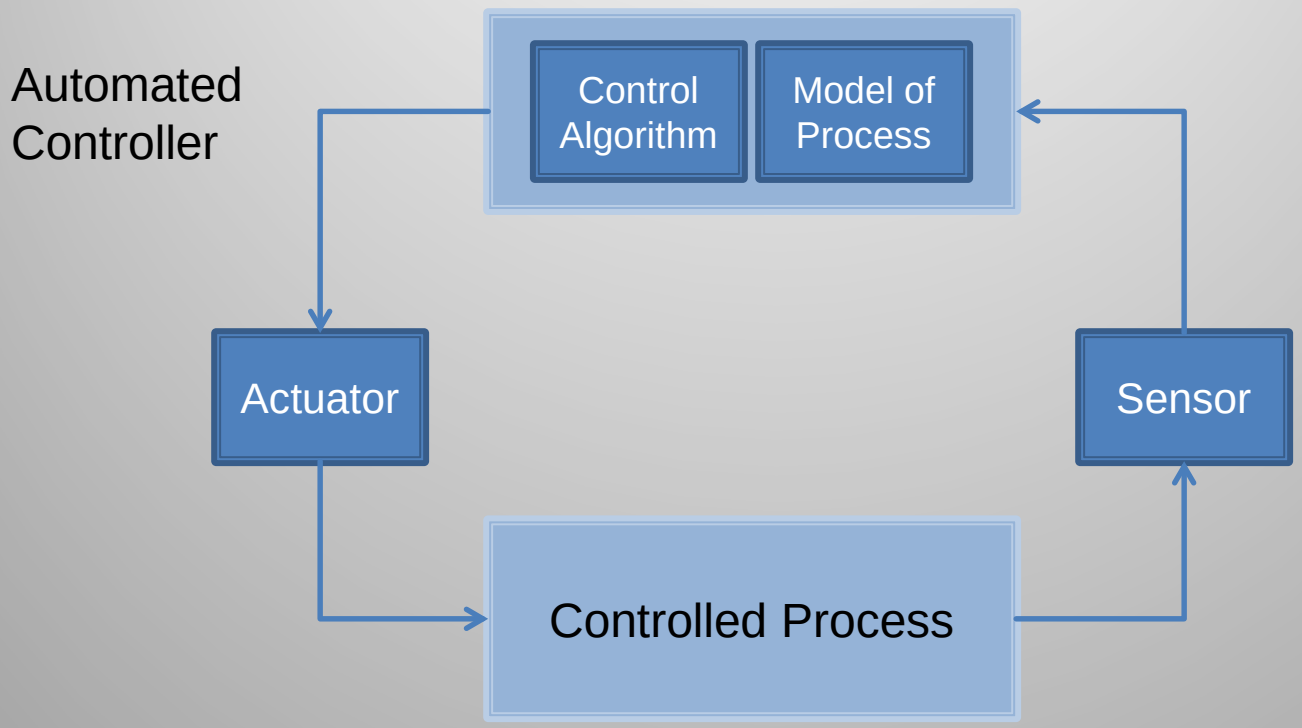
Step 2: Identify Potential Hazards/ Risks



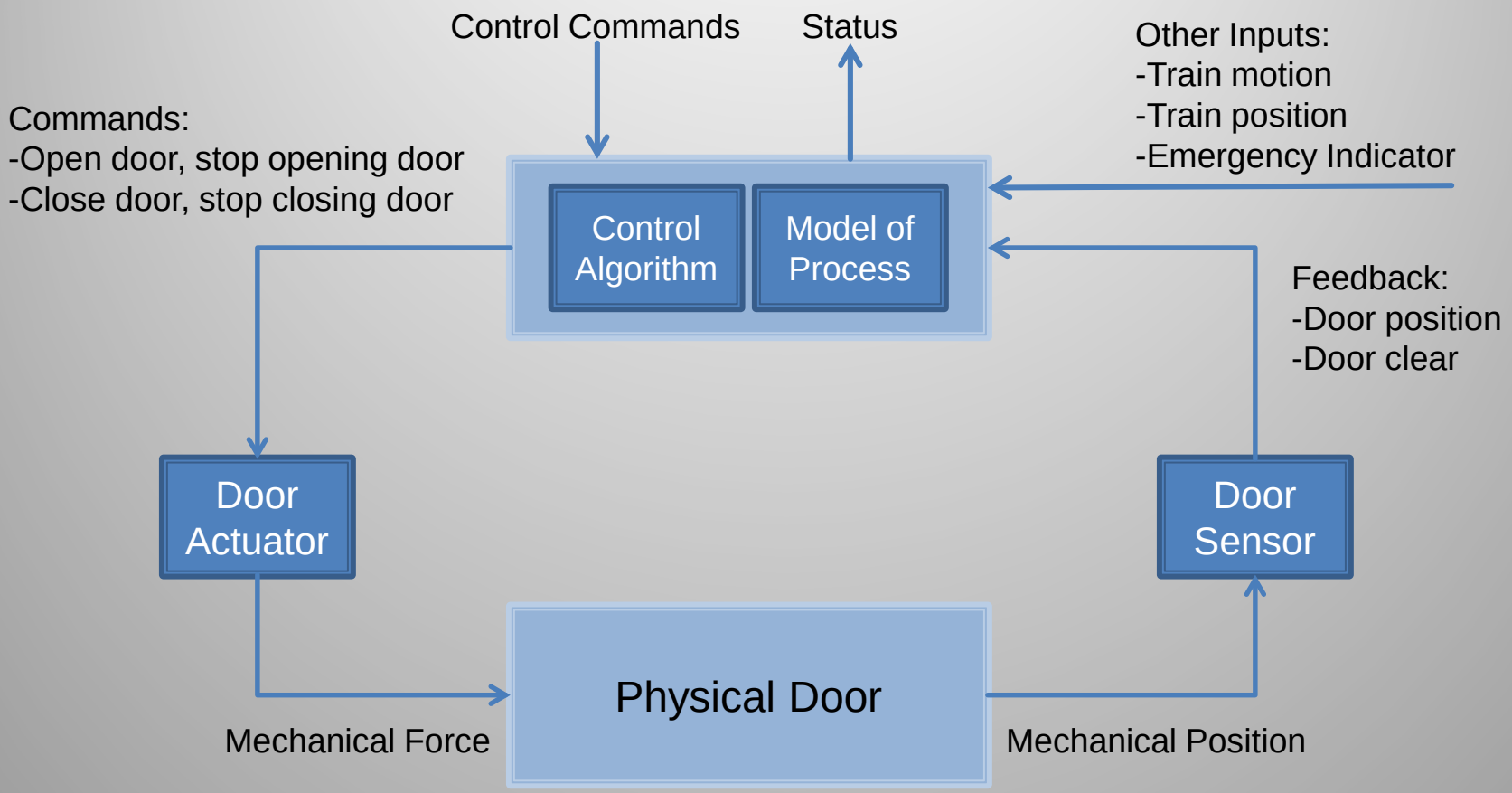
- H-1 Doors open when the train is moving (A-1)
- H-2 Doors close while person in the doorway (A-4)
- H-3 Doors stuck closed during emergency (A-2)
- H-4 Doors stuck open (A-1, A-3)
- H-5 Doors open when not aligned to platform (A-3)

STPA Control Structure Model

- Diagram the system as a control structure



Step 3: Model the Automated Door Controller System



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

Prefatory STPA context tables

Control Action	Train Motion	Train Position	Emer.	Door State	Hazard/ Risk
Open not provided	Stopped	Aligned	No	Person not in doorway	No
Open not provided	Stopped	Not Aligned	No	Person not in doorway	No
Open not provided	Stopped	Aligned	No	Person in doorway	Yes (H-2)
Open not provided	Stopped	Not Aligned	No	Person in doorway	No
Open not provided	Stopped	N/A	Yes	N/A	Yes (H-3)
Open not provided	Moving	N/A	N/A	N/A	No

Step 4: Create Context Table for Open Door Control Action

Prefatory STPA context tables

Control Action	Train Motion	Train Position	Emer.	Hazard/ Risk Any	Hazard/ Risk Early	Hazard/ Risk Late
Open	Moving	N/A	No	Yes (H-1)	Yes (H-1)	Yes (H-1)
Open	Moving	N/A	Yes	Yes (H-1)	Yes (H-1)	Yes (H-1)
Open	Stopped	N/A	Yes	No	No	Yes (H-3)
Open	Stopped	Not Aligned	No	Yes (H-5)	Yes (H-5)	Yes (H-5)
Open	Stopped	Aligned	No	No	No	No

Step 5: Plan Hazard/Risk Mitigation Strategies

Prefatory STPA Analysis of context tables

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

Context Tables Using Spreadsheet, Exhaustive STPA Approach

	Open Provided																														
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	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Aligned:	T	T	T	T	T	T	T	T	F	F	F	F	F	F	F	F	T	T	T	T	T	T	T	T	F	F	F	F	F	F	F	F
Emergency:	F	F	F	F	T	T	T	T	F	F	F	F	T	T	T	T	F	F	F	F	T	T	T	T	F	F	F	F	T	T	T	T
Doorway Obstructed	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
Doorway Closed	T	F	T	F	T	T	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
Hazard (Me)	N	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
Hazard (Chart)	N	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
Hazard (Equation)	N	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

Open Provided

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
Stopped:	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	F
Aligned:	T	T	T	T	T	T	T	T	F	F	F	F	F	F	F	F	T	T	T	T	T	T	T	T	F	F	F	F	F	F	F	F
Emergency:	F	F	F	F	T	T	T	T	F	F	F	F	T	T	T	T	F	F	F	F	T	T	T	T	F	F	F	F	T	T	T	T
Doorway Obstructed	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
Doorway Closed	T	F	T	F	T	T	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
Hazard (Me)	N	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
Hazard (Chart)	N	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
Hazard (Equation)	N	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

Open Provided

Case	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64
Stopped:	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	F
Aligned:	T	T	T	T	T	T	T	T	F	F	F	F	F	F	F	F	T	T	T	T	T	T	T	T	F	F	F	F	F	F	F	F
Emergency:	F	F	F	F	T	T	T	T	F	F	F	F	T	T	T	T	F	F	F	F	T	T	T	T	F	F	F	F	T	T	T	T
Doorway Obstructed	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
Doorway Closed	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
Hazard (Me)	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N	Y	Y	Y	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
Hazard (Chart)	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N	Y	Y	Y	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
Hazard (Equation)	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N	Y	Y	Y	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N

Open Not Provided

Case	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96
Stopped:	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	F
Aligned:	T	T	T	T	T	T	T	T	F	F	F	F	F	F	F	F	T	T	T	T	T	T	T	T	F	F	F	F	F	F	F	F
Emergency:	F	F	F	F	T	T	T	T	F	F	F	F	T	T	T	T	F	F	F	F	T	T	T	T	F	F	F	F	T	T	T	T
Doorway Obstructed	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
Doorway Closed	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
Hazard (Me)	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N	Y	Y	Y	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
Hazard (Chart)	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N	Y	Y	Y	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
Hazard (Equation)	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N	Y	Y	Y	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N

Open Provided Too Late or Out of Sequence

98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127	128
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	F
T	T	T	T	T	T	T	F	F	F	F	F	F	F	T	T	T	T	T	T	T	T	F	F	F	F	F	F	F	F	F
F	F	F	T	T	T	F	F	F	F	T	T	T	F	F	F	F	T	T	T	T	F	F	F	F	T	T	T	T	T	T
F	T	T	F	F	T	T	F	F	T	T	T	F	T	T	F	F	T	F	F	T	T	T	F	F	T	F	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
Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Open Stopped Too Soon or Applied Too Long

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")

	And / Or Chart			
		Or		
	Stopped	F	T	
	Aligned		F	
And	Emergency		F	
	Obstructed			
	Closed			
	Use null (del) or blank for d			

Open Not Provided When:
Stopped = "F" Or (Stopped = "T" And Aligned = "F" And Alarm = "F") Or (Stopped = "T" And Closed = "F")

	And / Or Chart			
		Or		
	Stopped	T	T	T
	Aligned	T	F	T
And	Alarm		T	
	Obstructed			T
	Closed			
	Use null (del) or blank for do			

Automation of Context Table Analysis

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

	And / Or Chart			
		Or		
	Stopped	T	T	T
	Aligned	T	T	F
And	Alarm			T
	Obstructed		T	
	Closed			
	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")

	And / Or Chart			
		Or		
	Stopped	T	F	
	Aligned			
And	Alarm			
	Obstructed			
	Closed			

The Hazomatic

Automated Context Table with And/Or Charts

	Open Provided	Open Provided	Open Provided	Open Provided	Open Provided	Open Provided	Open Provided	Open Provided	Open Provided	Open Provided	Open Provided	Open Provided	Open Provided	Open Provided	Open Provided	Open Provided	Open Provided	Open Provided	Open Provided	Open Provided	Open Provided	Open Provided	Open Provided	Open Provided	Open Provided	Open Provided	Open Provided	Open Provided	Open Provided	Open Provided	Open Provided	Open Provided
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	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
Aligned:	T	T	T	T	T	T	T	T	F	F	F	F	F	F	F	F	T	T	T	T	T	T	T	T	F	F	F	F	F	F	F	F
Emergency:	F	F	F	F	T	T	T	T	F	F	F	F	T	T	T	T	F	F	F	F	T	T	T	T	F	F	F	F	T	T	T	T
Doorway Obstructed	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
Doorway Closed	T	F	T	F	T	T	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
Hazard (Me)	N	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
Hazard (Chart)	N	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
Hazard (Equation)	N	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

And / Or Chart

Or

And			
Stopped	F	T	
Aligned		F	
Emergency		F	
Obstructed			
Closed			

Use null (del) or blank for d

Hazards

20 Hazomatic

20

20 Clear

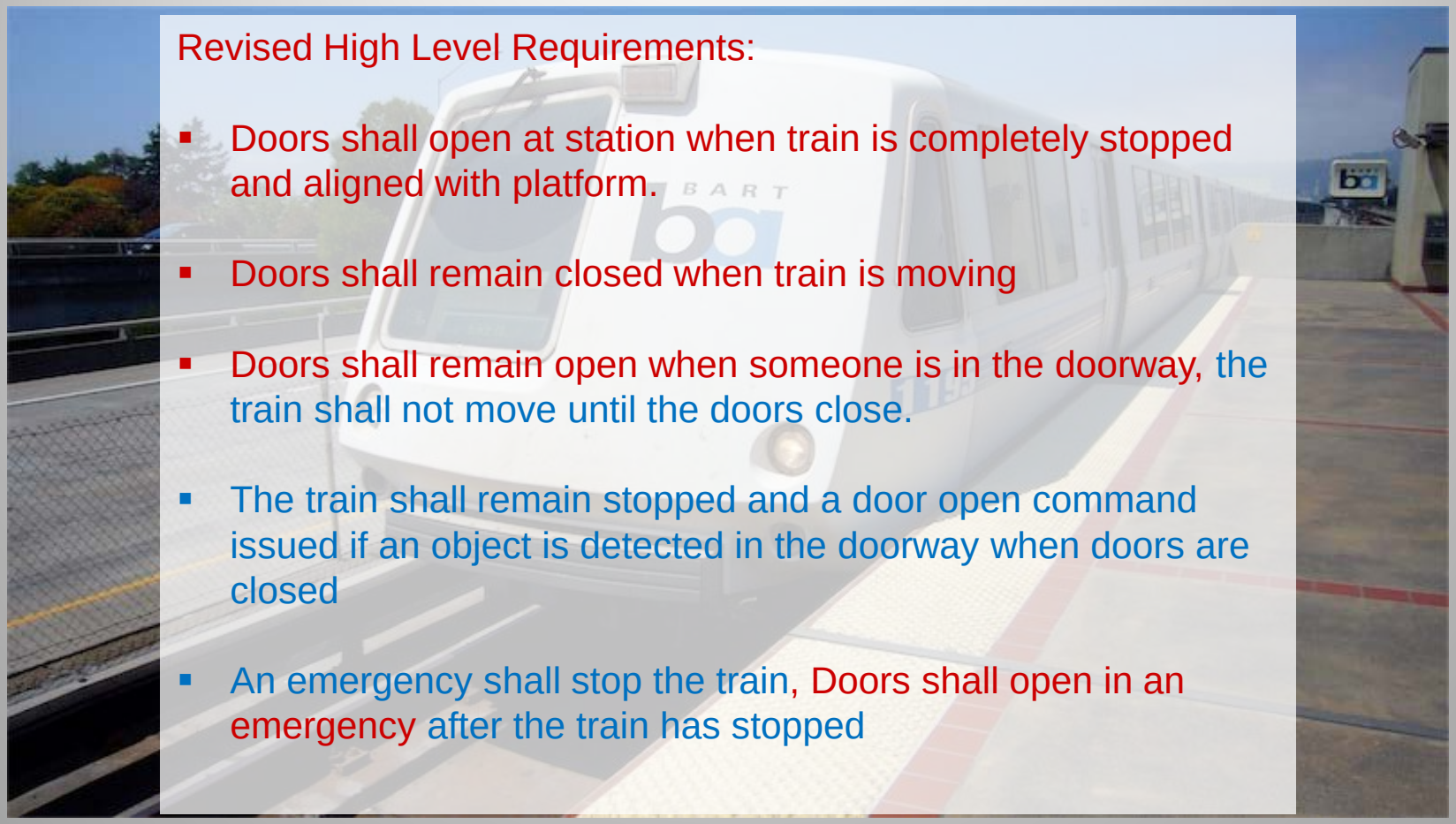
Exhaustive Context Tables Analysis

- Number of Combinations = 128
  - s = number of binary states
  - g = number of guide phrases
  - Combinations = 2^s x g = 2^5 x 4 = 128
- Number of Potential Hazards Combinations:

	me	and/or	equation
Open Provided =	20	20	20
Open Not Provided =	12	12	12
Open Too Late or Out of Sequence =	12	12	12
Open Stopped Too Soon Applied Too Long =	32	32	32
Total	76	76	76

- 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



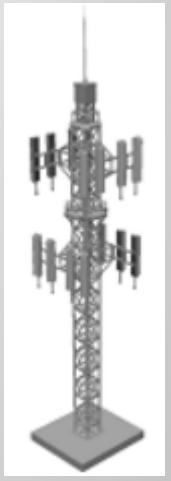
Thermostat



CO Detector



Home Wi-Fi Router



Cell Tower



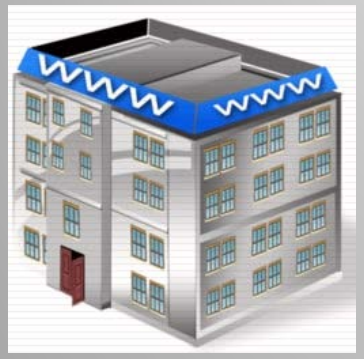
Smart Phone



Dash Button



Alarm System



Internet Service Provider



Camera Front Door



Camera Driveway



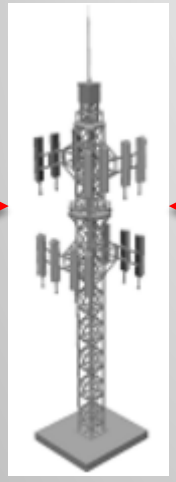
Vehicles



Motion Detection

Turn Down The Air Conditioning When No One is Home





Cell Tower



Internet Service Provider



Home Wi-Fi Router

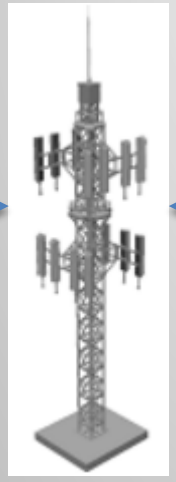


Thermostat

Lower Utility Bills
Energy Preservation

Turn Down Air Conditioning If No Motion for an Hour





Cell Tower



Internet Service Provider



Home Wi-Fi Router



Thermostat

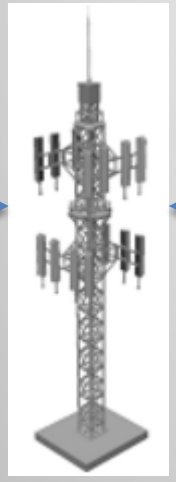
Lower Utility Bills
Energy Preservation



Motion Detection

Turn Down Air Conditioning if Burglar Alarm Set To Away





Cell Tower



Internet Service Provider



Home Wi-Fi Router



Thermostat

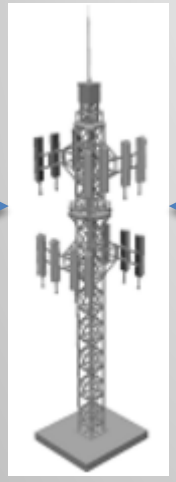
Lower Utility Bills
Energy Preservation



Alarm System

Is Teen Driver Home Yet?





