28th Annual INCOSE
international symposium

Washington, DC, USA
July 7 - 12, 2018

Casey Medina, CSEP

Risk Management Limbo – How Low Can You Go?

Question:

What do Engineers Think of Risk Management?

Those who have had a good experience

Drive Requirements

Keeps people safe

Think it through

Keeps R&D honest

Useful if done correctly

Time consuming, but useful

Those who have had a bad experience

UGH!

Yikes!

AHHHHH!

PITA – Pain in the A@#

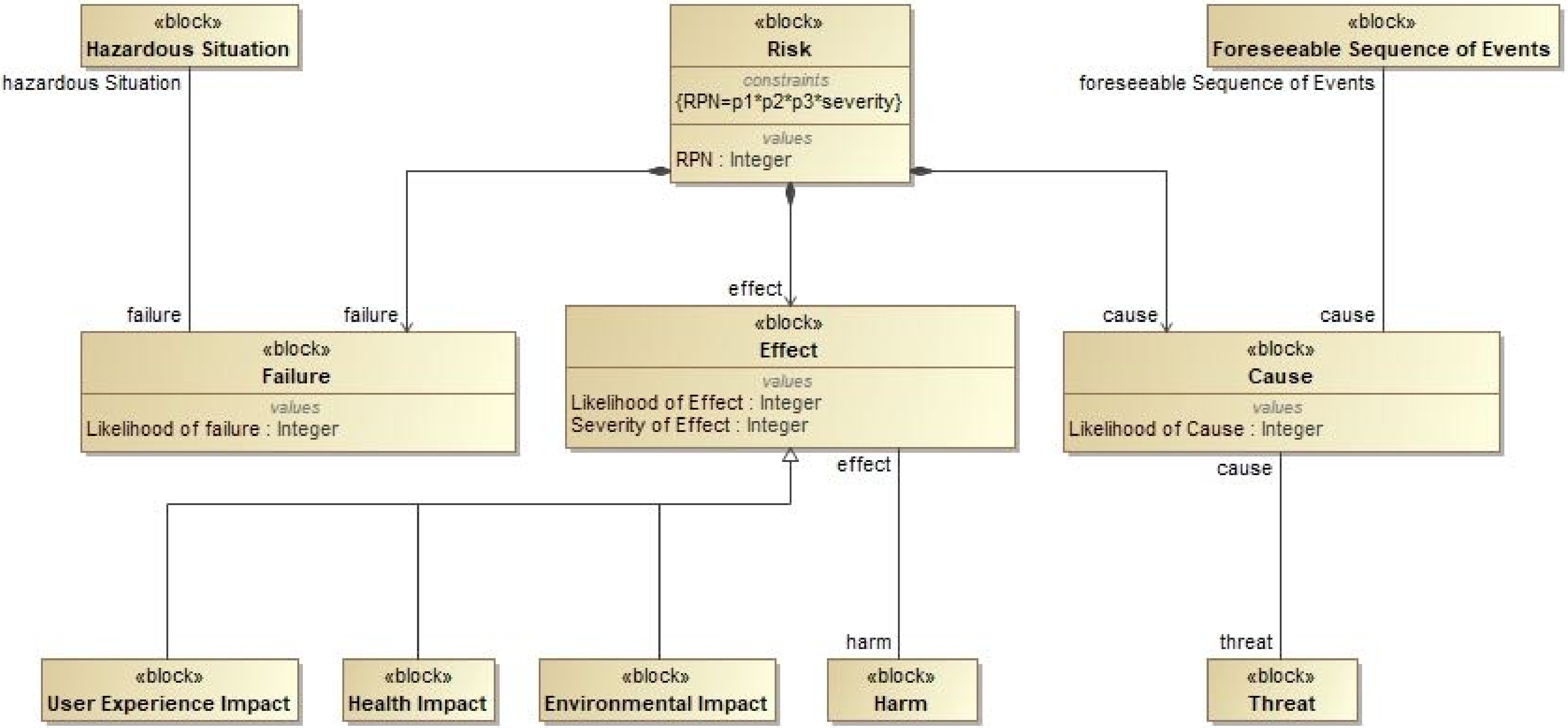
Nonsense - We’ve already taken care of risk in the design.

Necessary to check-the-box for compliance

As Low As Possible

B media

We Need a Common Vocabulary



Risk = f(threat, potential outcomes, performance effects)

What are Threat Classes?

- Malicious human interactions
- Use errors
- Natural environment
- Stimuli from external systems

Lifecycle of a Threat

- Phase 1 – Threat condition(s) appears
- Phase 2 – System encounters threat condition(s)
- Phase 3 – System’s response to the threat condition(s) has resolved

Adapted from the work of Jackson and Ferris.

What can the system do?

- Eliminate the cause
- Avoid the failure
- Reduce the likelihood or severity of the effects

ISO 14971:2012 Mitigation Types

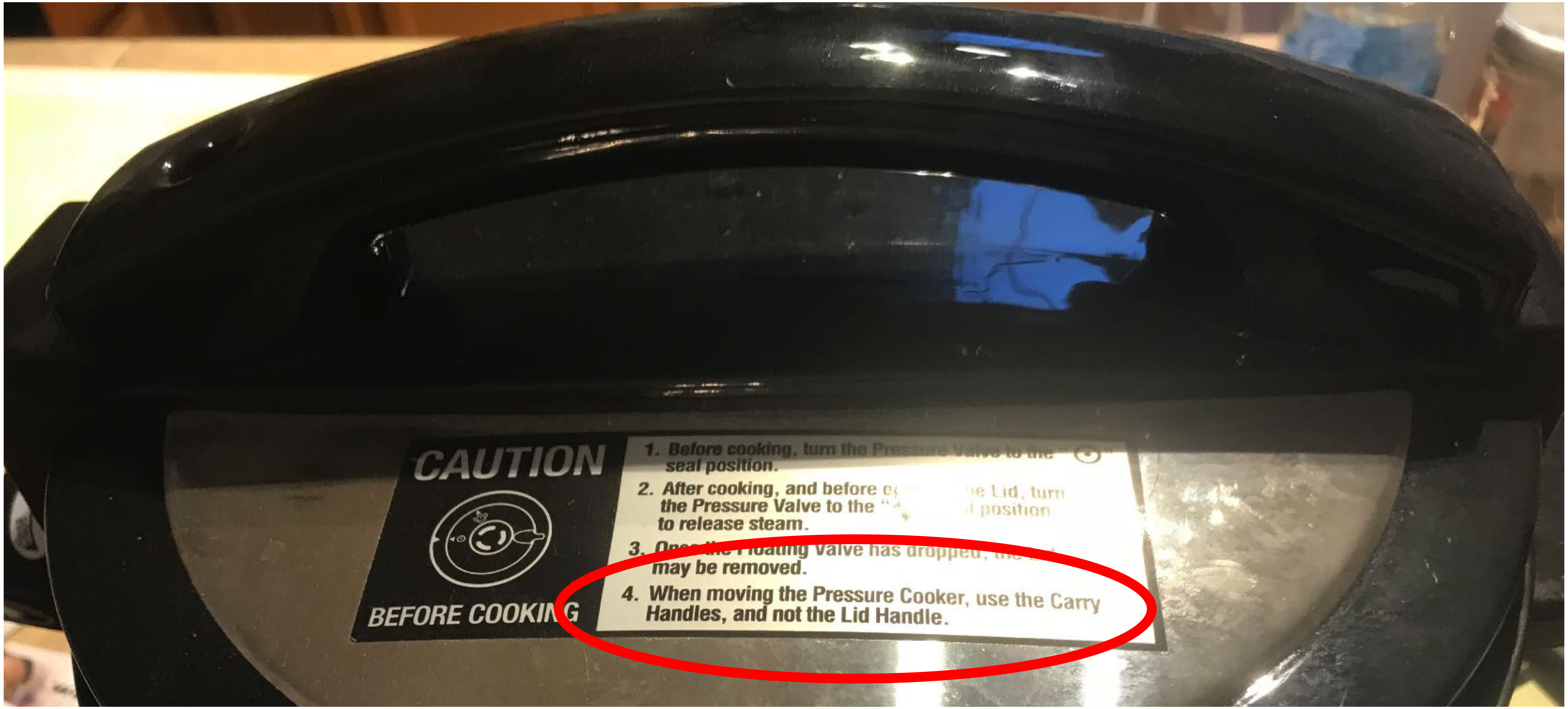
- Inherent Safety by Design
- Protective Measures in the System or Manufacturing Process