Cell Tower



Internet Service Provider



Home Wi-Fi Router



Camera Driveway

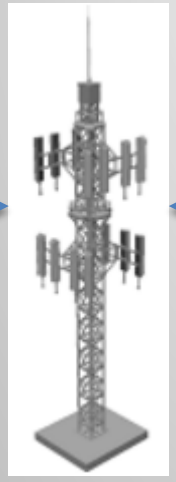
Safety
Win Arguments With Teens



Motion Detection

Turn Off Gas Source If CO Detected





Cell Tower



Internet Service Provider



Home Wi-Fi Router



Thermostat

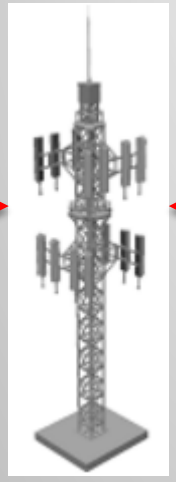
Safety



CO Detector

On Vacation





Cell Tower



Internet Service Provider



Home Wi-Fi Router

Security



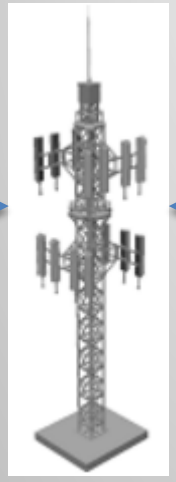
House Sounds



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

Self Driving Trucks and Cars

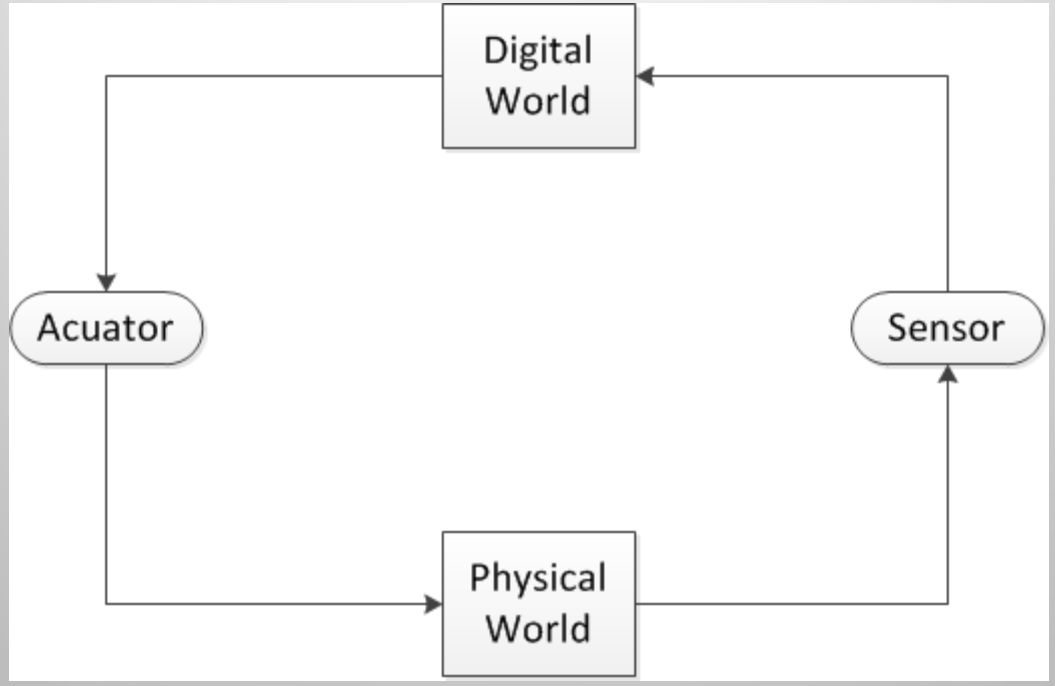


Safety
Security
Energy Preservation

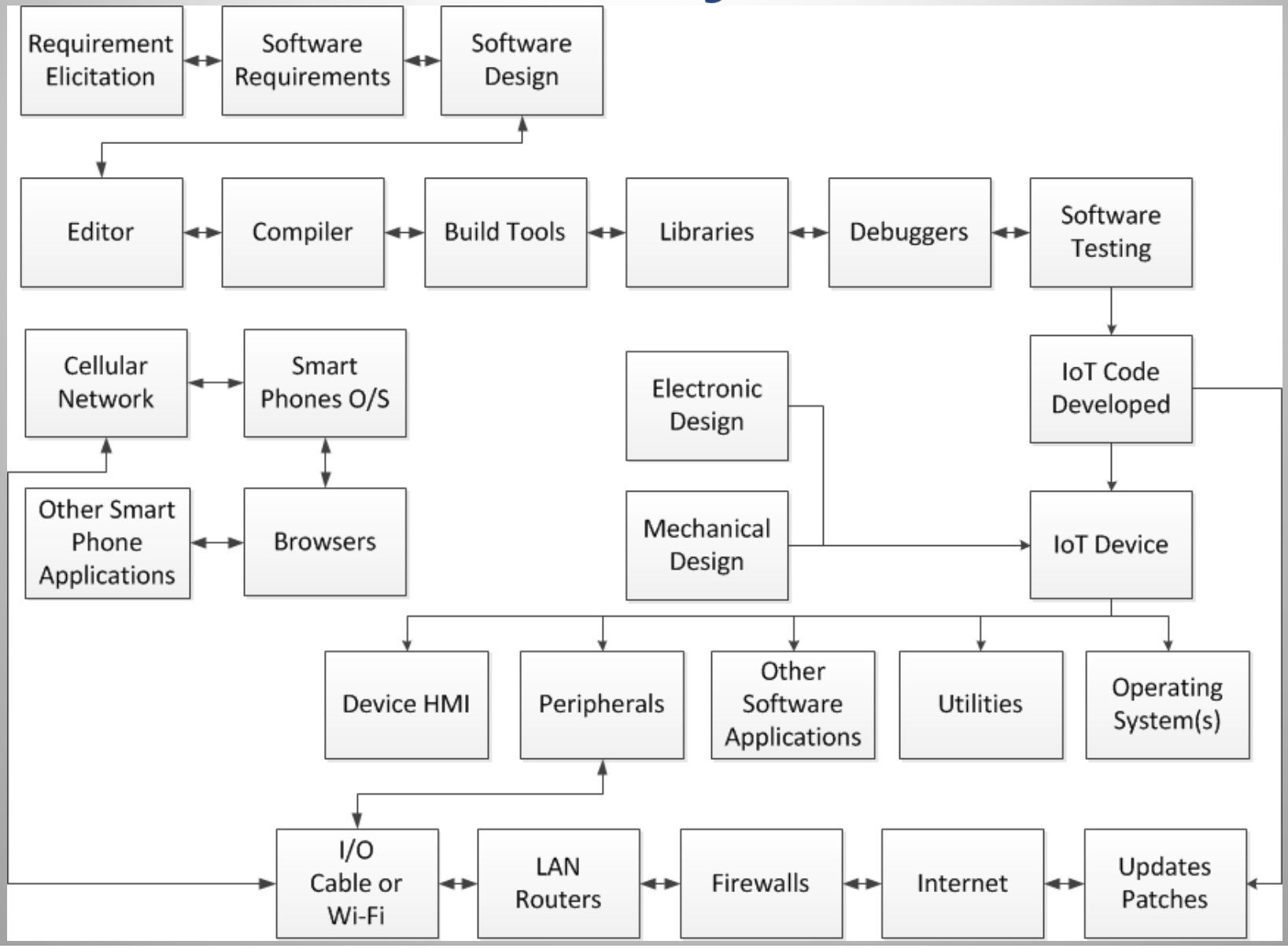
Is STPA Useful for IoT Vulnerability Analysis?

- 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

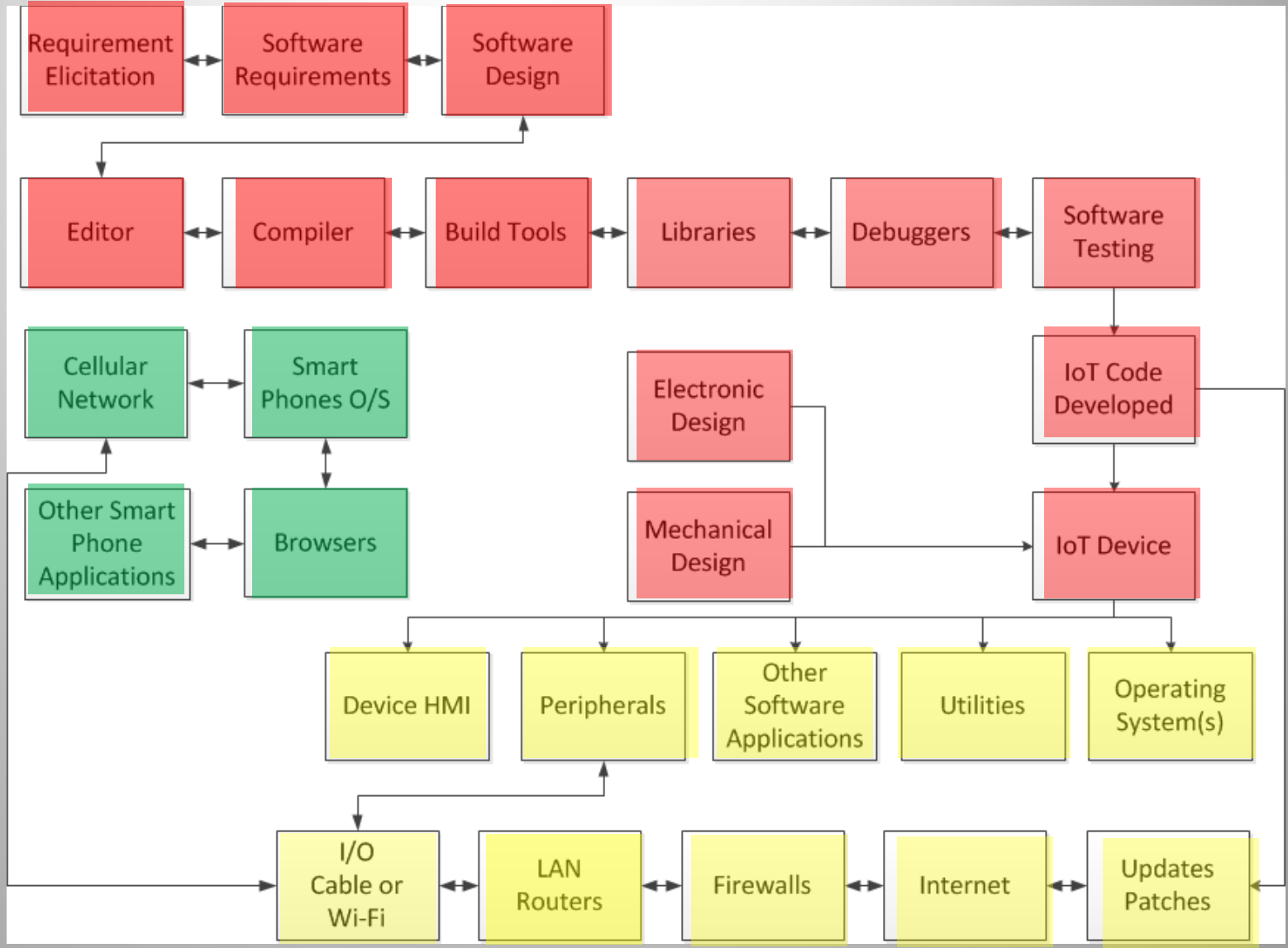


IoT Basic Device Physical Model

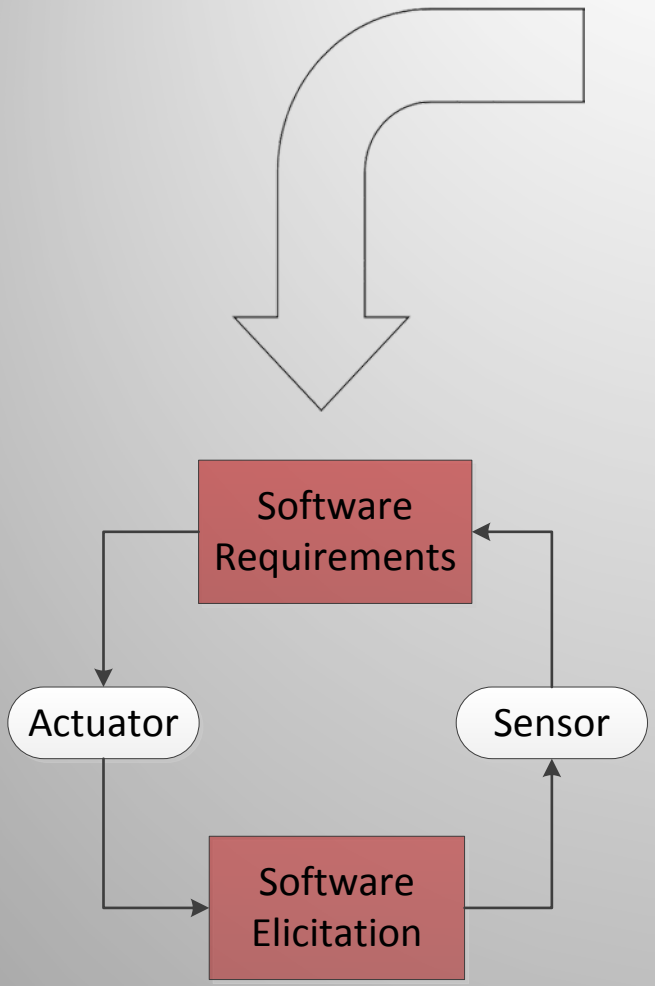
Development Subsystem

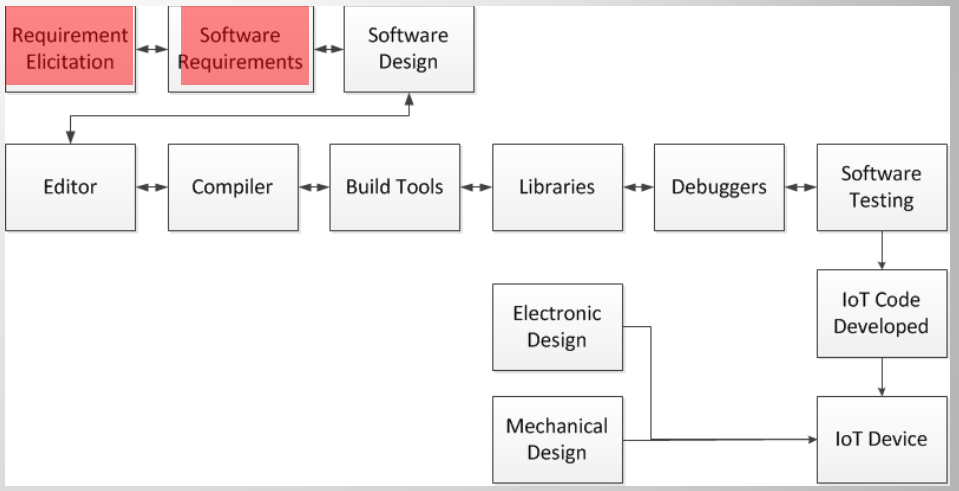
Mobile Phone Subsystem

External Communications Subsystem



Development Sub-Subsystem





Development Sub-Subsystem Analysis

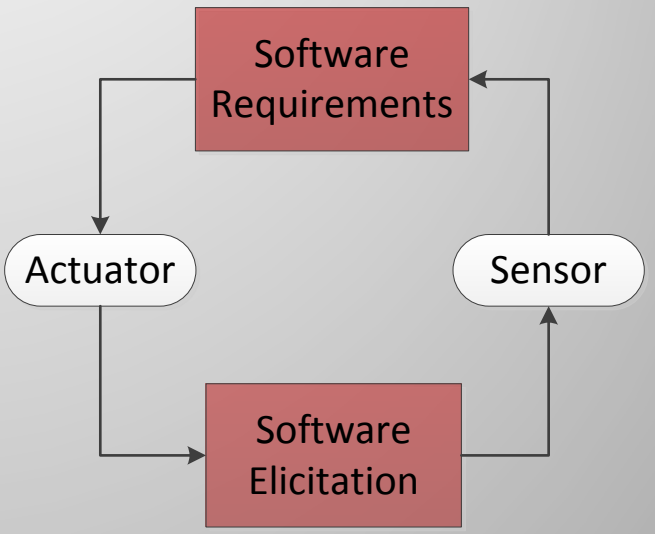
STPA Guide Phrases

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.

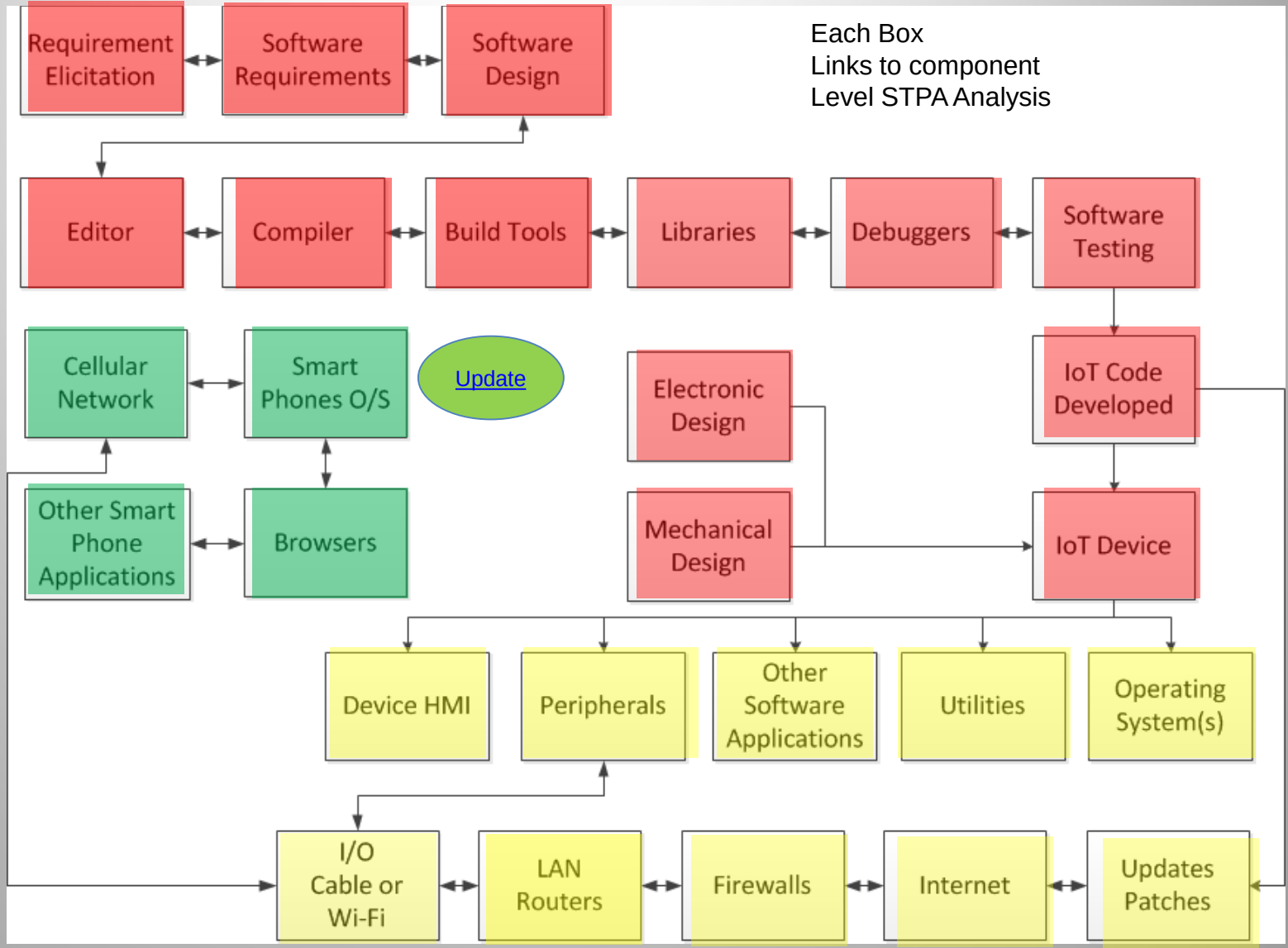


IoT Basic Device Physical Model

Development Subsystem

Mobile Phone Subsystem

External Communications Subsystem



Combinations of Things That Could Go Wrong in IoT

Physical Model	Risks	Comb.	Average
Development Risks	110	94592	9.2
Communications Risk	64	6080	6.4
Mobile Risks	27	1424	5.4
Total	201	102096	7.0

Assume “or” of all three

Assume “and” of all

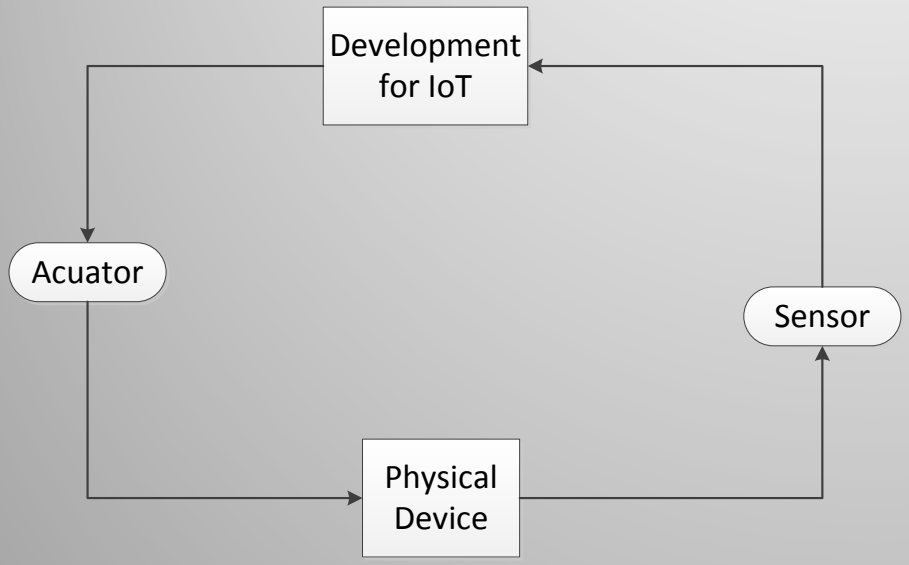
s = number of binary states
g = number of guide phrases
Combinations = 2^s x g = 2^{201} x 4 = ####

Age of the Universe in Plank time 8E+60
Plank time = 10E-43 seconds

Estimated number of electrons in the universe =10E+88

Using Surrogates for STPA of IoT

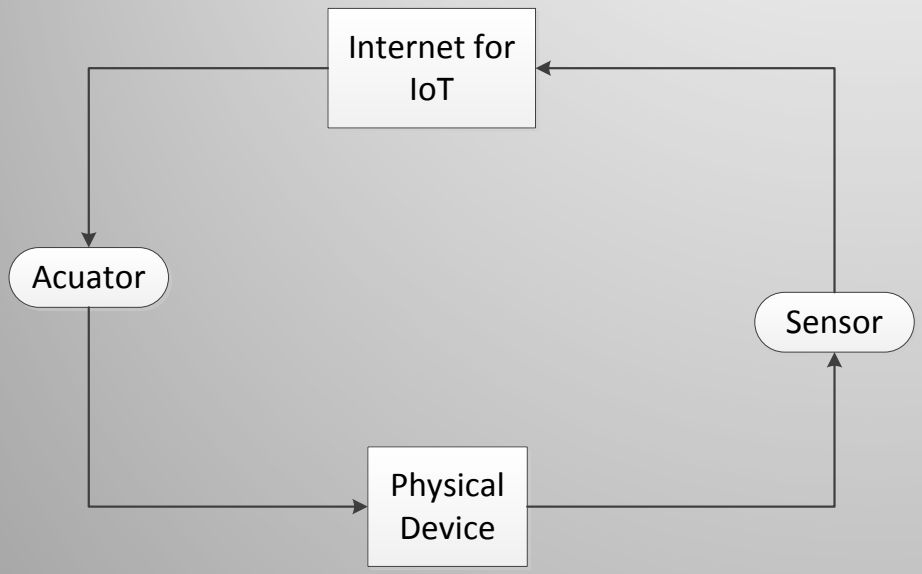
- Representative STPA which represents all the analyzed components of the physical model:



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

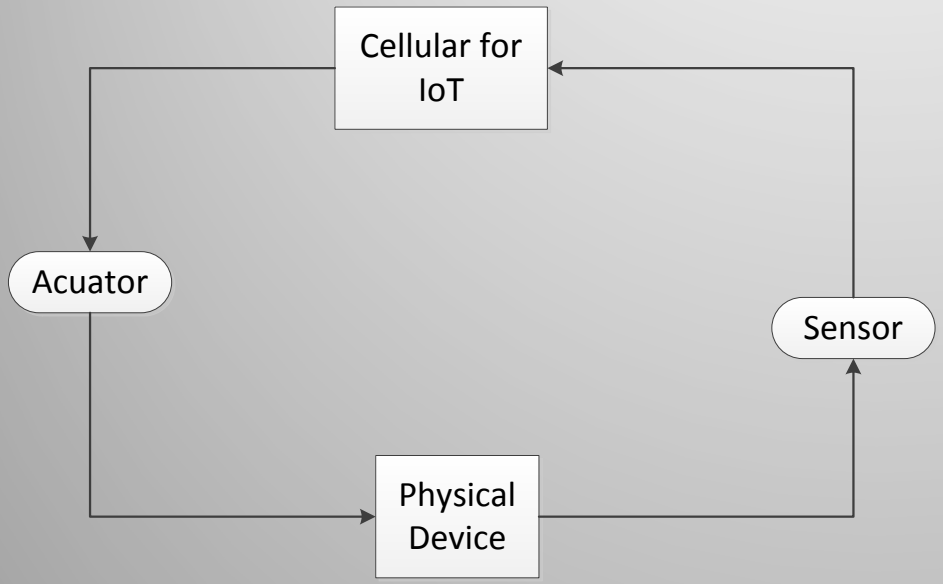
- Representative STPA which represents all the analyzed components of the physical model:



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

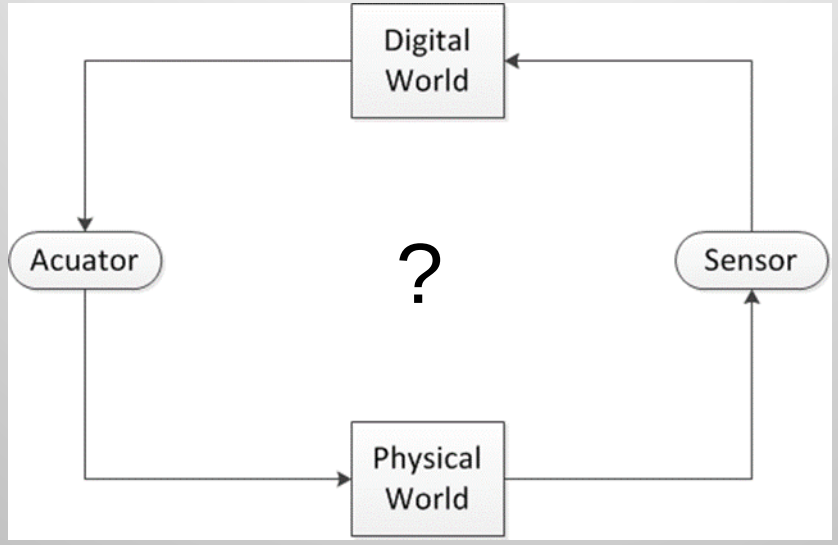
Using Surrogates for STPA of IoT

- 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

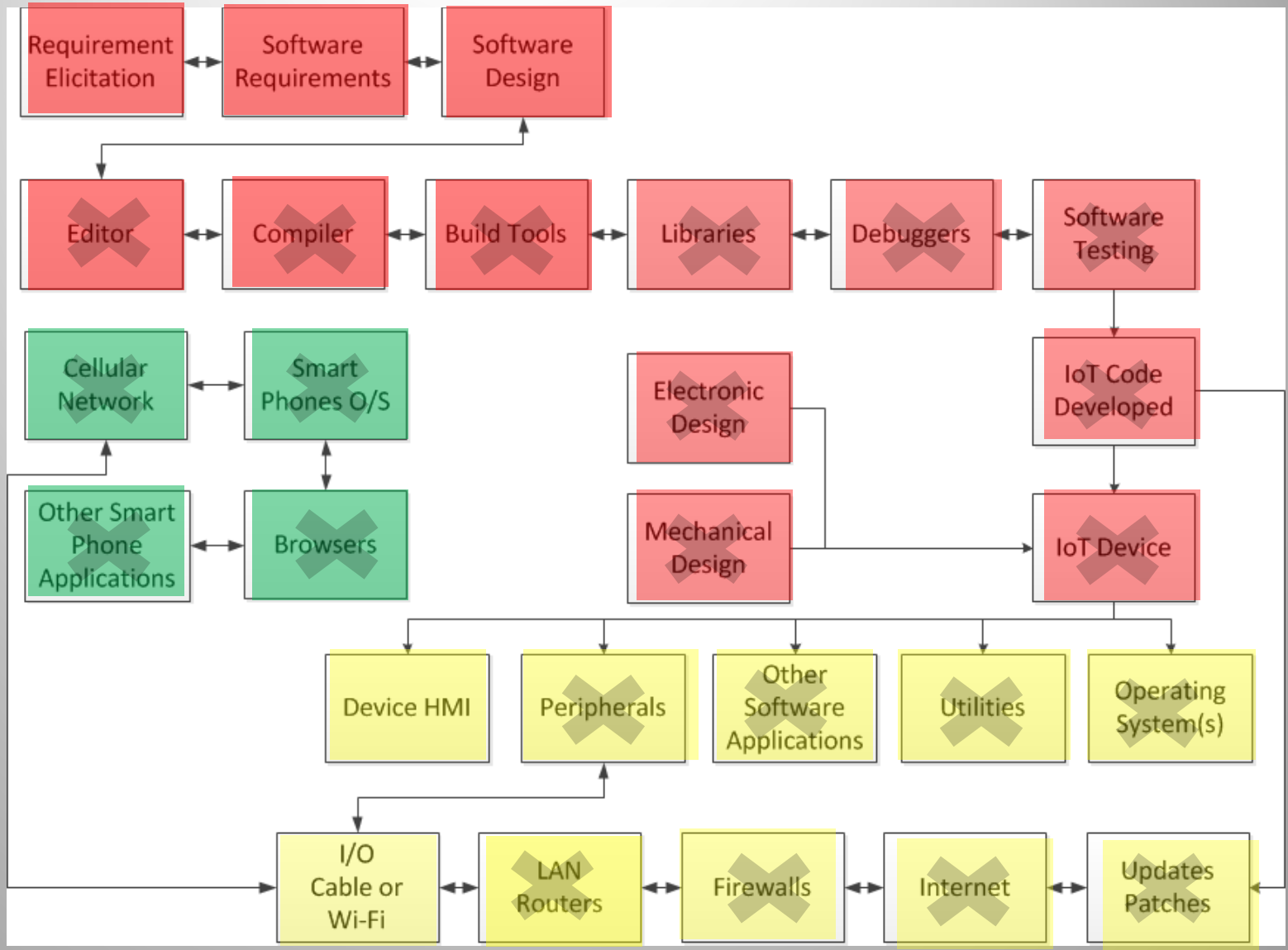
Good News:
"Apple Home Kit"
"Works With Nest"
} Emerging Standards

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	Entertain-ment 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

Update Dilemma Times 22

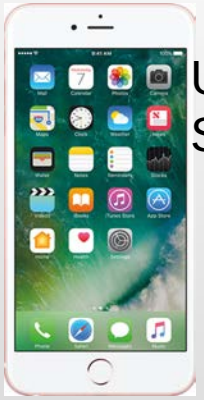


Obsolesce Update Story

https://www.wired.com/2017/02/russians-engineer-brilliant-slot-machine-cheat-casinos-no-fix/



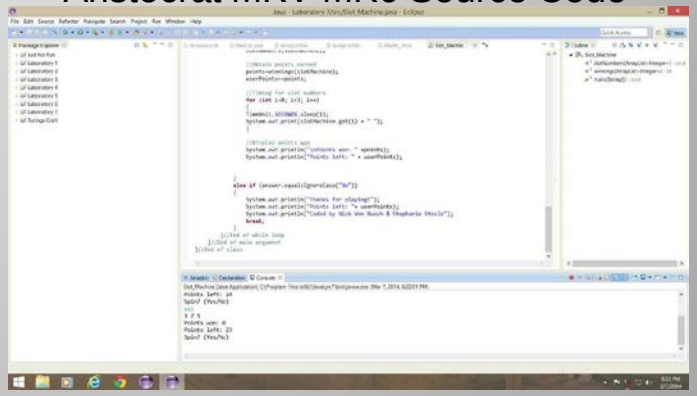
2 Min. Video



Upload to St. Petersburg



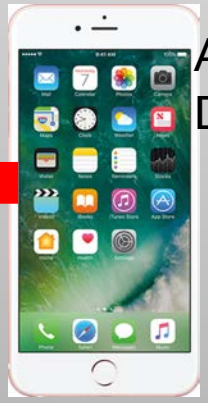
Aristocrat MKV MK6 Source Code

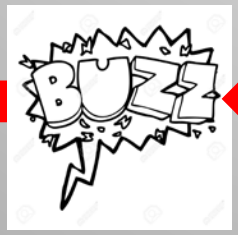


Aristocrat MKV MK6 Backplane Board

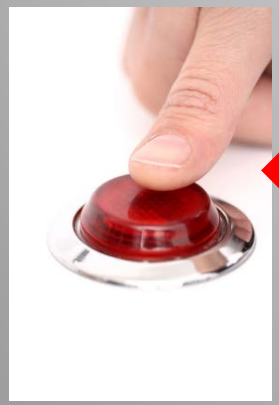


App Download





.25



Vehicles As Weapons, e-Jacking





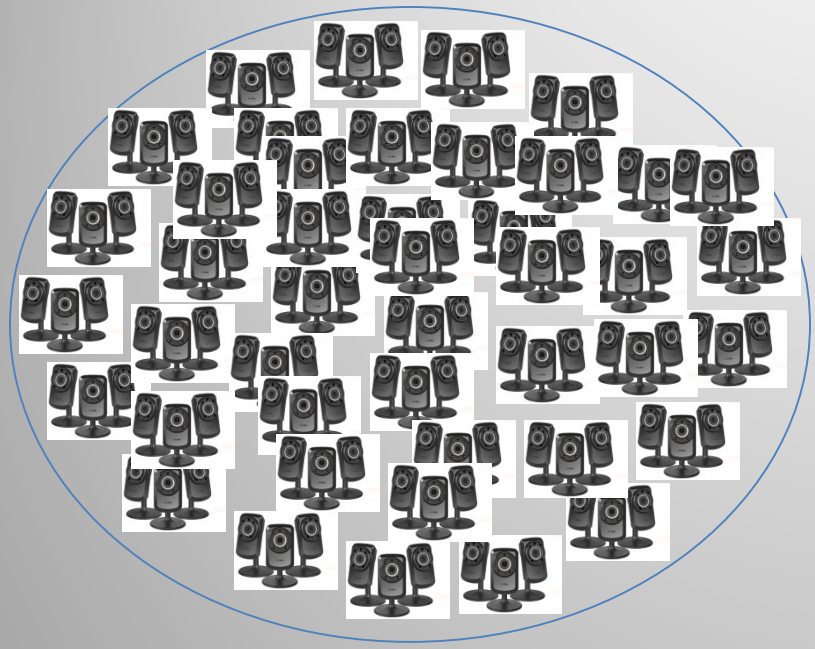
http://www.express.co.uk/news/world/600771/ISIS-Islamic-State-remote-controlled-cars-bomb-attacks-Syria-Iraq-drones-Britain

Wireless Carjacking

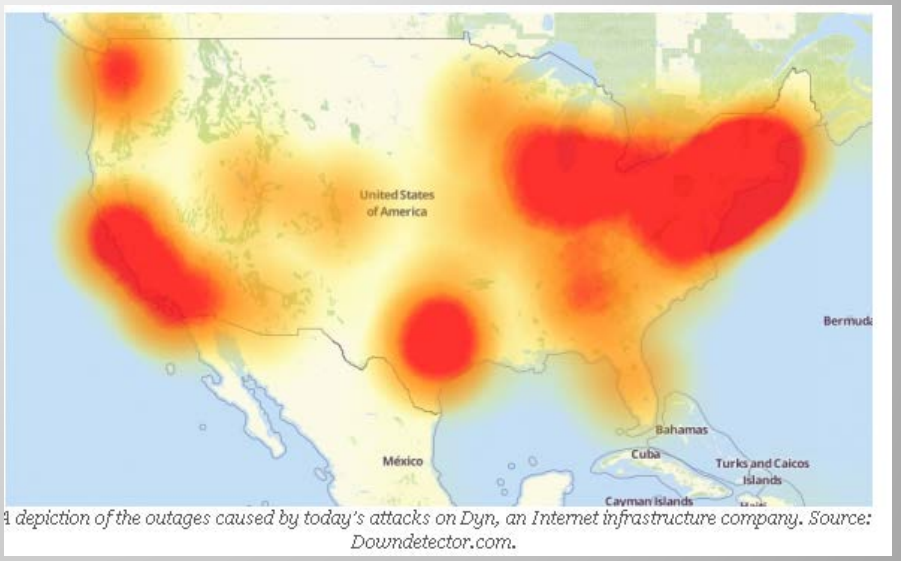


https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/#slide-2

DDoS Attacks – Bots Gone Wild



Video Cameras



A depiction of the outages caused by today's attacks on Dyn, an Internet infrastructure company. Source: Downdetector.com.

Wide Spread Internet Outages

https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/

Ransomware of Things (RoT)

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

OR



454,545 toasters
x 1,100 watts per toaster

=



500 Megawatts

Wide Spread Power Disruption

IoT Click and Enter Burglary





Assure No One Home

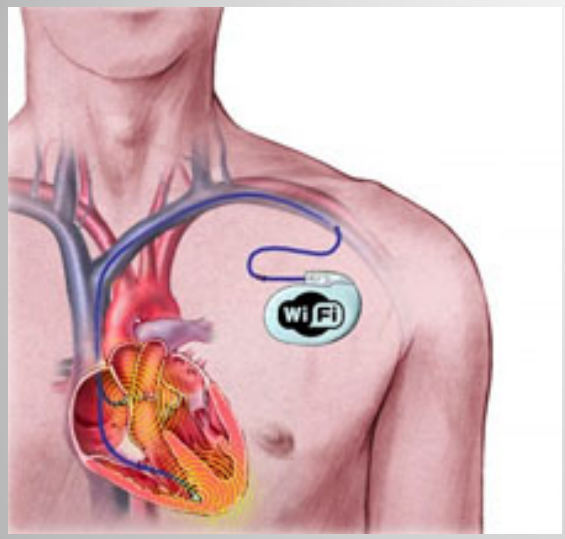
Disable Alarms
Open Doors

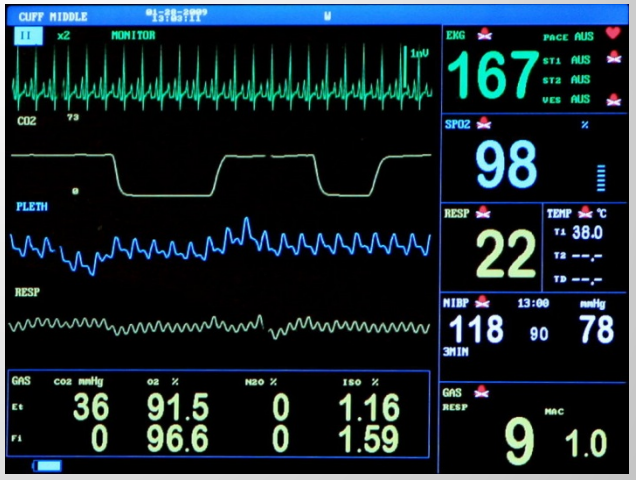




Self Parking Get Away Car

IoT Medical Race Condition







Send Ambulance



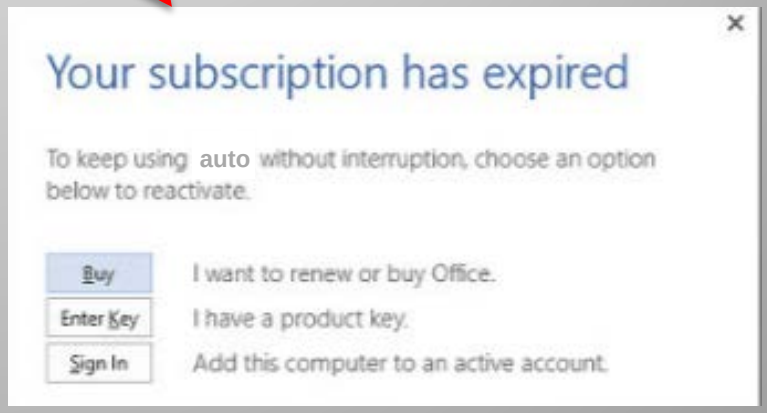
Increase Premium

Telltale heart: Pacemaker data leads to arson, fraud charges

http://www.foxnews.com/us/2017/02/08/police-use-data-on-mans-pacemaker-to-charge-him-with-ohio-arson.html

IoT Inconvenient Subscription Renewals





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?

IoT Monthly Auto Insurance Rates





Cell Tower



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





IoT New Meaning for Blue Screen of Death





Telecommunications and Web Software yet to be Mission Critical Level

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

Donald Reifer, "Industry Software Cost, Quality, and Productivity Benchmarks", DoD Software Tech News, July 2004

2016 Benchmark for Telecommunications and Web Getting Better – Donald Reifer



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

Year	2006 to 2008	2008 to 2010	2010 to 2012	2012 to 2014	2014 to 2016
Defects/KESLOC	4.0	3.4	2.9	2.3	1.6

Average Defects/KESLOC for Commercial - Telecommunications

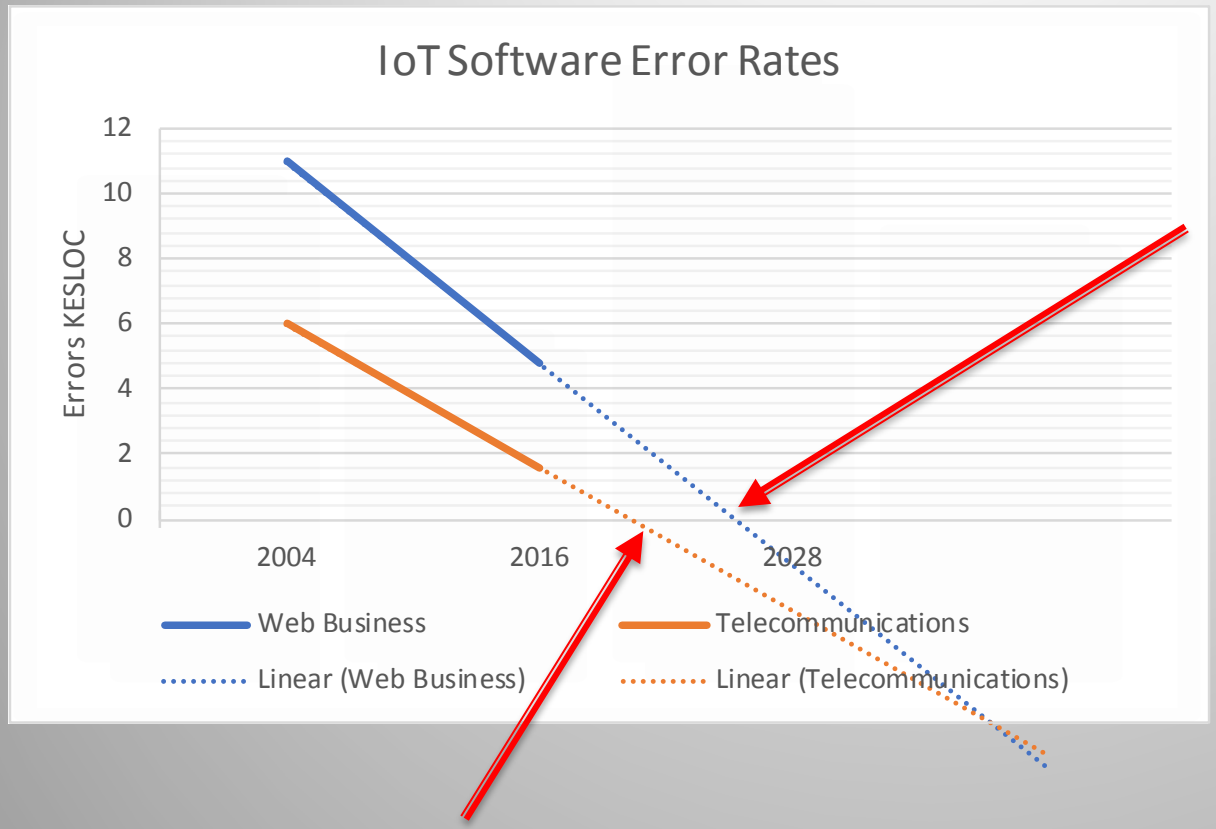
Year	2006 to 2008	2008 to 2010	2010 to 2012	2012 to 2014	2014 to 2016
Defects/KESLOC	7.0	6.4	5.8	5.3	4.8