Effective

Not Effective

- Information for Safety
- Disclosure of Residual risk

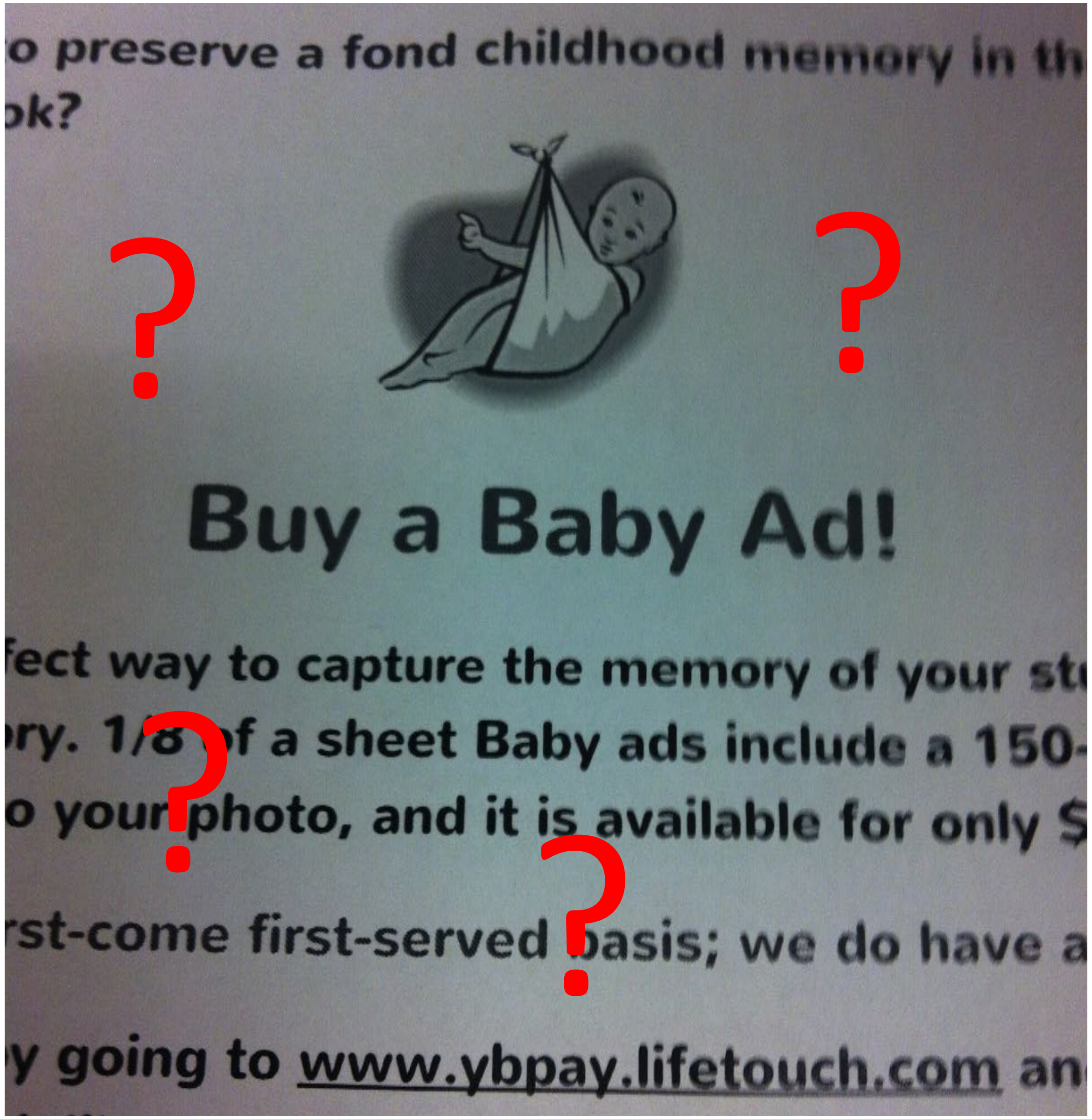
CAUTION: Burn Hazard
Contains Hot Contents
POWER
PRESSURE COOKER XL™
DELAY TIMER
CANNING/PRESERVING
SOUP/STEW
SLOW COOK
RICE/RISOTTO
BEANS/LENTILS
FISH/VEGETABLES STEAM
CHICKEN/MEAT
TIME ADJUSTMENT
KEEP WARM/CANCEL
FOOD: QUICK — MEDIUM — WELL
RICE: WHITE — BROWN — WILD
SAUTE