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

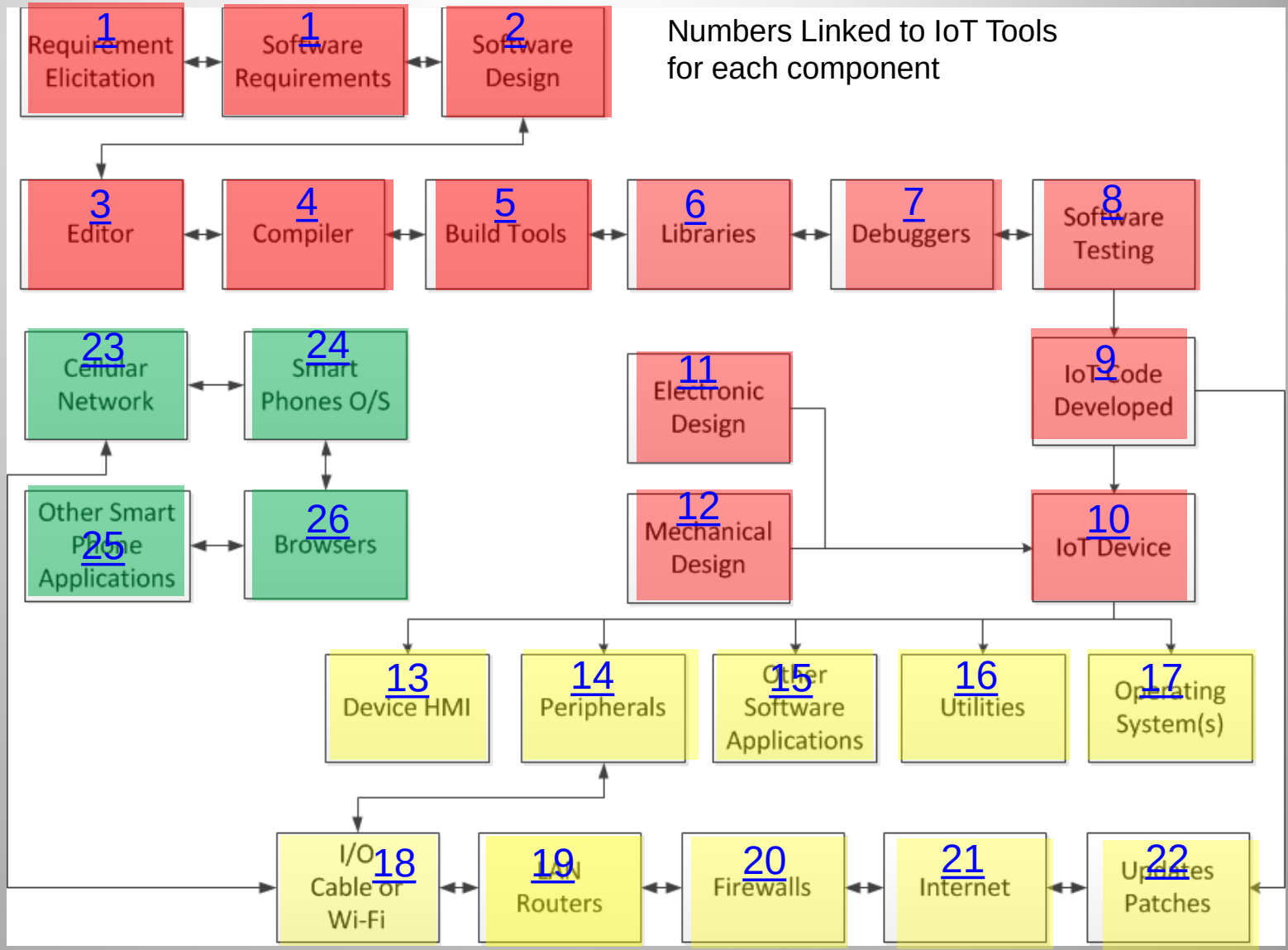


Web Business 2026

Defect Rates will approach but never reach zero.

Telecommunications 2021

Over 175 Tools to Support IoT



IoT and Mobile Mitigations

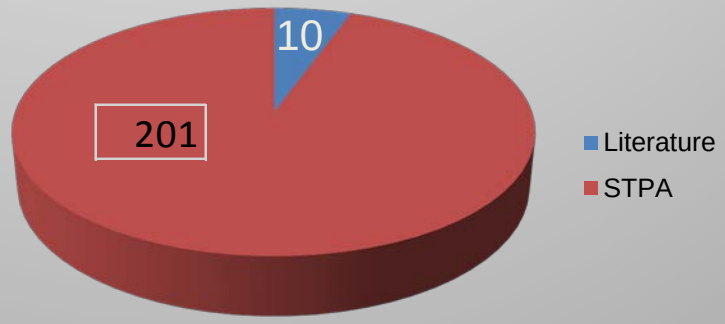
1. Do not use inexpensive household routers for IoT applications as the software is buggy.
2. Use strong (AES or better) encryption everywhere
3. Replace default factory user names and passwords with strong passwords, change periodically http://www.howtogeek.com/195430/how-to-create-a-strong-password-and-remember-it/
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 201 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

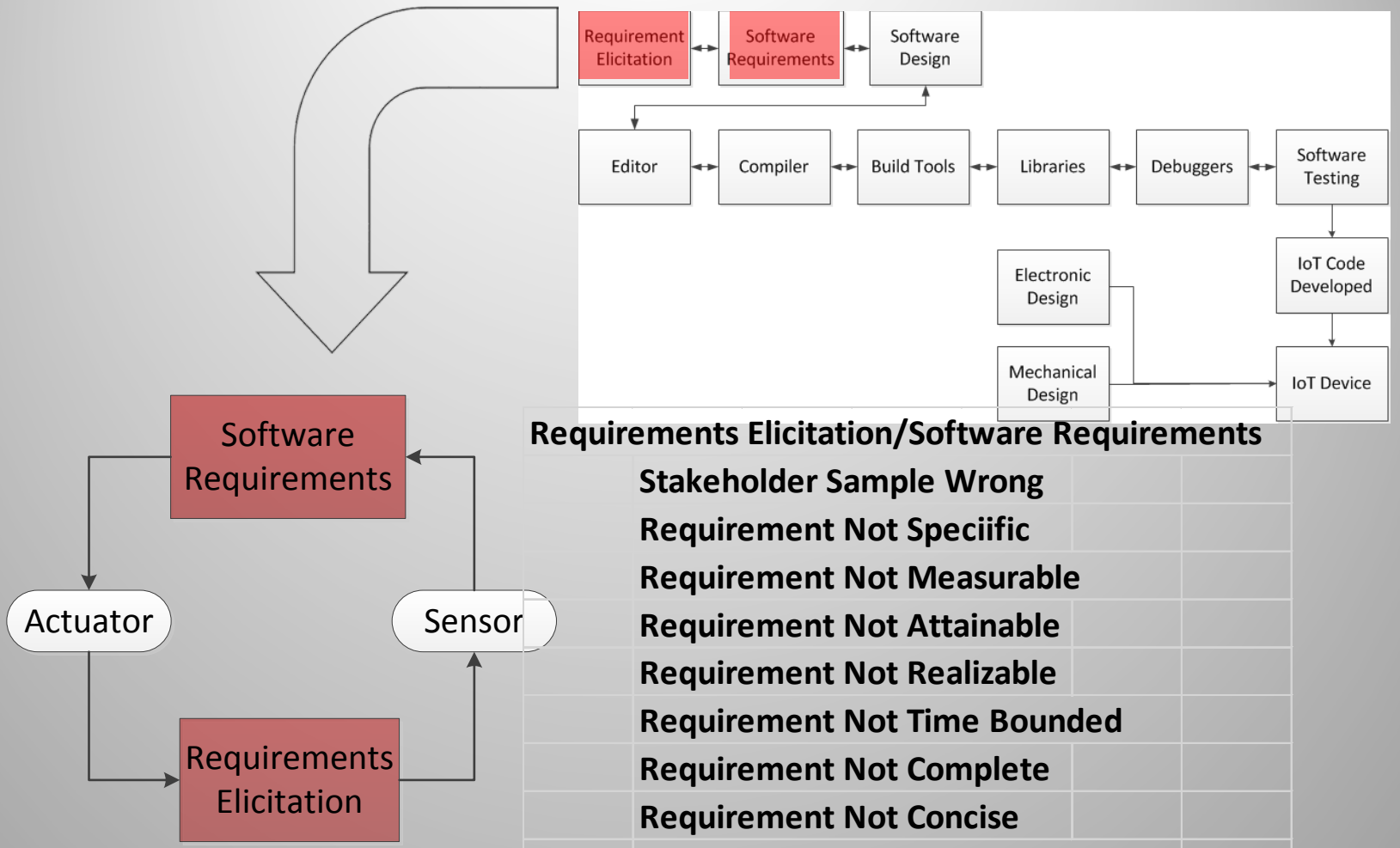
Smart Phone Aps and Browser



- Smart Phone Aps
  - McAfee
  - Norton
  - Trend
  - Panda
  - Webroot
  - iPhone N/A
- Browsers
  - Chrome
  - Firefox
  - Safari
  - Opera
  - Skyfire
  - UC Browser
  - BeFE

Backup Slides STPA Analysis

Development Sub-Subsystem Risks

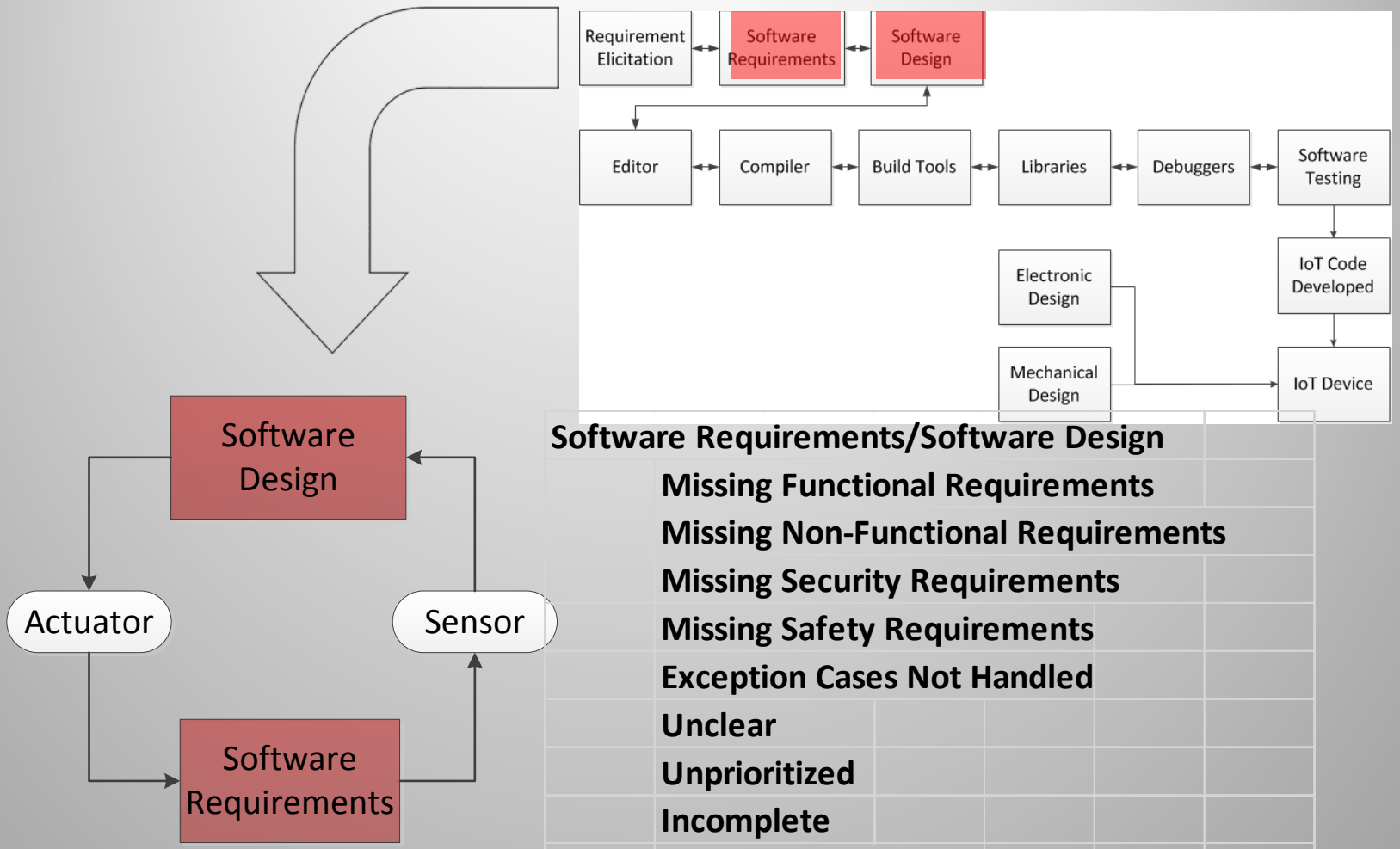


Requirements Elicitation/Software Requirements

- **Stakeholder Sample Wrong**
- **Requirement Not Speciific**
- **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

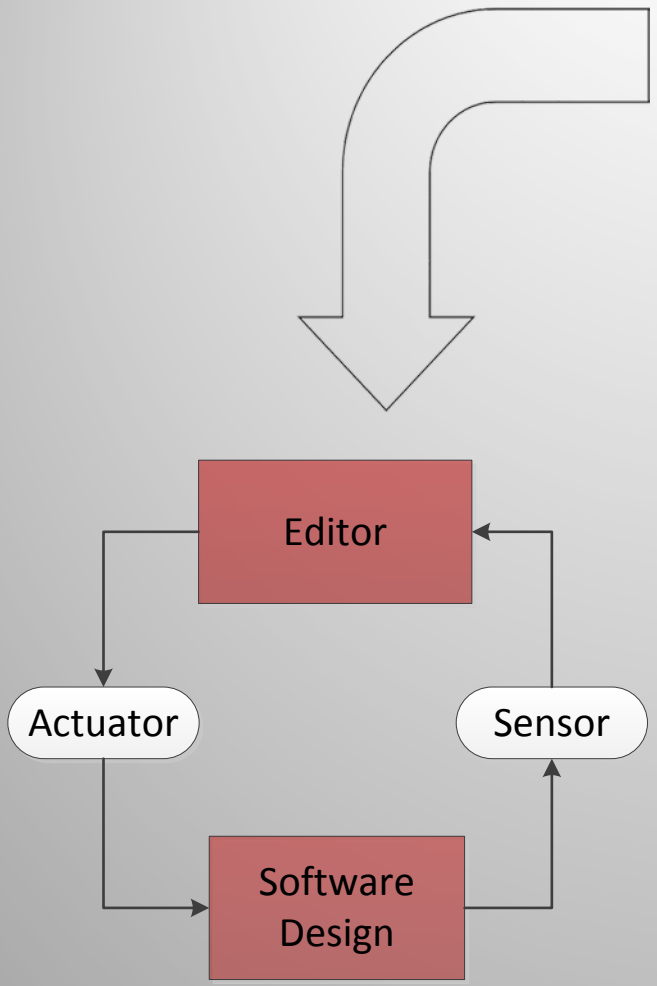


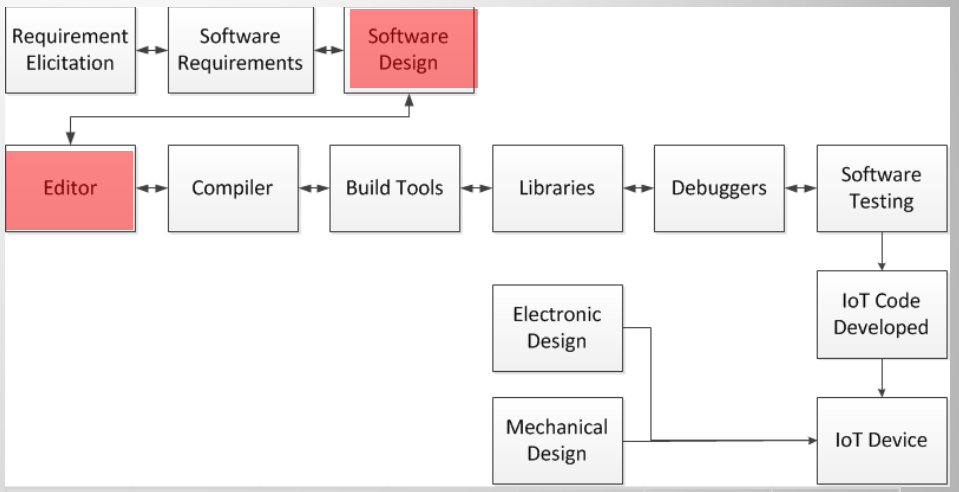
Software Requirements/Software Design

- **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



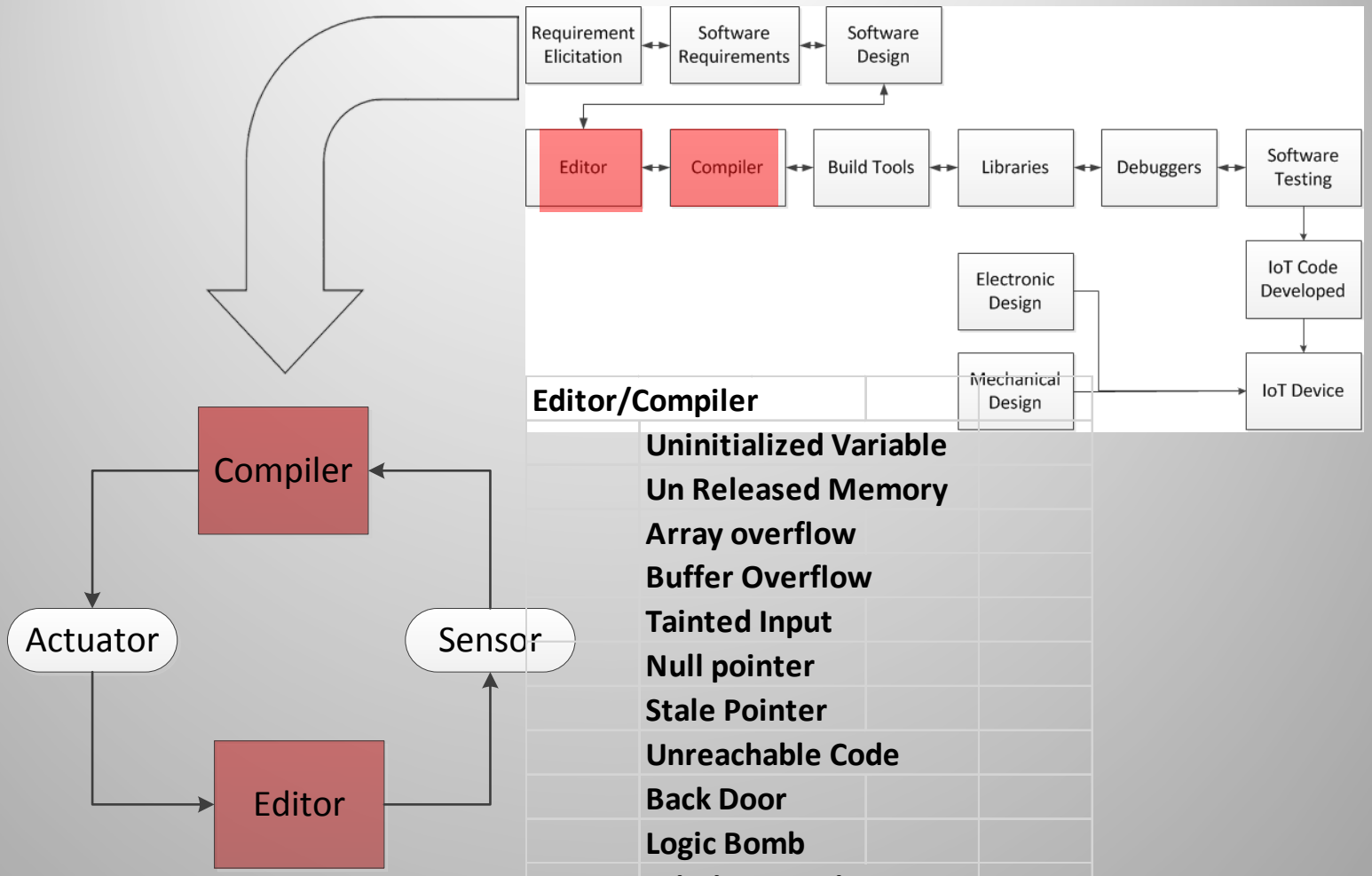


Software Design/Editor

- **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**

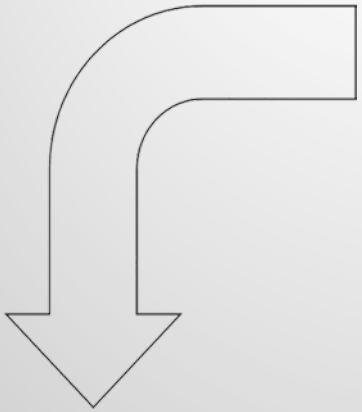
http://www.pcworld.com/article/146282/article.html

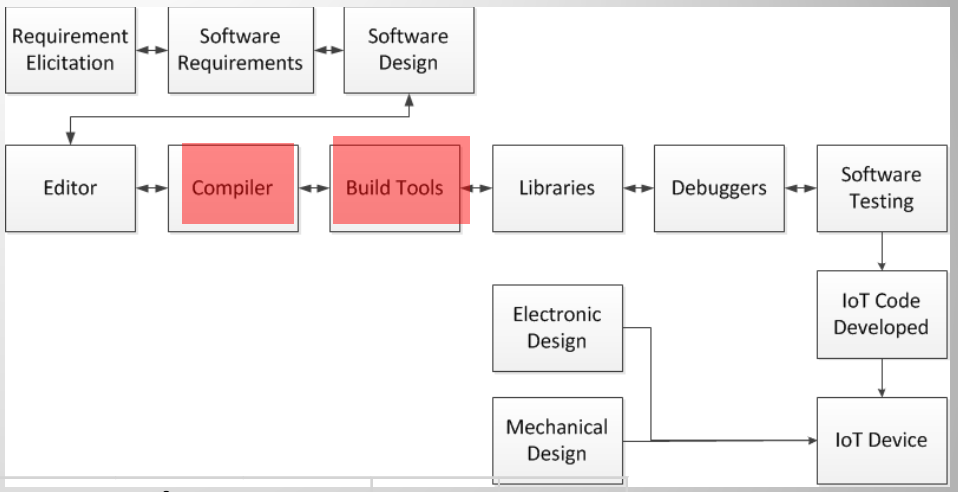
Development Sub-Subsystem Risks

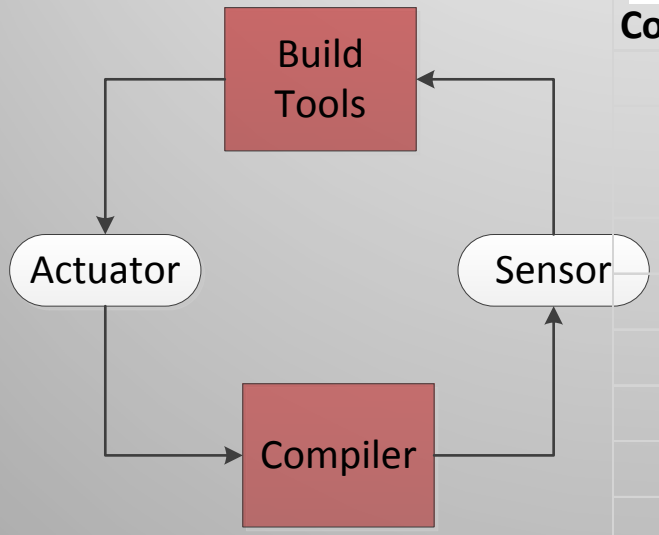


Editor/Compiler
Uninitialized Variable
Un Released Memory
Array overflow
Buffer Overflow
Tainted Input
Null pointer
Stale Pointer
Unreachable Code
Back Door
Logic Bomb
Missing Requirements
Misunderstood Requirements
Syntax Error

Development Sub-Subsystem Risks



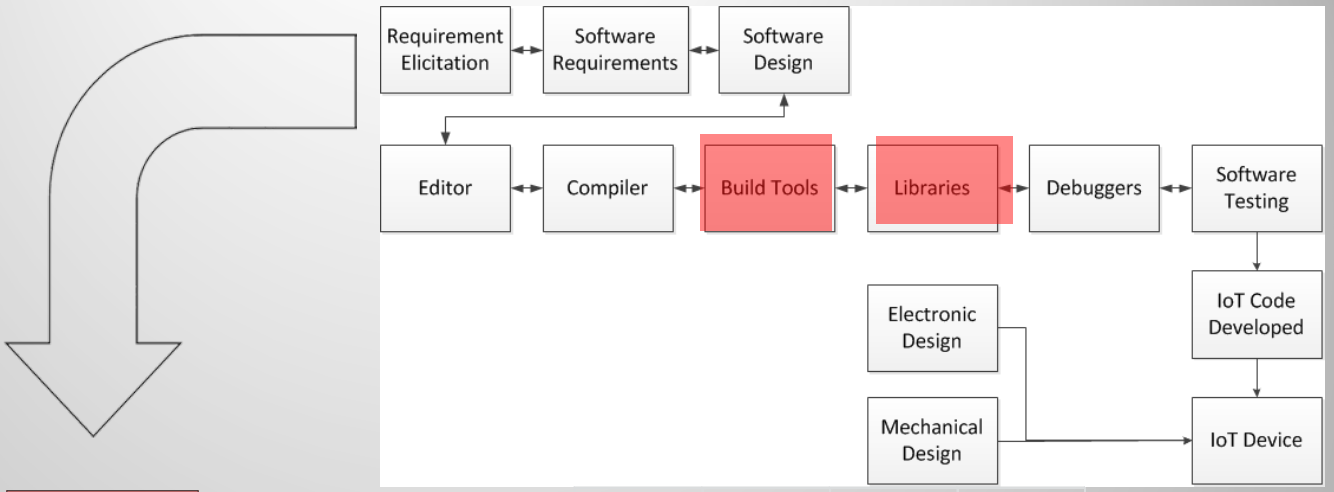


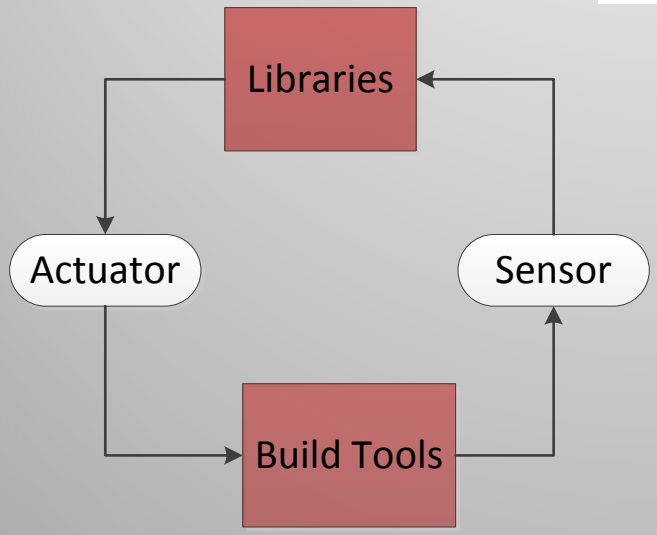


Compiler/Build Tools

- **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



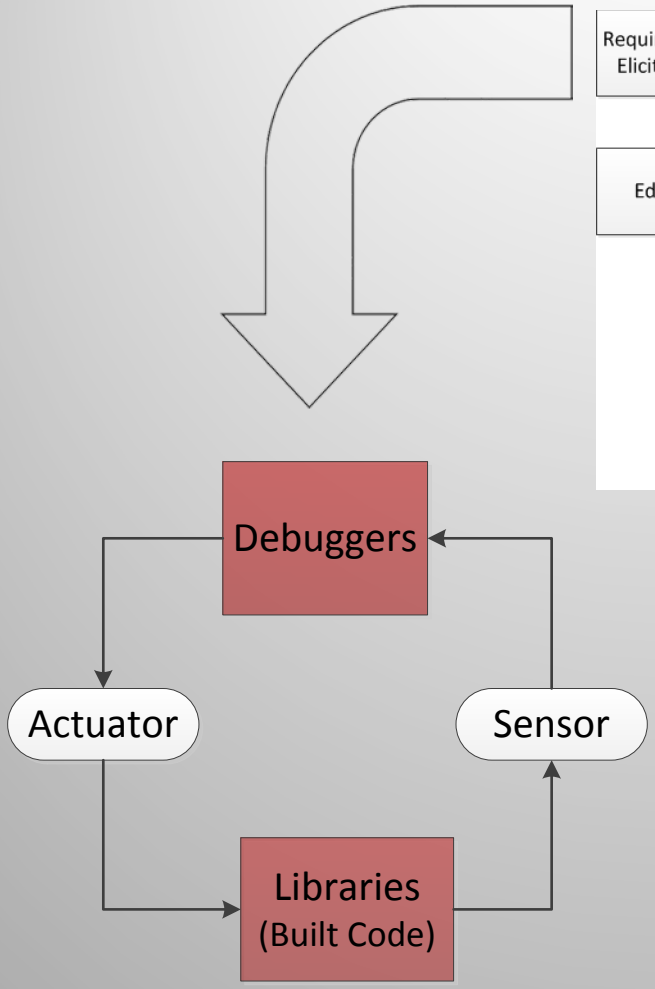


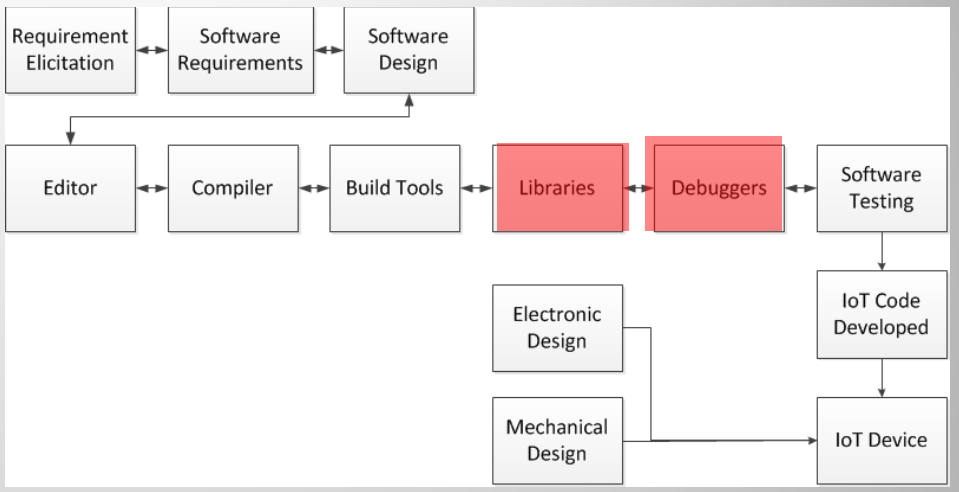
Build Tools/Libraries

- **Wrong Library Version**
- **Misnamed Library**
- **Library Vulnerability**
- **Library Not Updated**
- **Library Back Door**
- **Untrusted Supply Chain**
- **Library Not Updated**

https://msdn.microsoft.com/en-us/library/8x5x43k7.aspx

Development Sub-Subsystem Risks

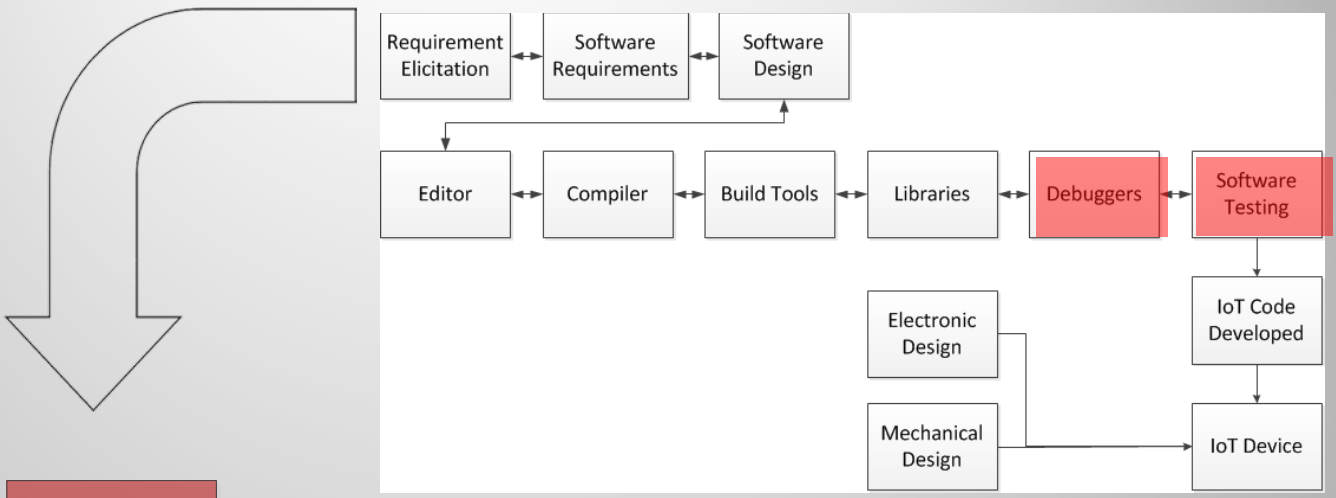


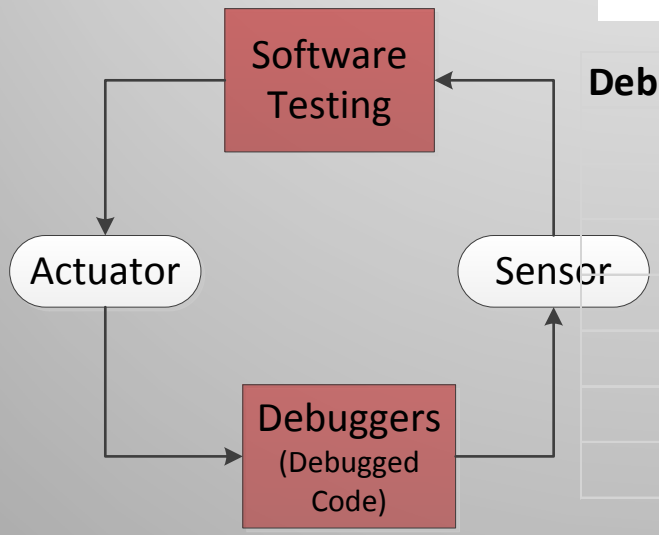


Libraries/Debuggers

- **Heisenberg Effect**
- **Diagnostics Residual**
- **Intermittent Problem**
- **Residual Debug Code**
- **Unrealistic Simulators**

Development Sub-Subsystem Risks

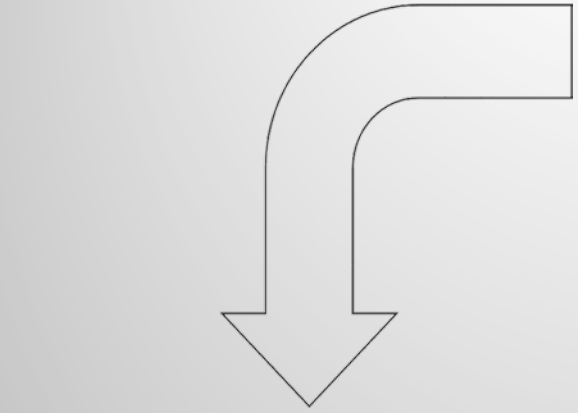


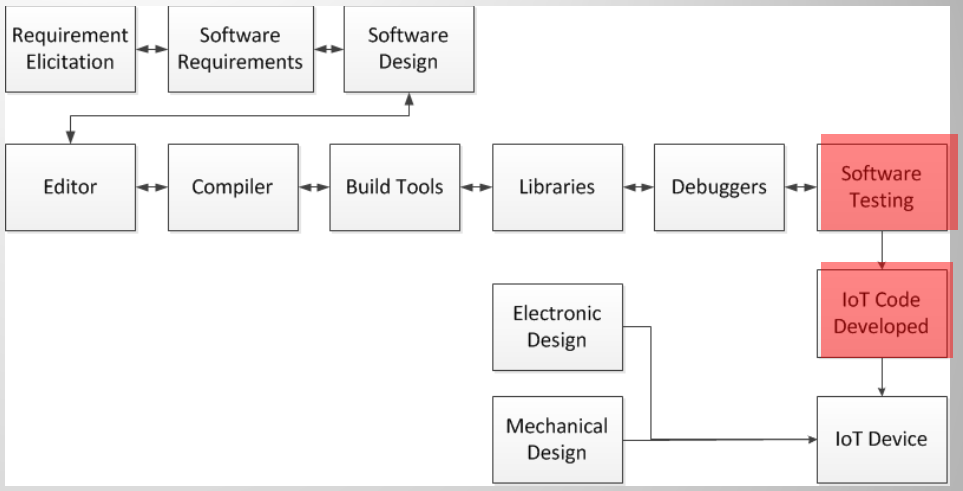


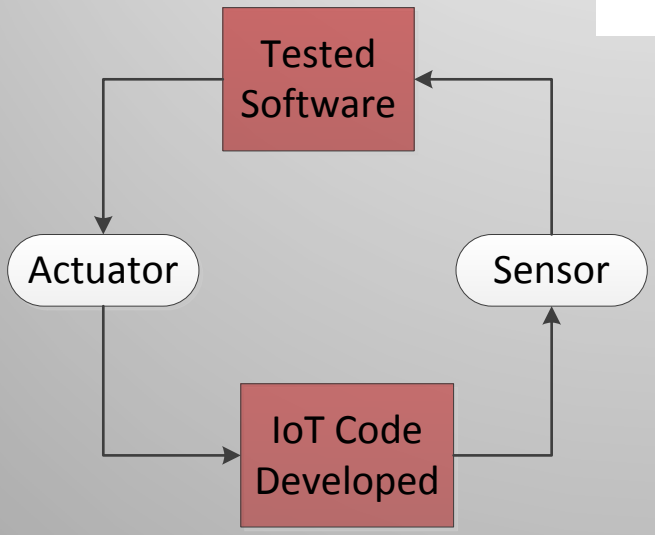
Debuggers/Software Testing

- **Low Coverage**
- **No/Few Security Tests**
- **Rushed Testing**
- **No/Few Requirements Traceability**
- **Redundant Testing**
- **No/Few Performance Tests**
- **Weak Platfoirm Testing**

Development Sub-Subsystem Risks



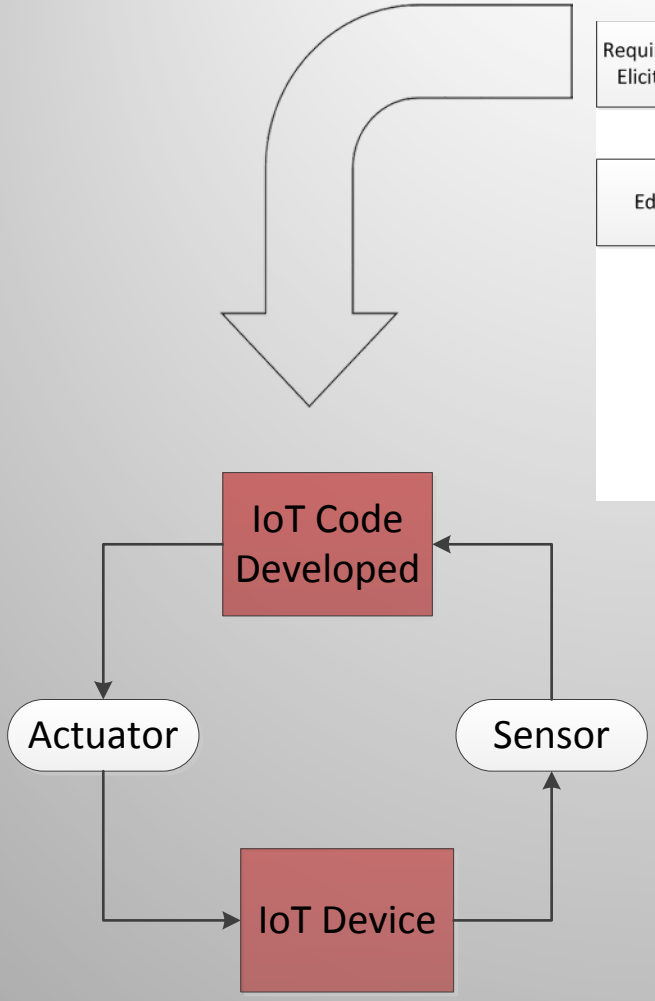


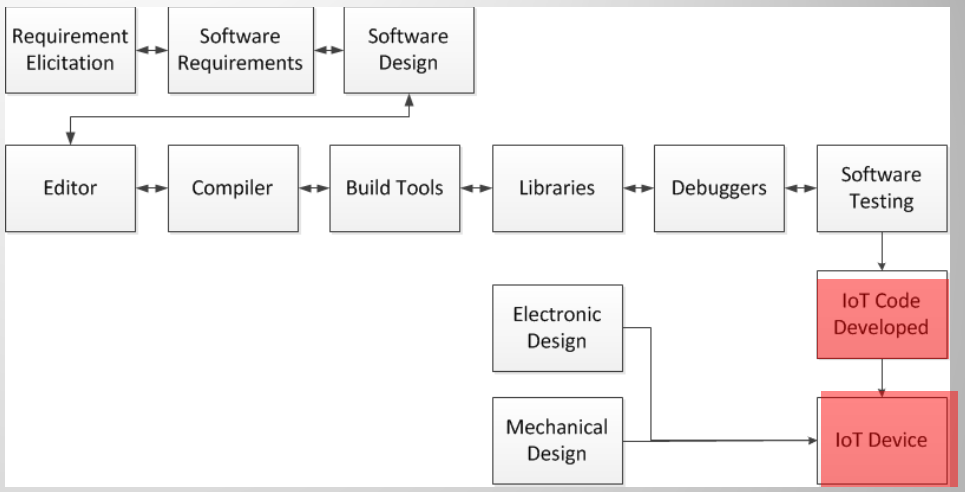


Software Testing/IoT Code Developed

- **Residual Bugs**
- **Slow Performance**
- **Race Condition**
- **Weak Error Recovery**
- **Weak On Line Help**
- **Weak Documentation**