CAUTION

BEFORE COOKING

1. Before cooking, turn the Pressure Valve to the "⊙" seal position.
2. After cooking, and before [illegible] the Lid, turn the Pressure Valve to the "[illegible]" position to release steam.
3. Once the Floating Valve has dropped, the Lid may be removed.
4. When moving the Pressure Cooker, use the Carry Handles, and not the Lid Handle.



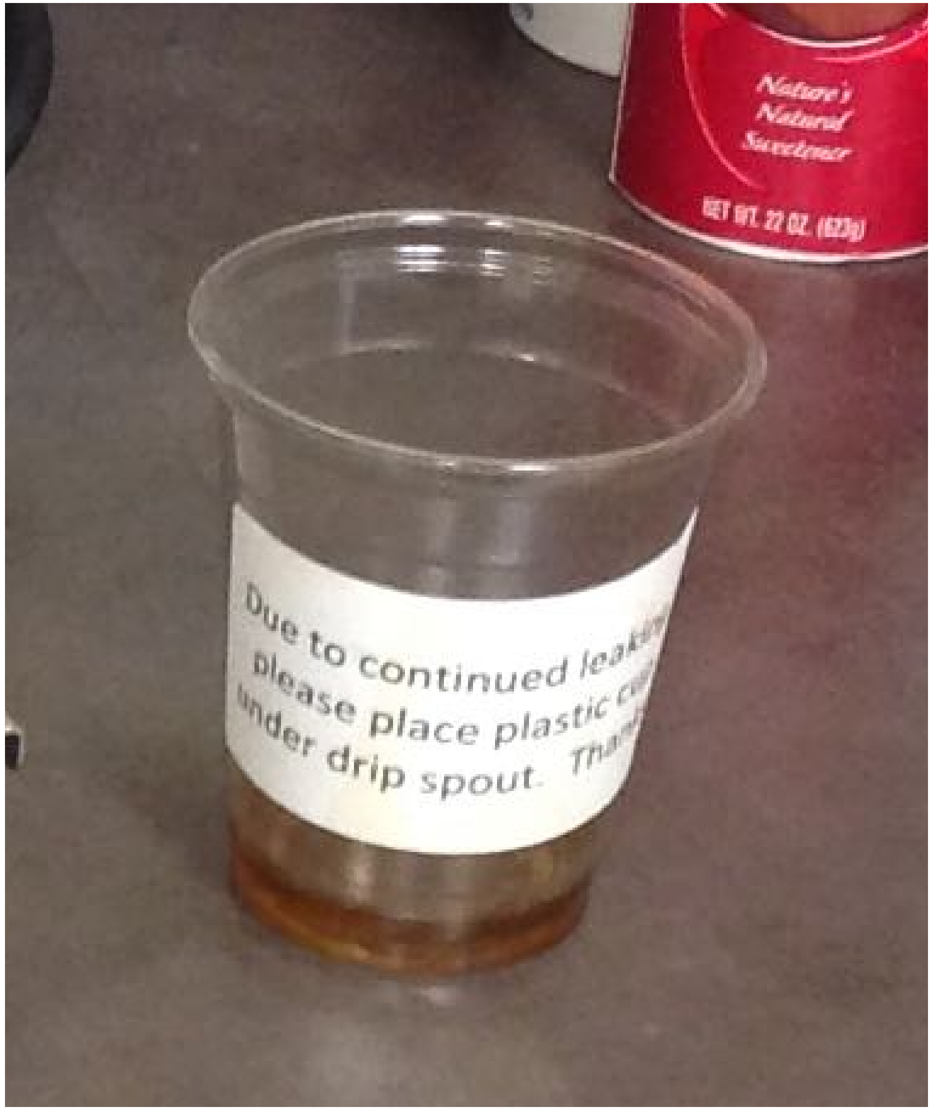
o preserve a fond childhood memory in th
ok?

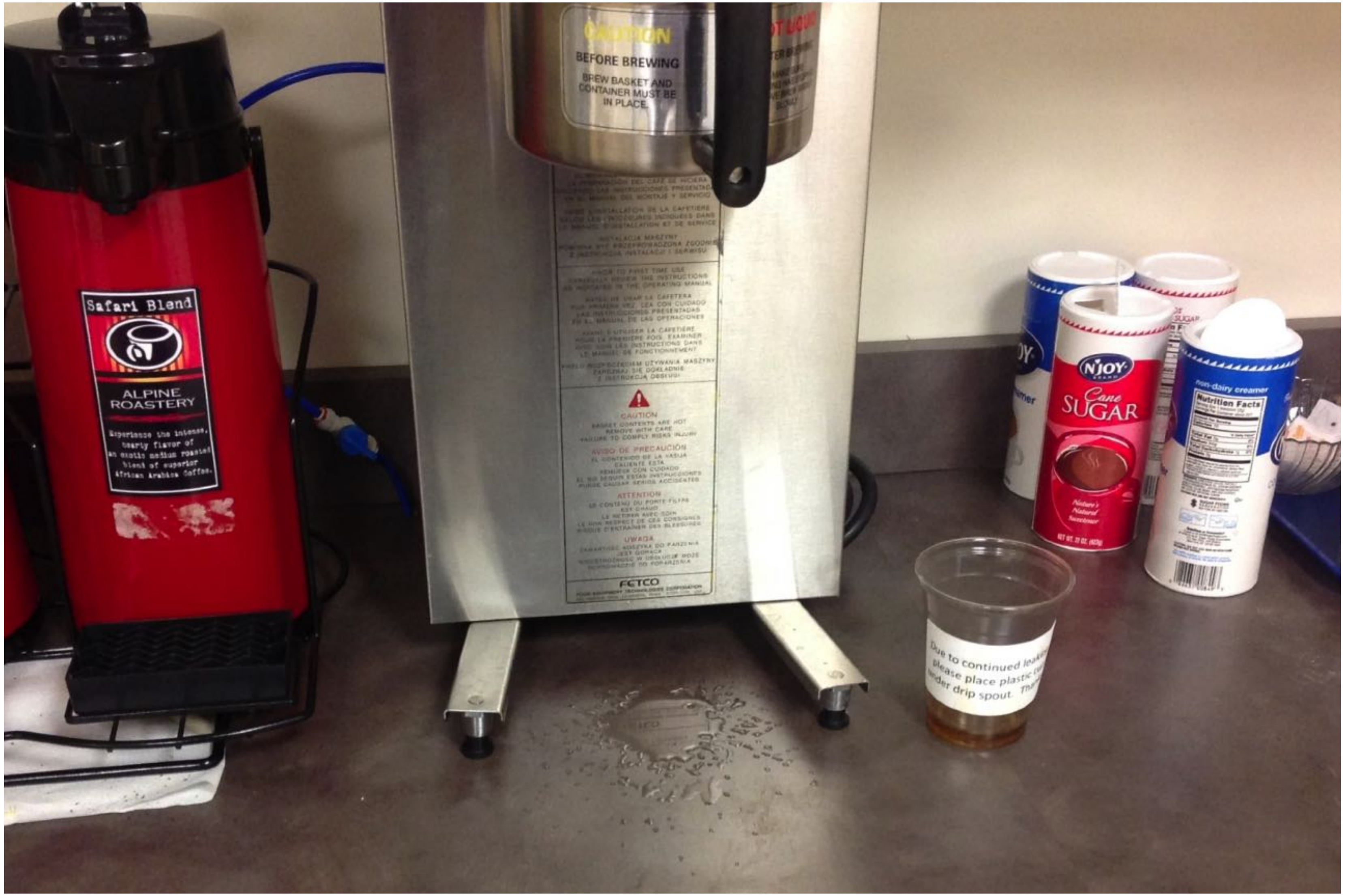
Buy a Baby Ad!

fect way to capture the memory of your st
ry. 1/8 of a sheet Baby ads include a 150
o your photo, and it is available for only $

rst-come first-served basis; we do have a

y going to www.ybpay.lifetouch.com an


Nature's Natural Sweetener
NET WT. 22 OZ. (623g)
Due to continued leaking
please place plastic cup
under drip spout. Tha