Development Sub-Subsystem Risks

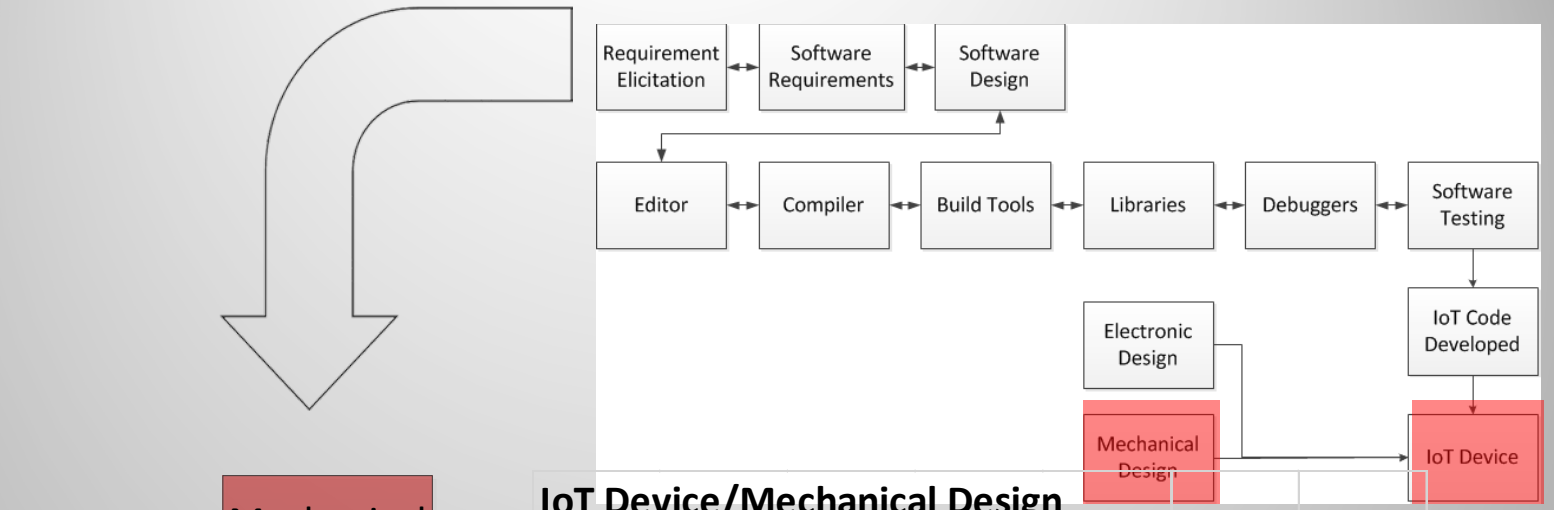


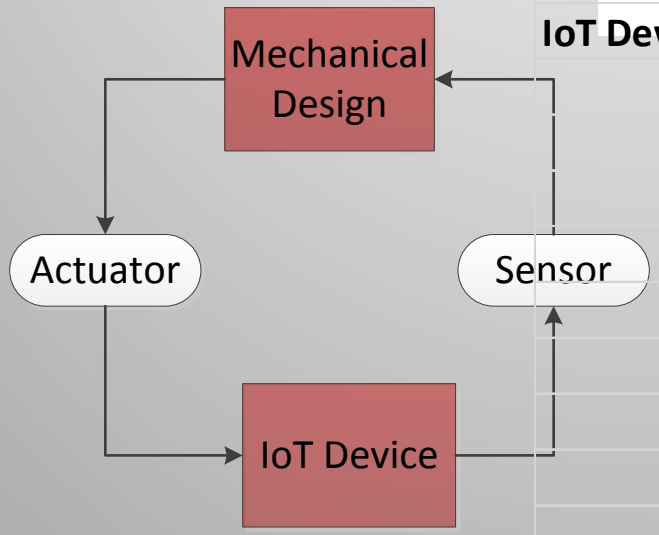


IoT Code Developed/IoT Device

- **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

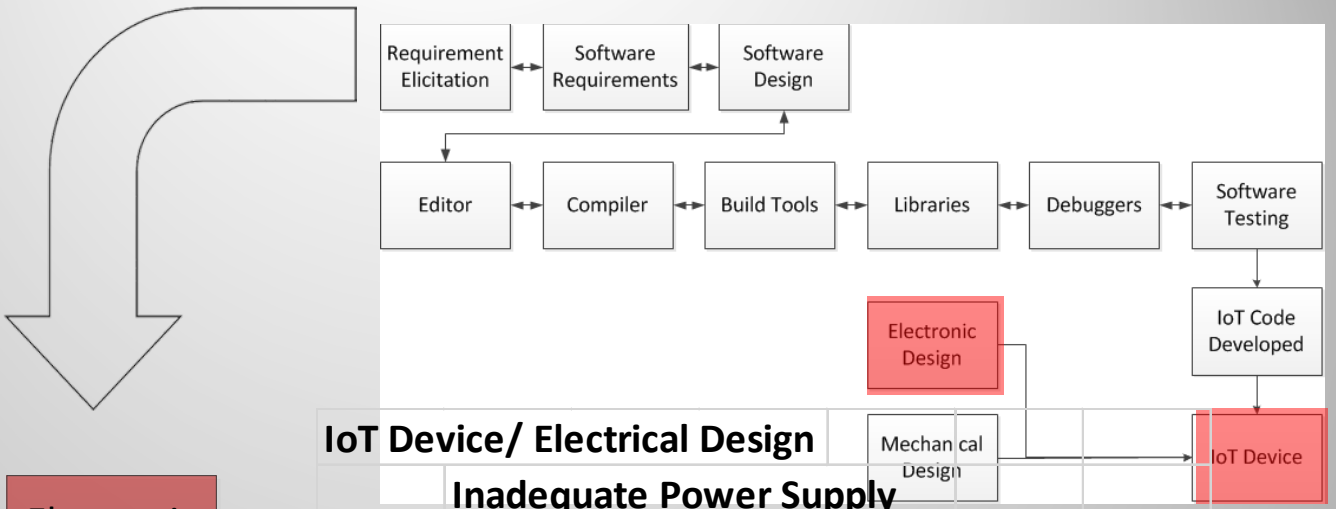


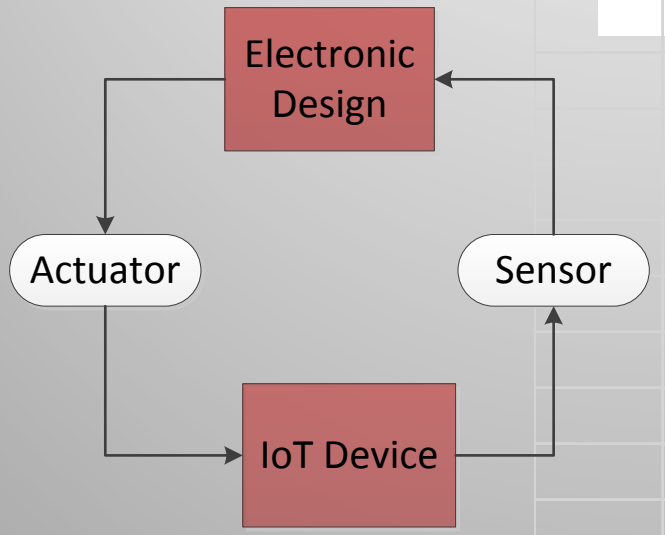


IoT Device/Mechanical Design

- **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**

Development Sub-Subsystem Risks

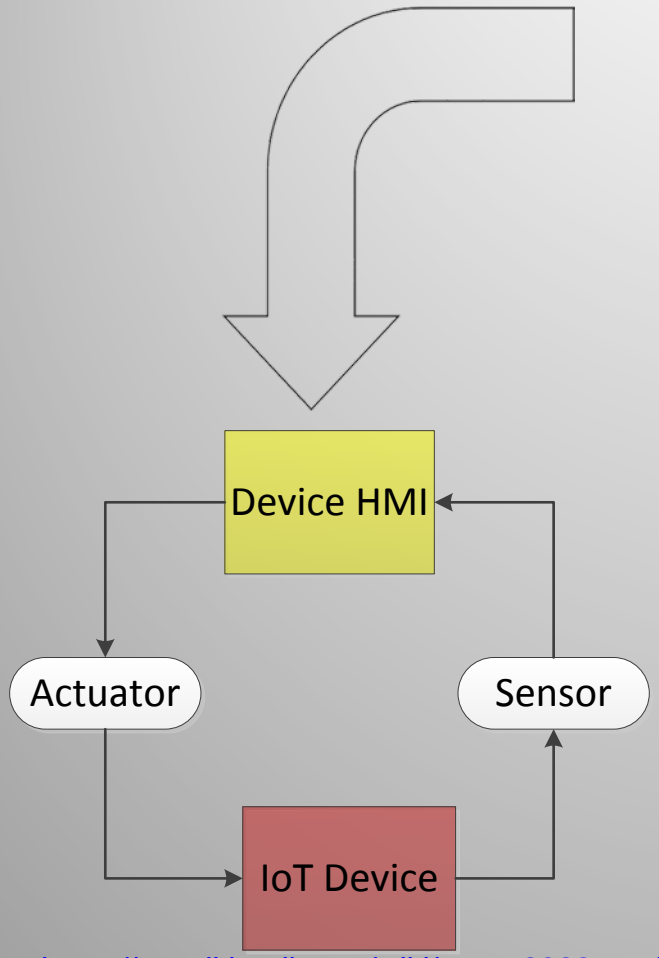


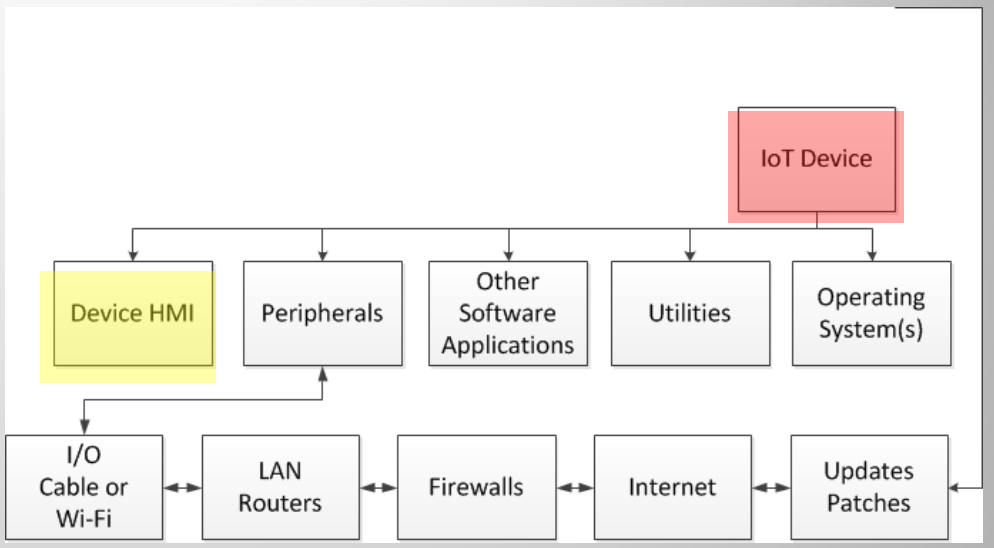


IoT Device/ Electrical Design

- **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



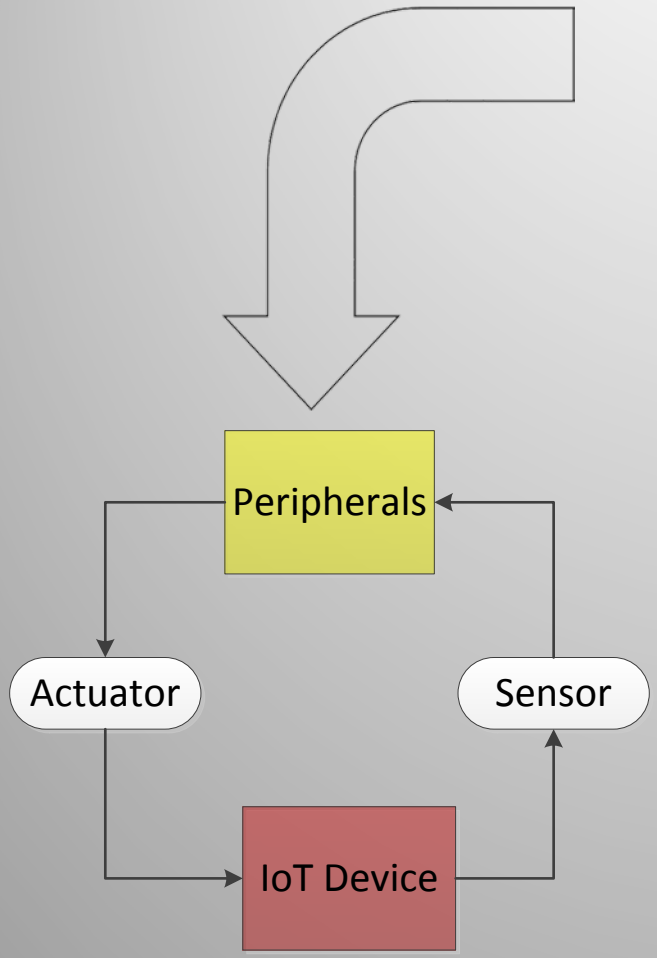


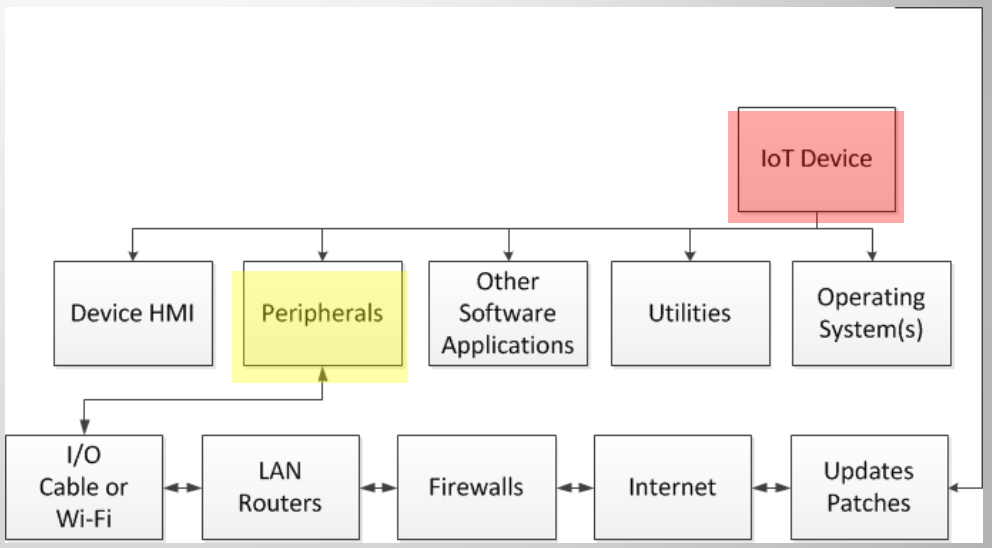
IoT/Device HMI

- **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

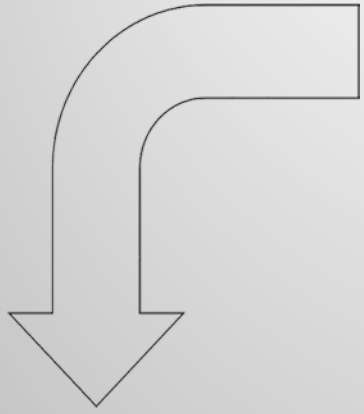


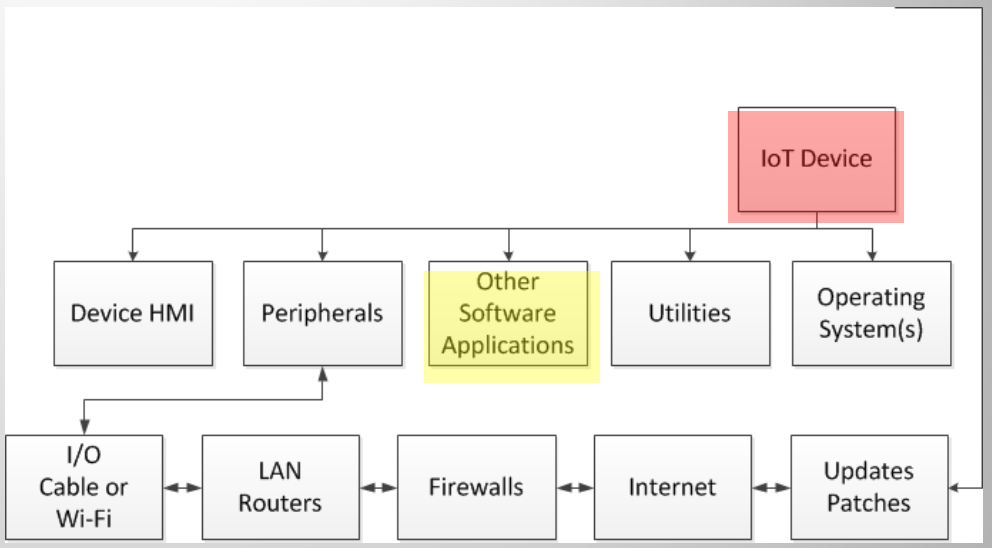


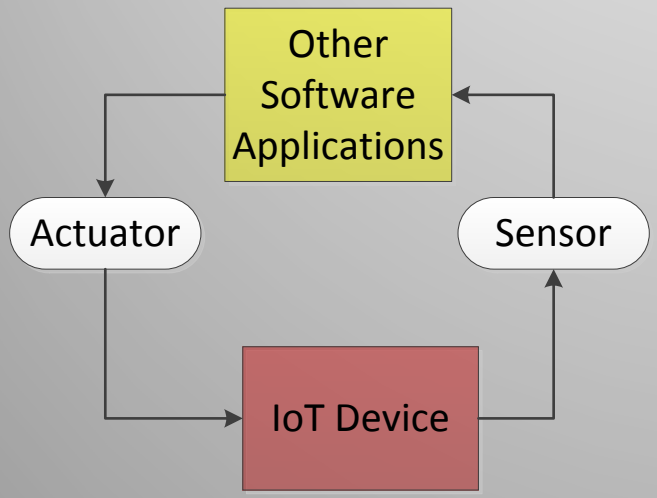
IoT/Peripherals

- **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

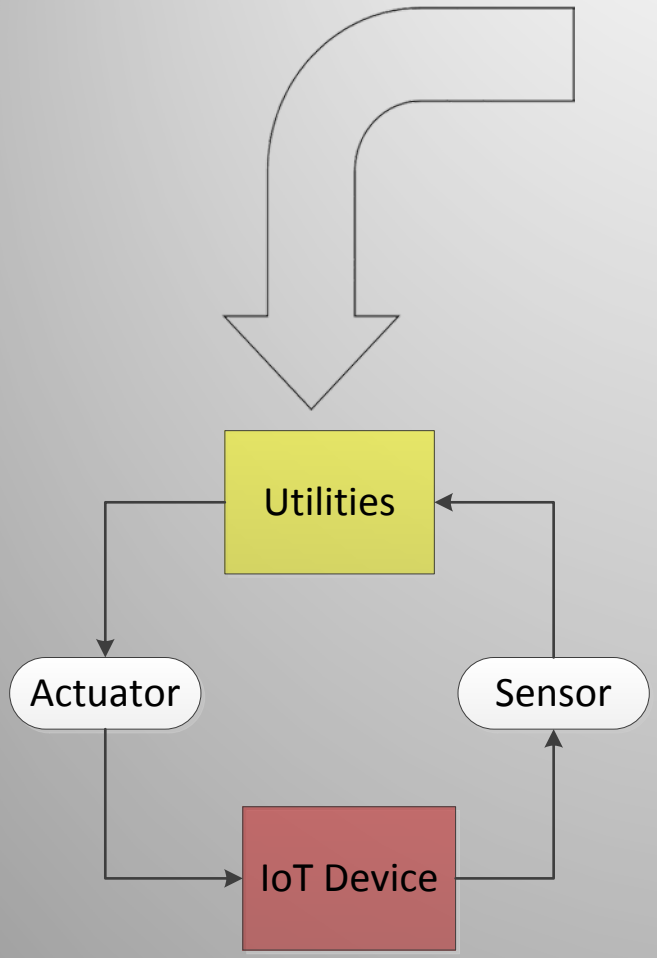


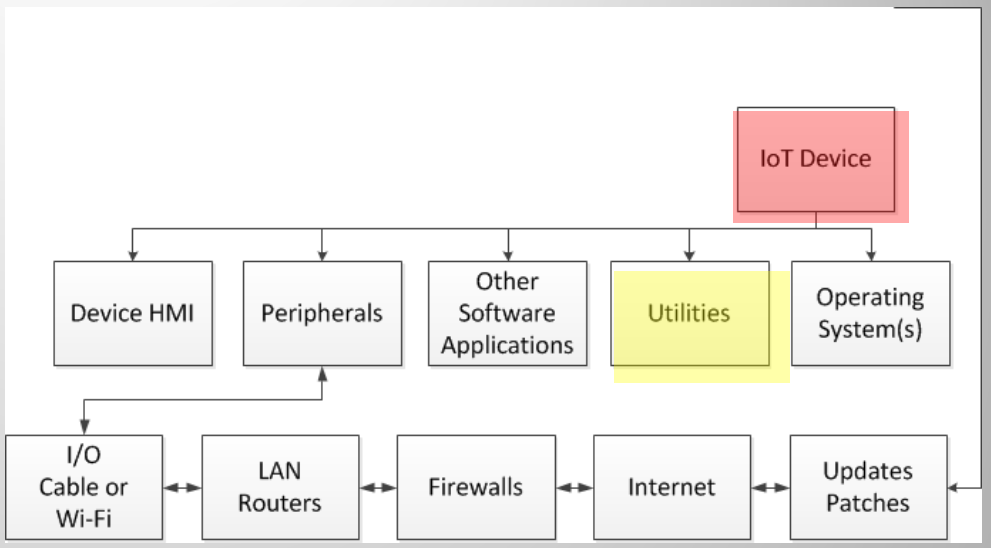




IoT/Other SW Apps
File Names Not Unique
Versions Not Compatible
Supply Chain Not Secure
Trojans Present
Back Door Present
Not Enough Memory
Rogue Applications

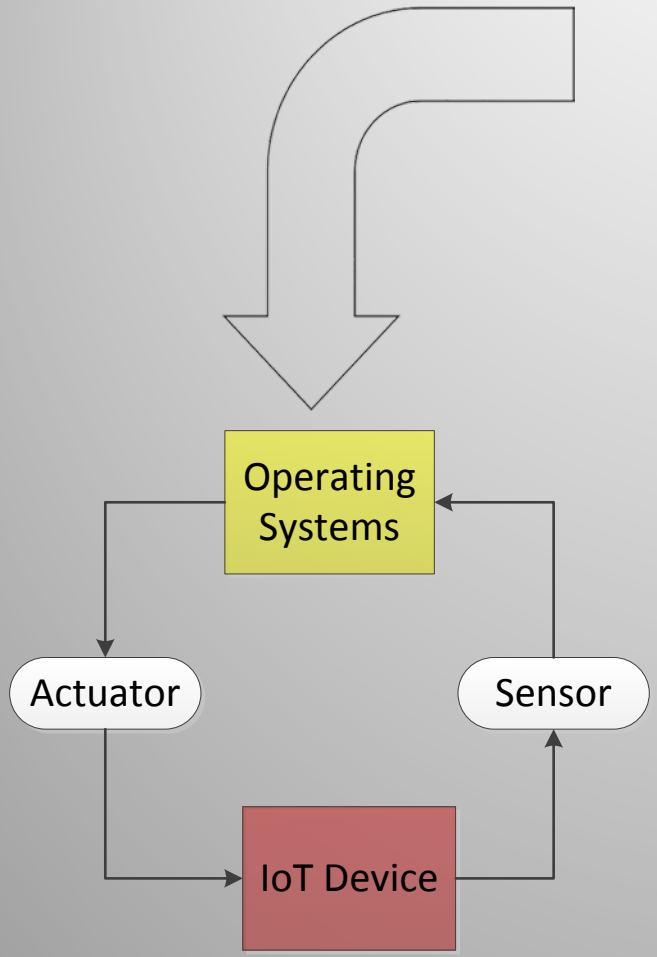
External Communications Sub-Subsystem Risks

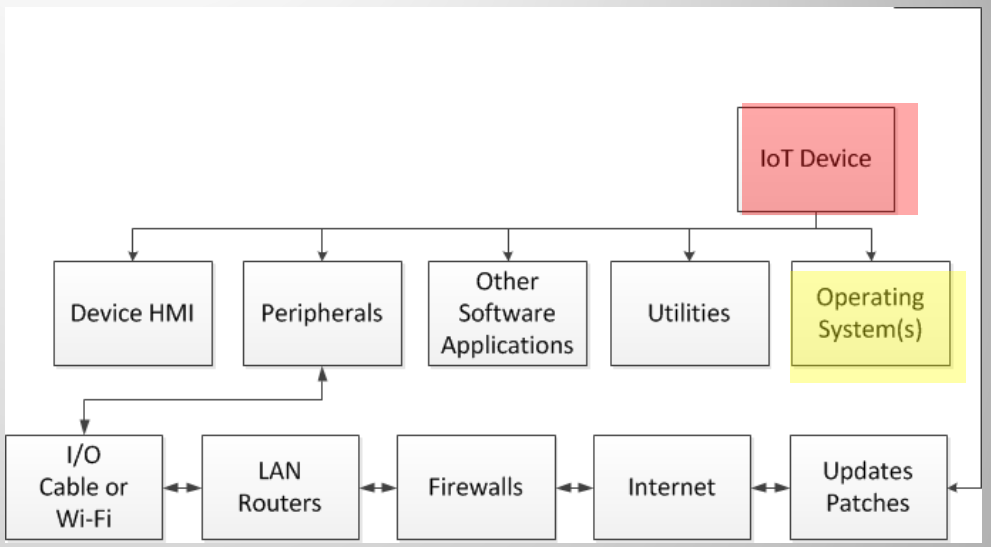




IoT/Utilities
Wrong Version
Known Vulnerabilities in Version
Version Not Updated
Wrong Numerical Precision
Wrong Data Format
Counterfeit Item
No Upgrade Path
Browser Vulnerabilities

External Communications Sub-Subsystem Risks

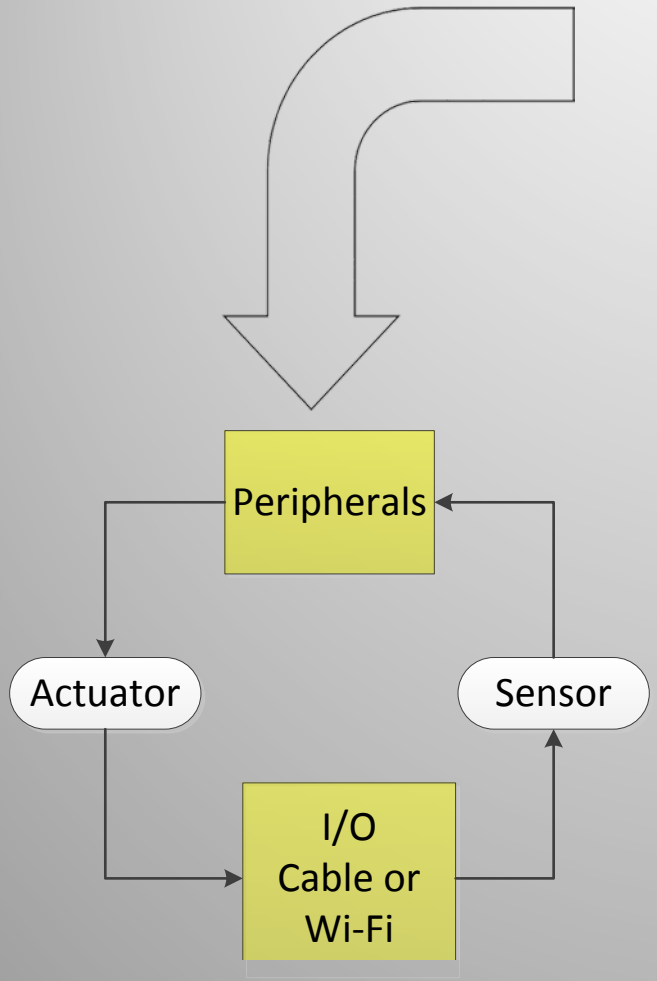


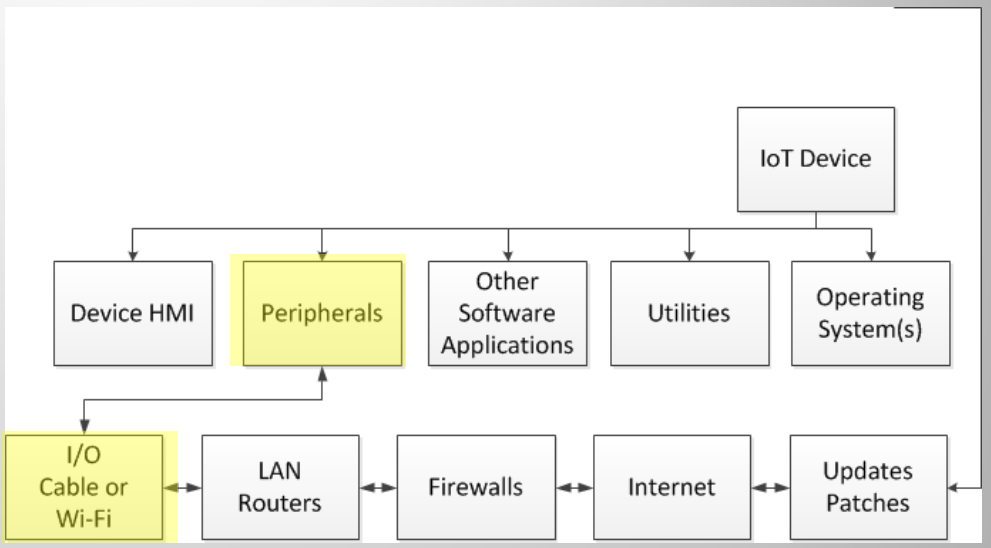


IoT/Utilities

- **Wrong Version**
- **Known Vulnerabilities in Version**
- **Version Not Updated**
- **Wrong Numerical Precision**
- **Wrong Data Format**
- **Counterfeit Item**
- **No Upgrade Path**
- **Browser Vulnerabilities**

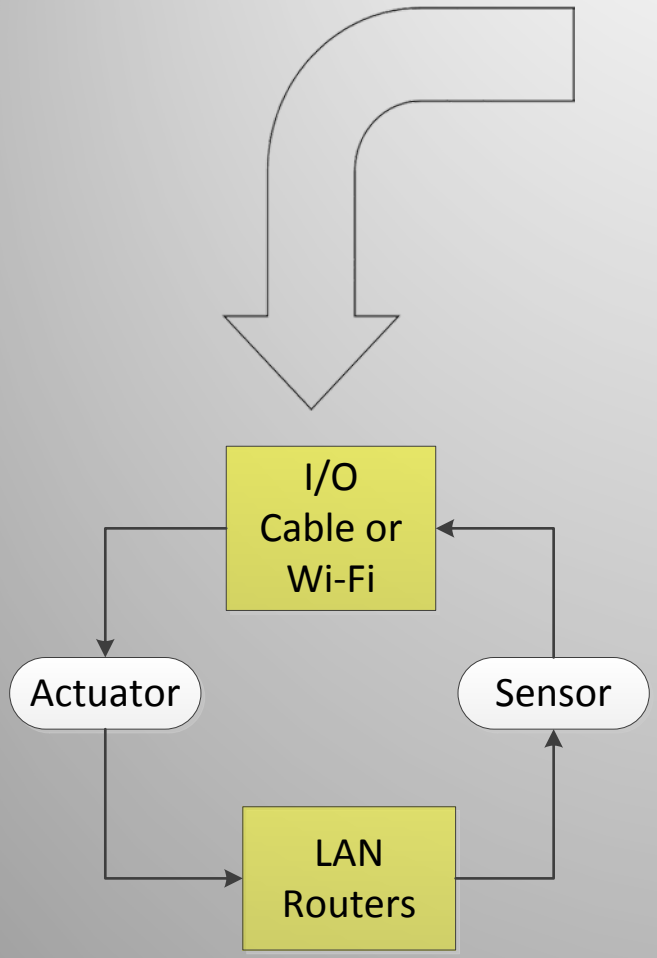
External Communications Sub-Subsystem Risks

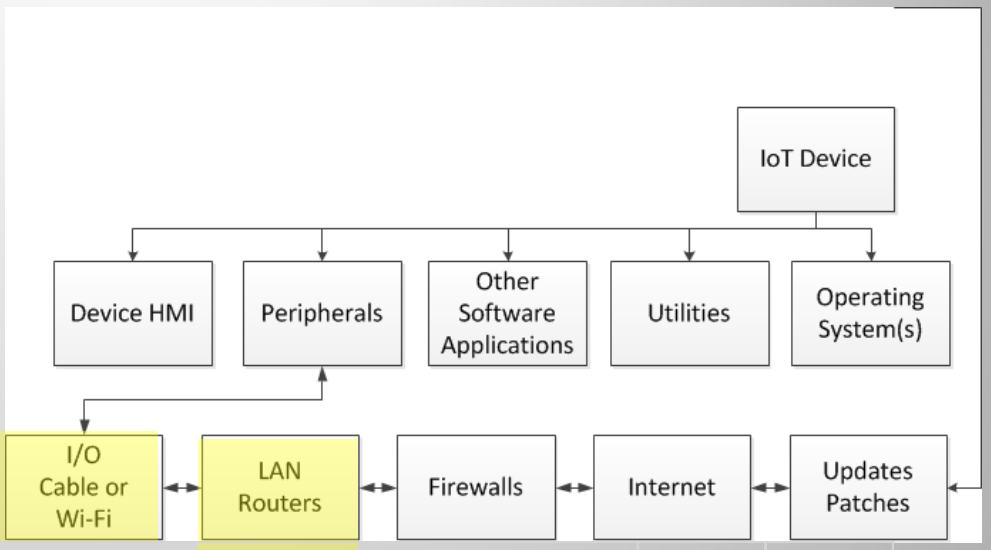




Peripheral/ IO Cable or Wi-Fi
Not Encrypted
Weak Encryption
Network Not Password Protected
Open I/O Ports
Driver Not Updated
Trap Door in Driver

External Communications Sub-Subsystem Risks

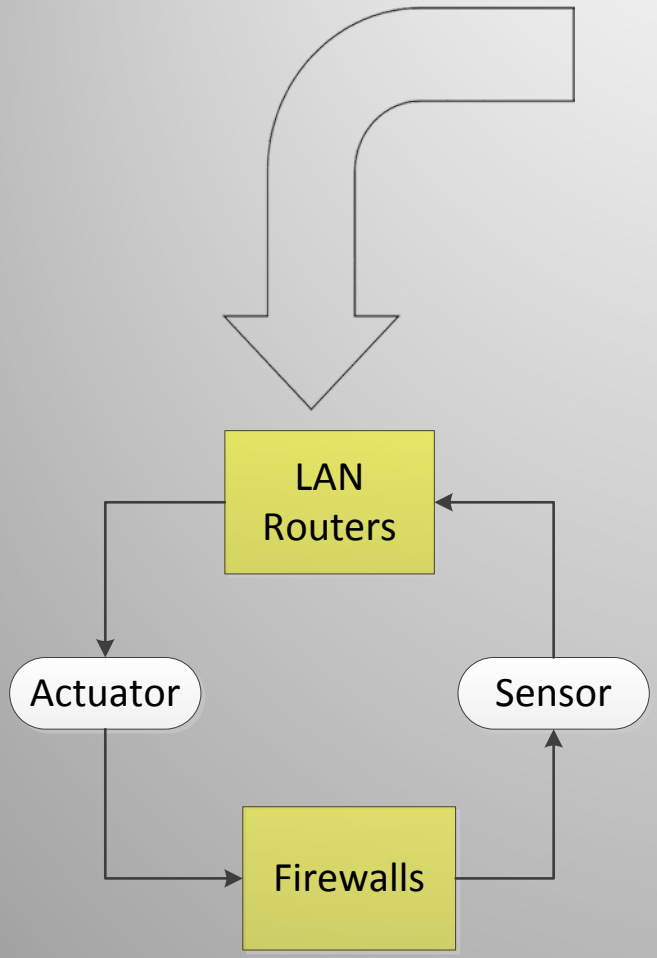


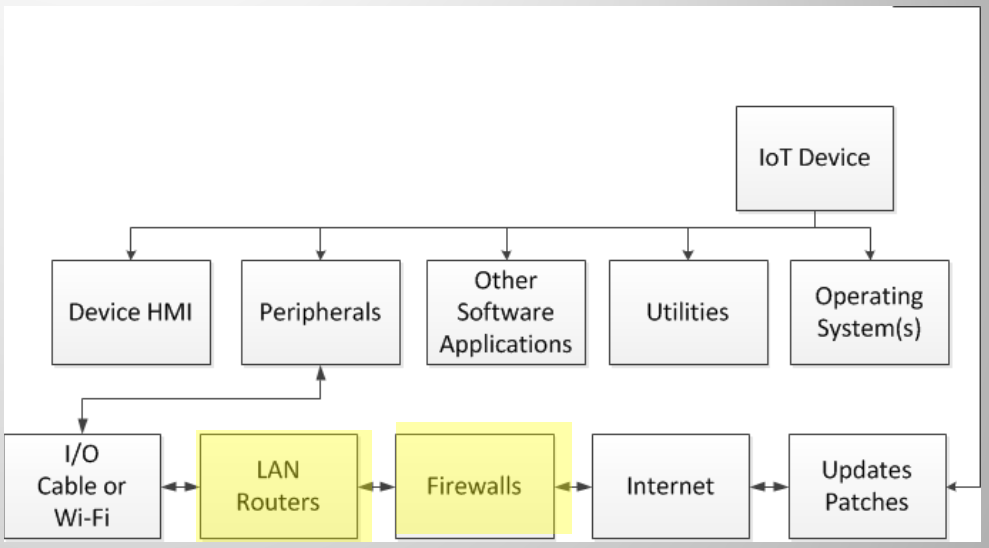


I/O Cable or Wi-Fi / LAN Routers

- **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**

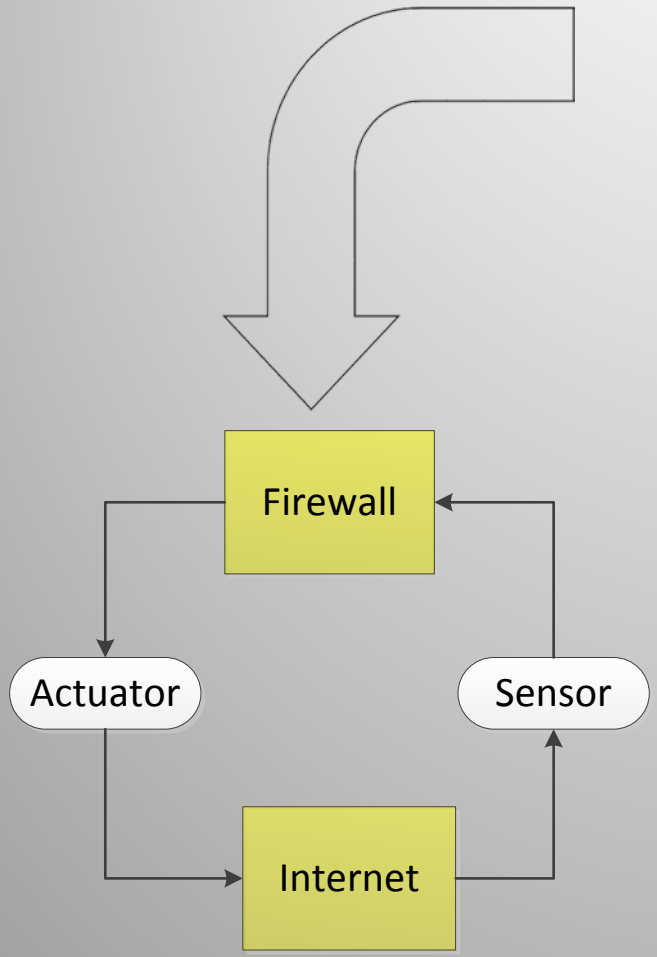
External Communications Sub-Subsystem Risks

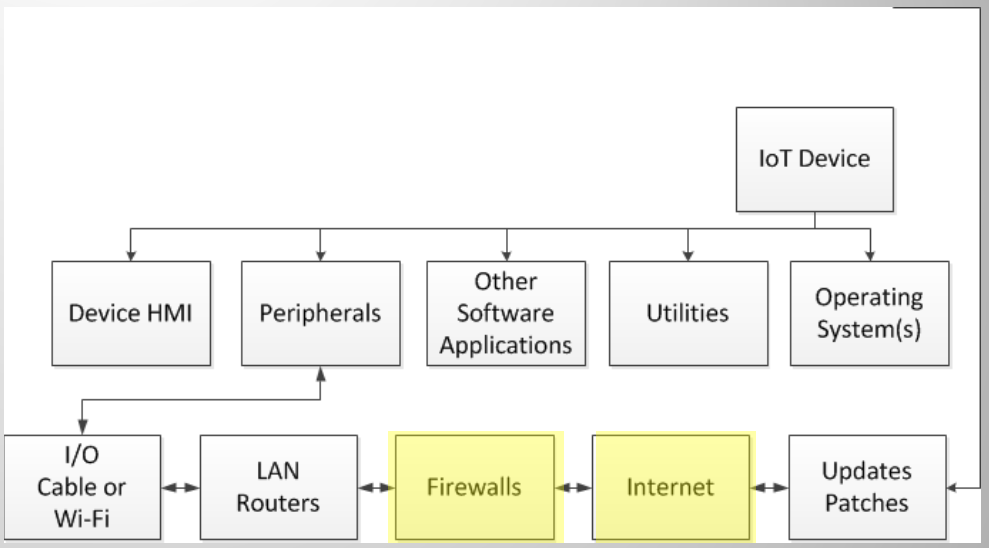




LAN Routers/Firewall
Ports Left Open
Wrong Security Policy
Firewall No Longer Supported
Firewall Contains Back Door
Capacity Insufficient
VPN Not Available
Not Updated

External Communications Sub-Subsystem Risks

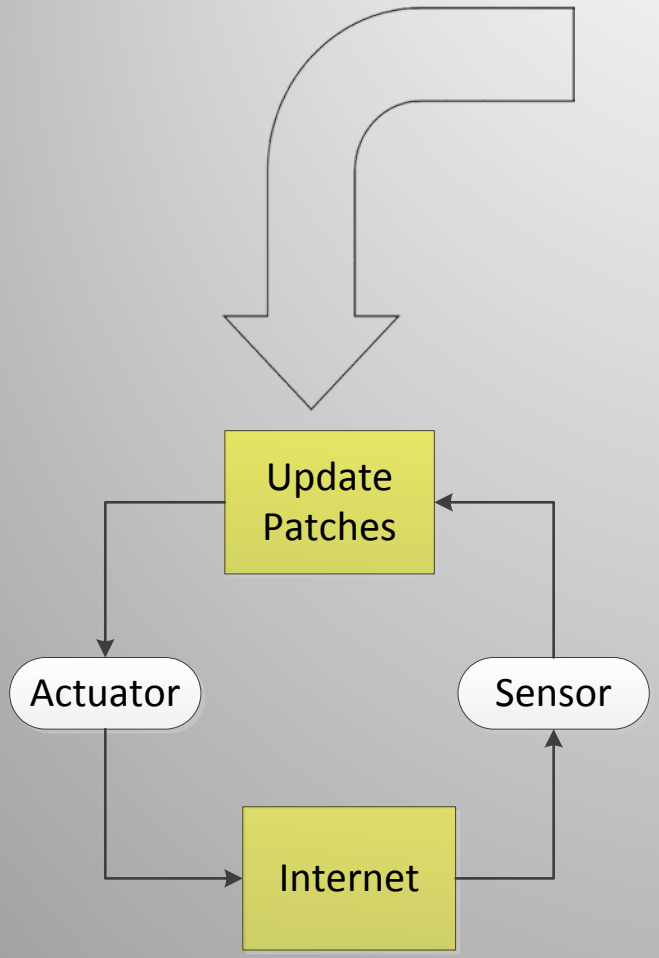


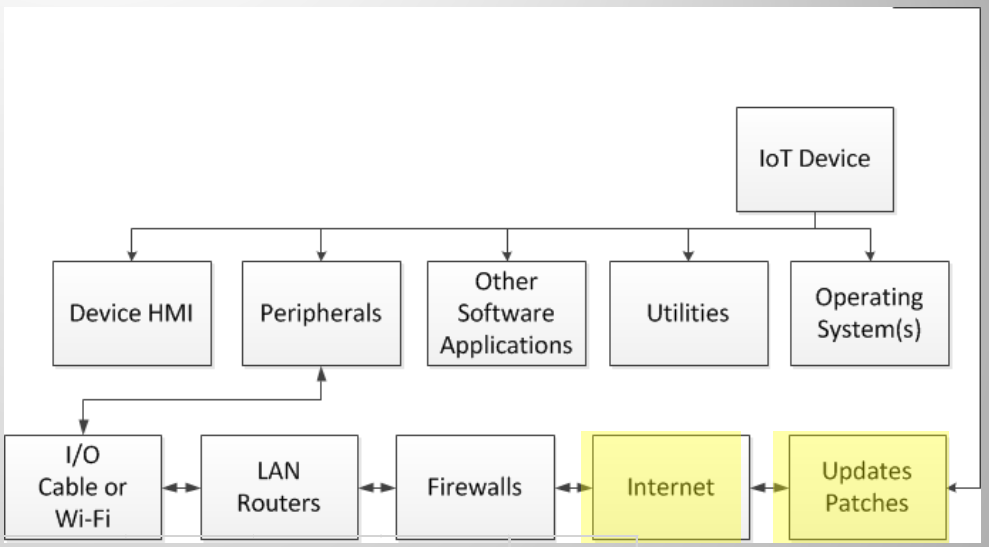


Firewall/Internet

- **Capacity Insufficient**
- **VPN Not Available**
- **No Port Scanning Detectors**
- **Required Port Blocked**