Safari Blend
ALPINE ROASTERY
Experience the intense, earthy flavor of an exotic medium roasted blend of superior African Arabica Coffee.
CAUTION
BEFORE BREWING
BREW BASKET AND CONTAINER MUST BE IN PLACE
FETCO
N'JOY
Cane SUGAR
non-dairy creamer
Nutrition Facts
Due to continued leaki
please place plastic cu
under drip spout. Tha

Network Reslience Concepts - Resilinets

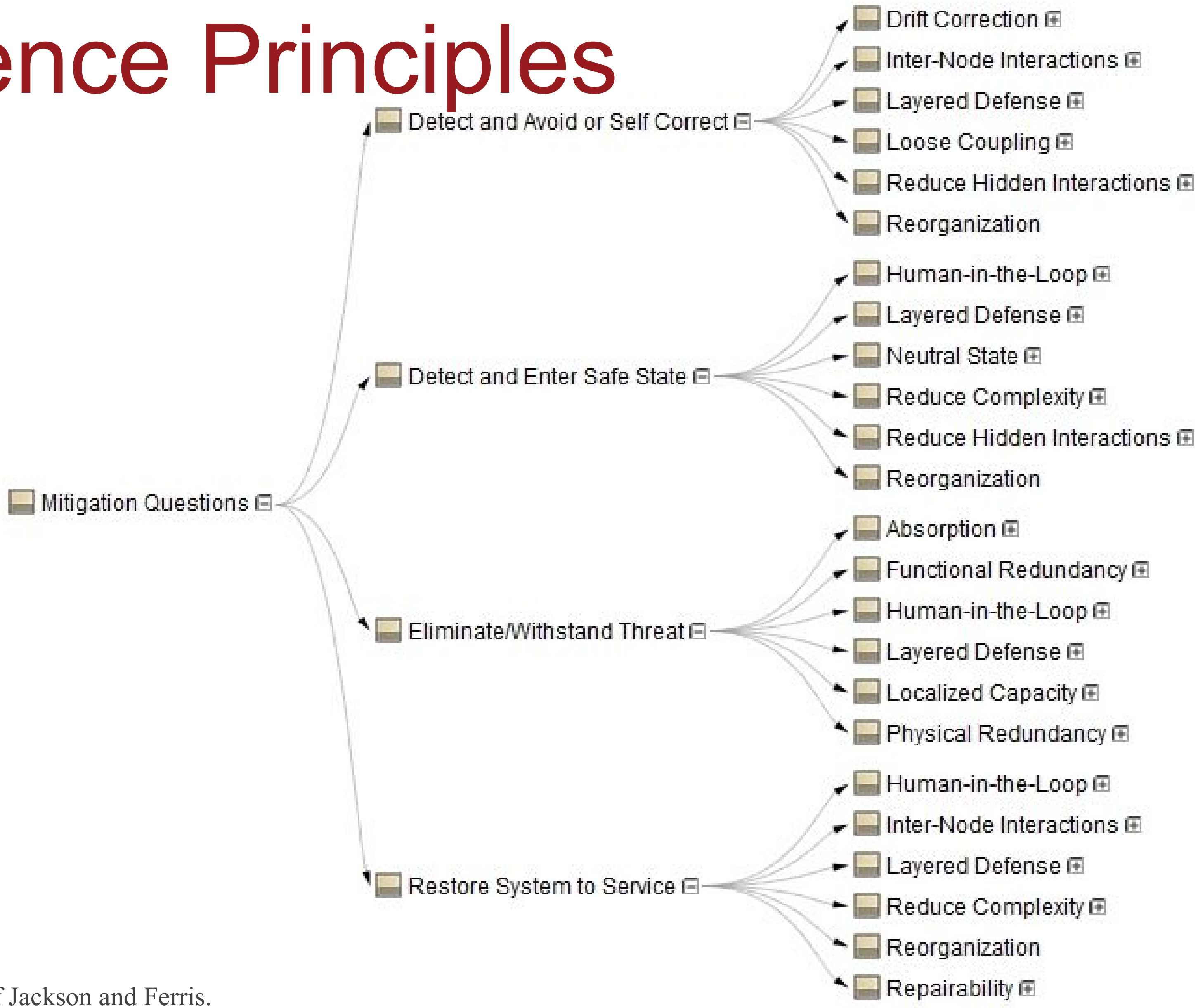
- Defend
- Detect
- Remediate
- Recover

Sterbenz et al.