External Communications Sub-Subsystem Risks

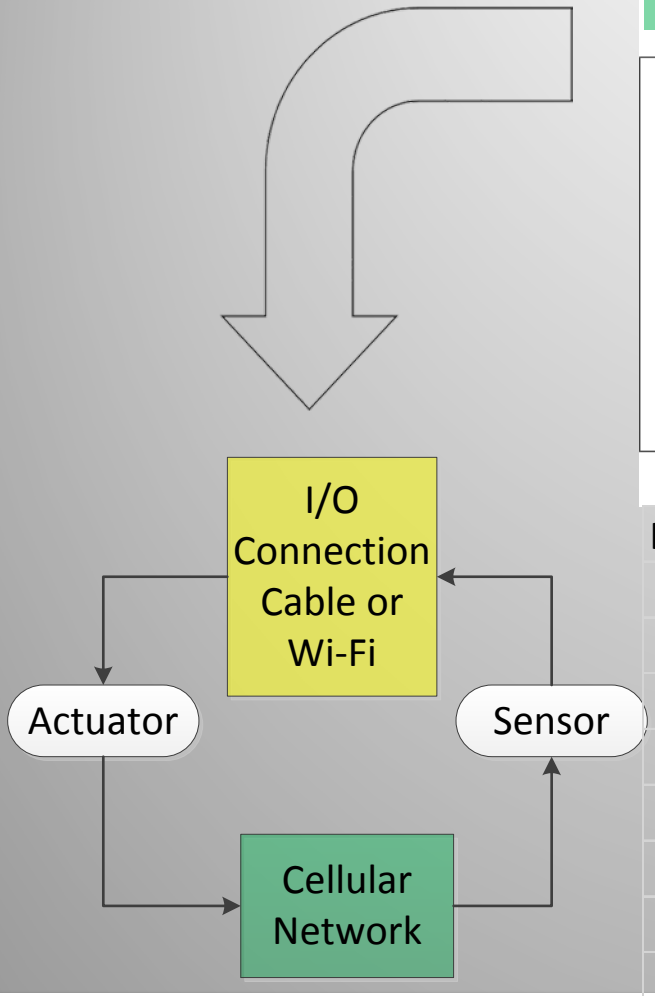


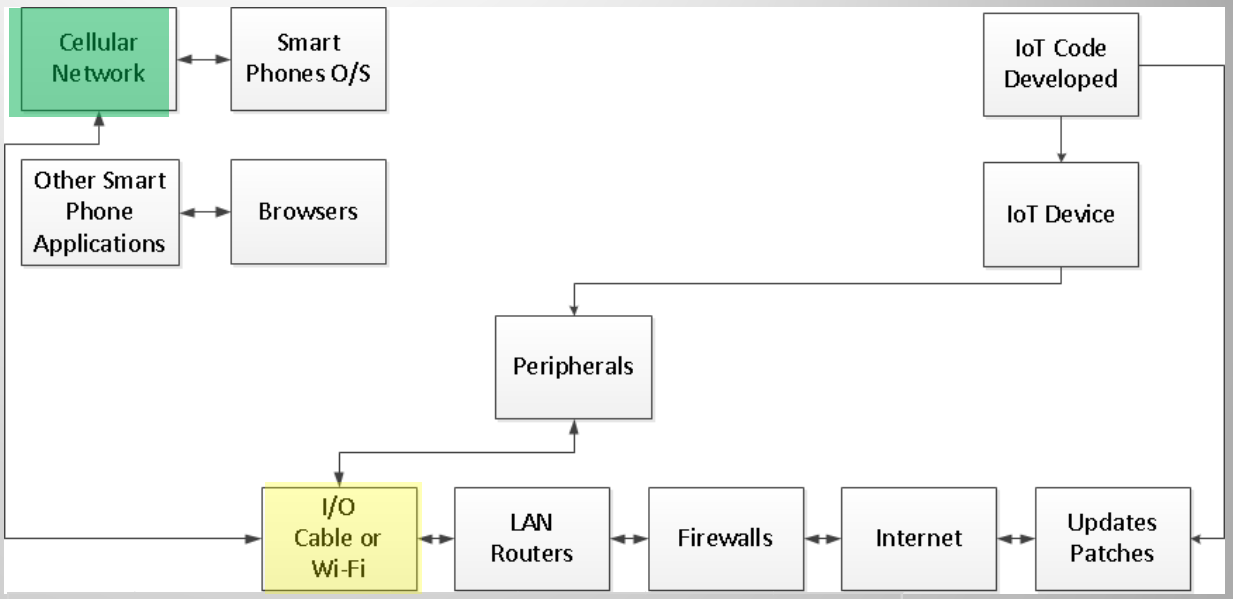


Internet/Update Patched

- **Patch Infected With Virus**
- **Patch Has Vulnerability**
- **Device No Longer Supported**
- **Updates Not Done**

Mobile Phone and Update Sub-Subsystem Risks

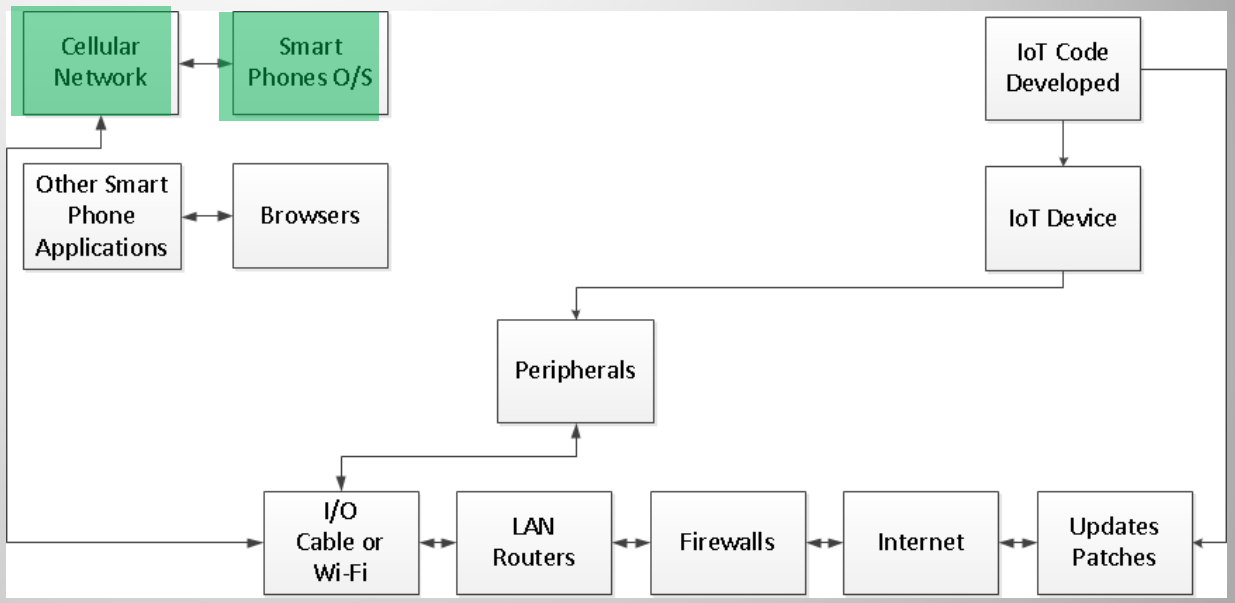


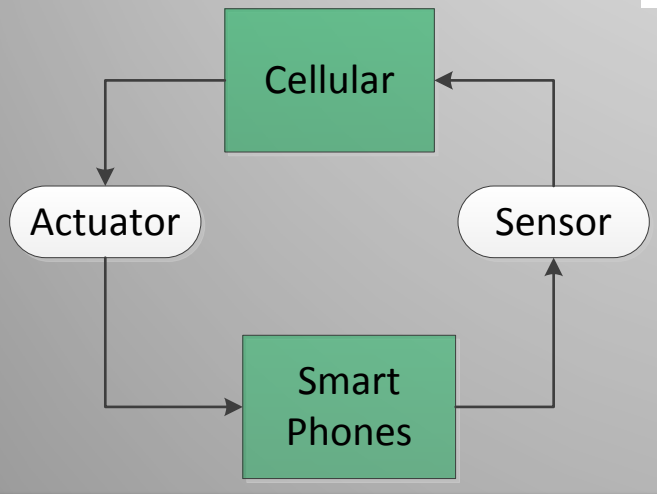


I/O Connection Cable or Wi-Fi/Cellular Network

- **Not Encrypted**
- **Inadequate Encryption A5/1, A5/2**
- **Backbone Vulnerabilities SS7**
- **Backdoors**
- **Public Unsecured Wi-Fi**
- **Operating System Vulnerabilities**
- **O/S Not Upgraded**

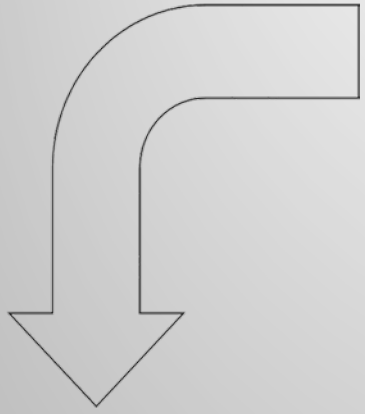
Mobile Phone and Update Sub-Subsystem Risks

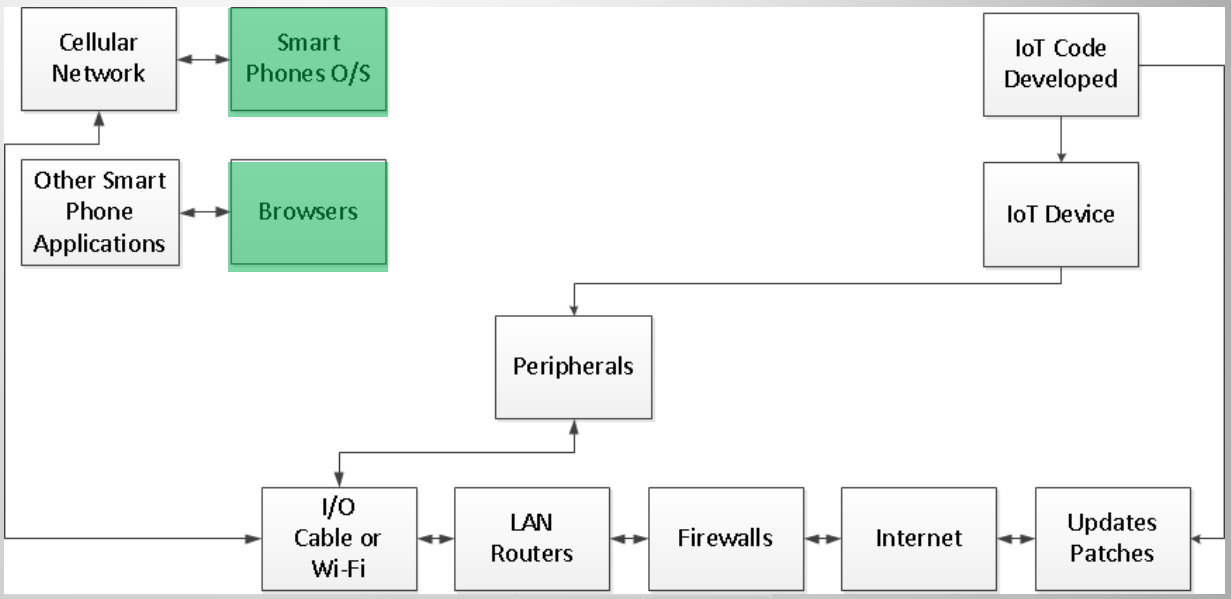


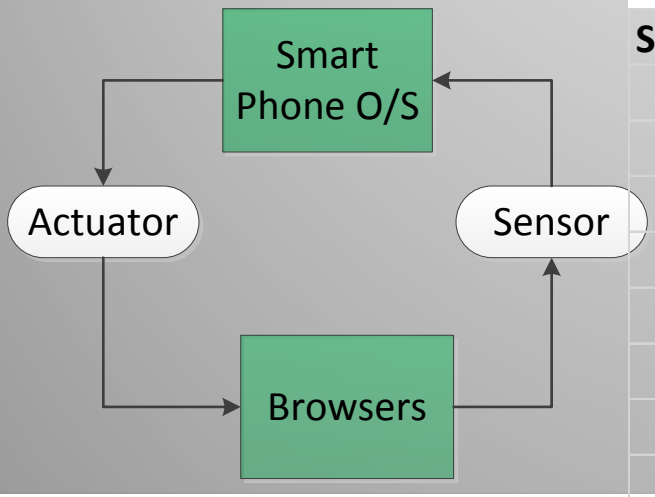


Cellular/Smart Phones
Juice Jacking
Faux Cell Tower

Mobile Phone and Update Sub-Subsystem Risks



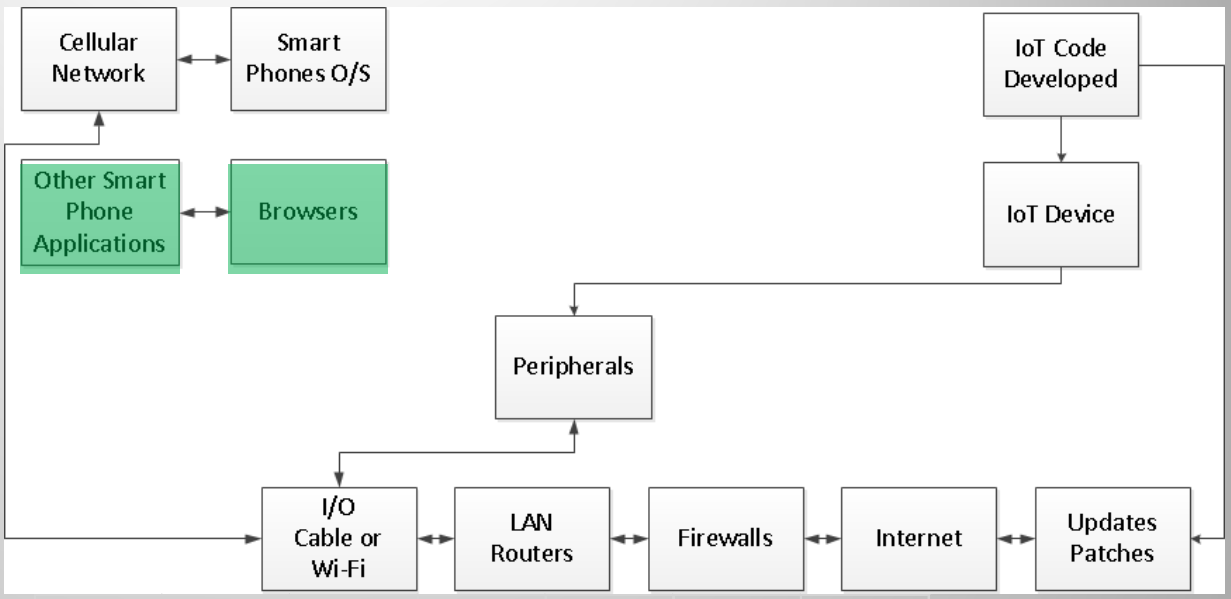


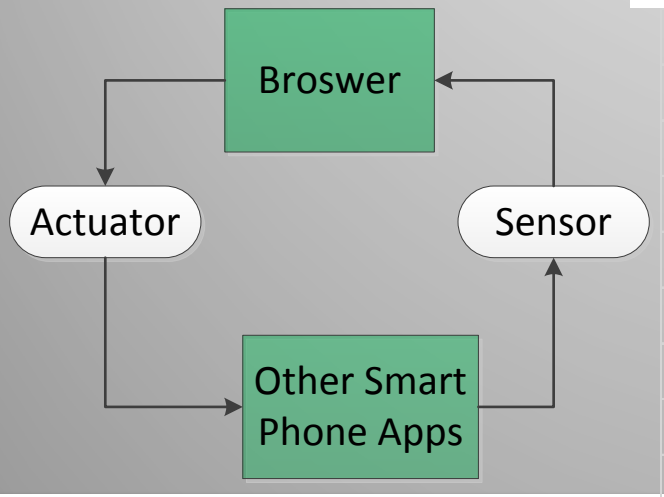


Smart Phones/Browser

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

Mobile Phone and Update Sub-Subsystem Risks

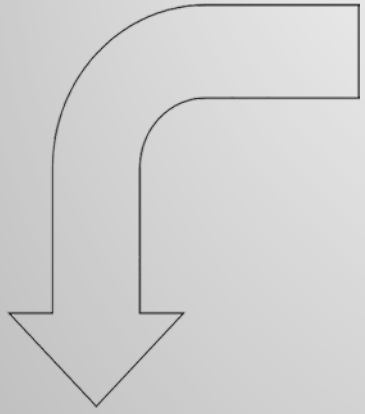


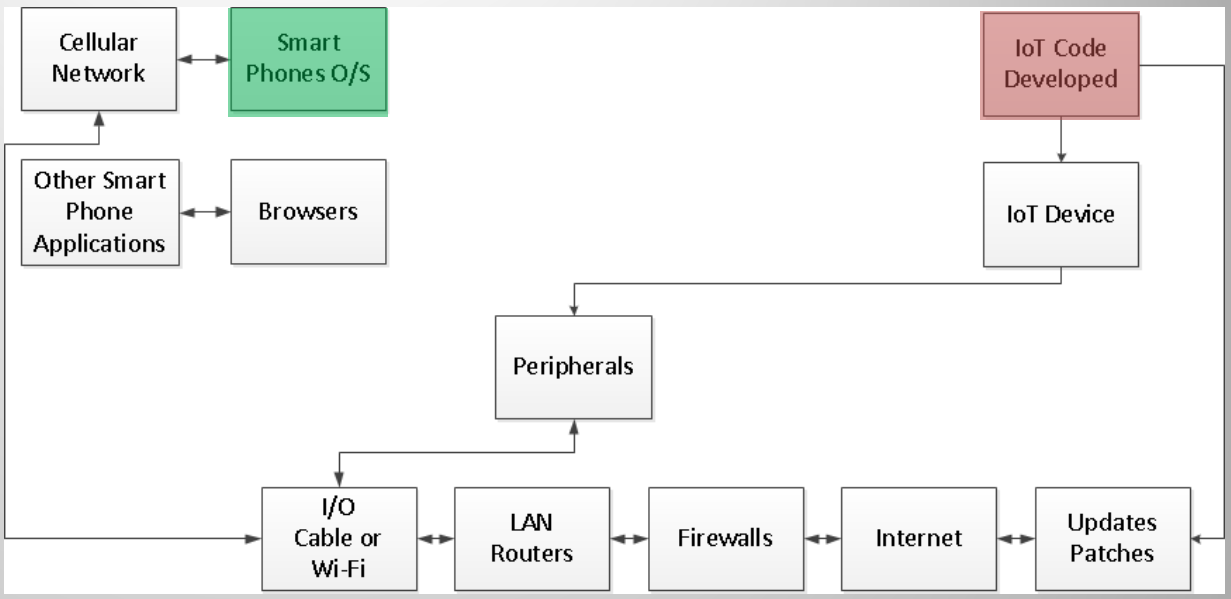


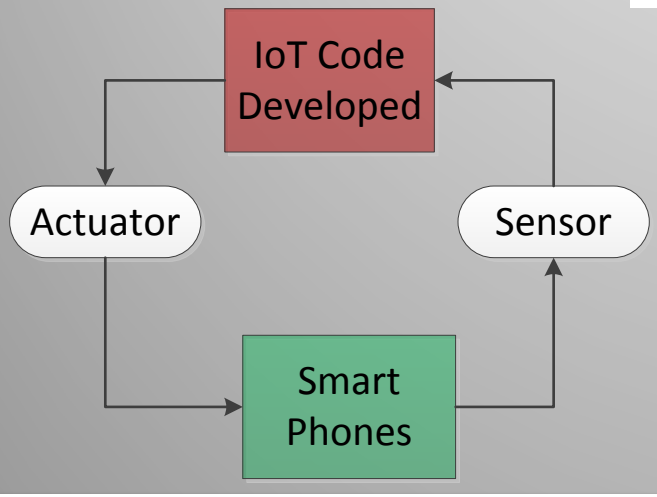
Browsers/Other Apps

- **Not Downloaded From Trusted Source**
- **Malicious Apps**
- **Apps Not Updated**
- **App No Longer Supported**
- **Apps Not Updated**

Mobile Phone and Update Sub- Subsystem Risks







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