How do the methodologies map?

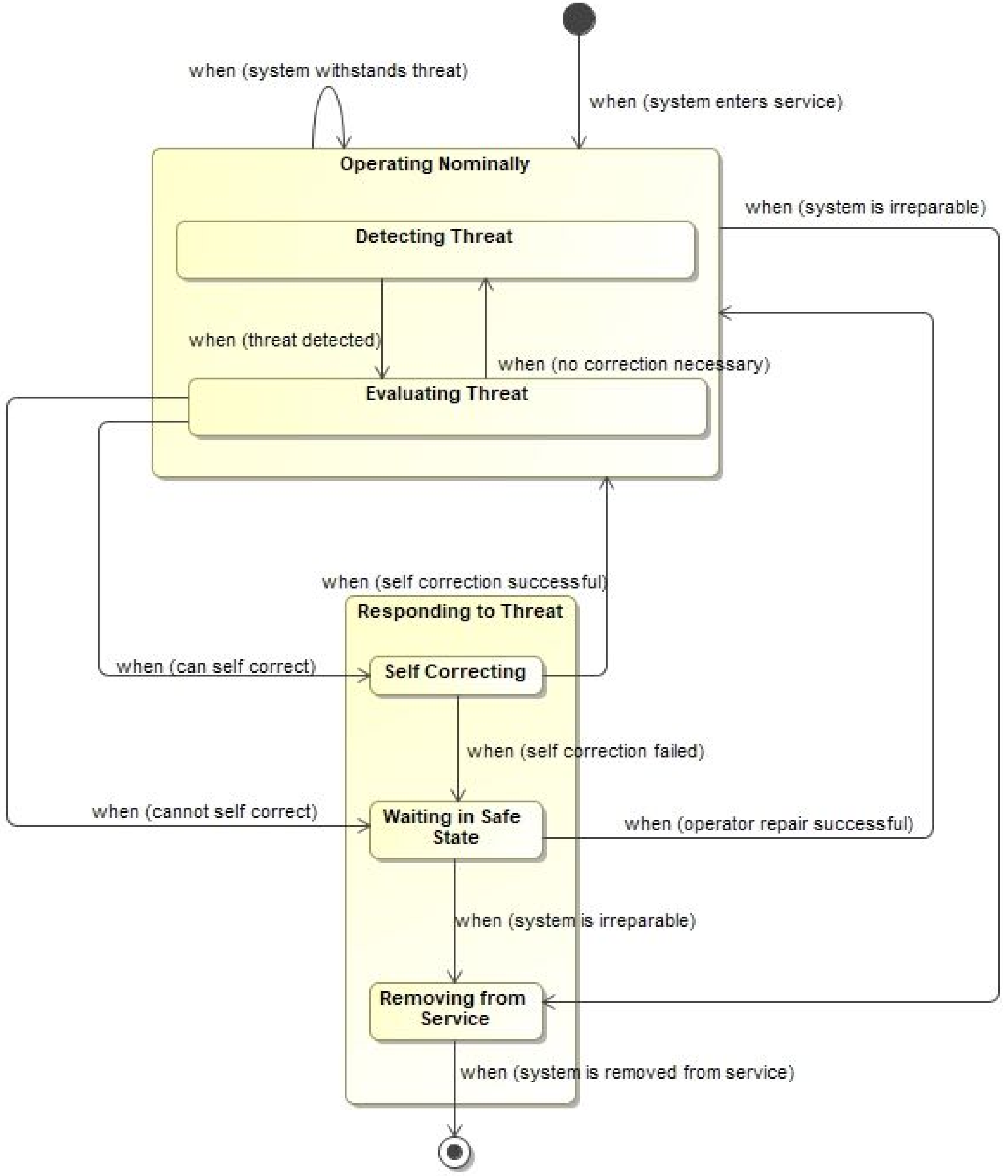
	ISO 14971:2012	Resilinets
Eliminate/Withstand	Inherent Safety by Design	Defend
Detect and Avoid/Self-Correct	Protective Measures	Detect, Remediate, Recover
Detect and Enter Safe State	Protective Measures, Information for Safety*	Detect, Remediate, Recover
Restore to Service	Protective Measures, Information for Safety*	Recover

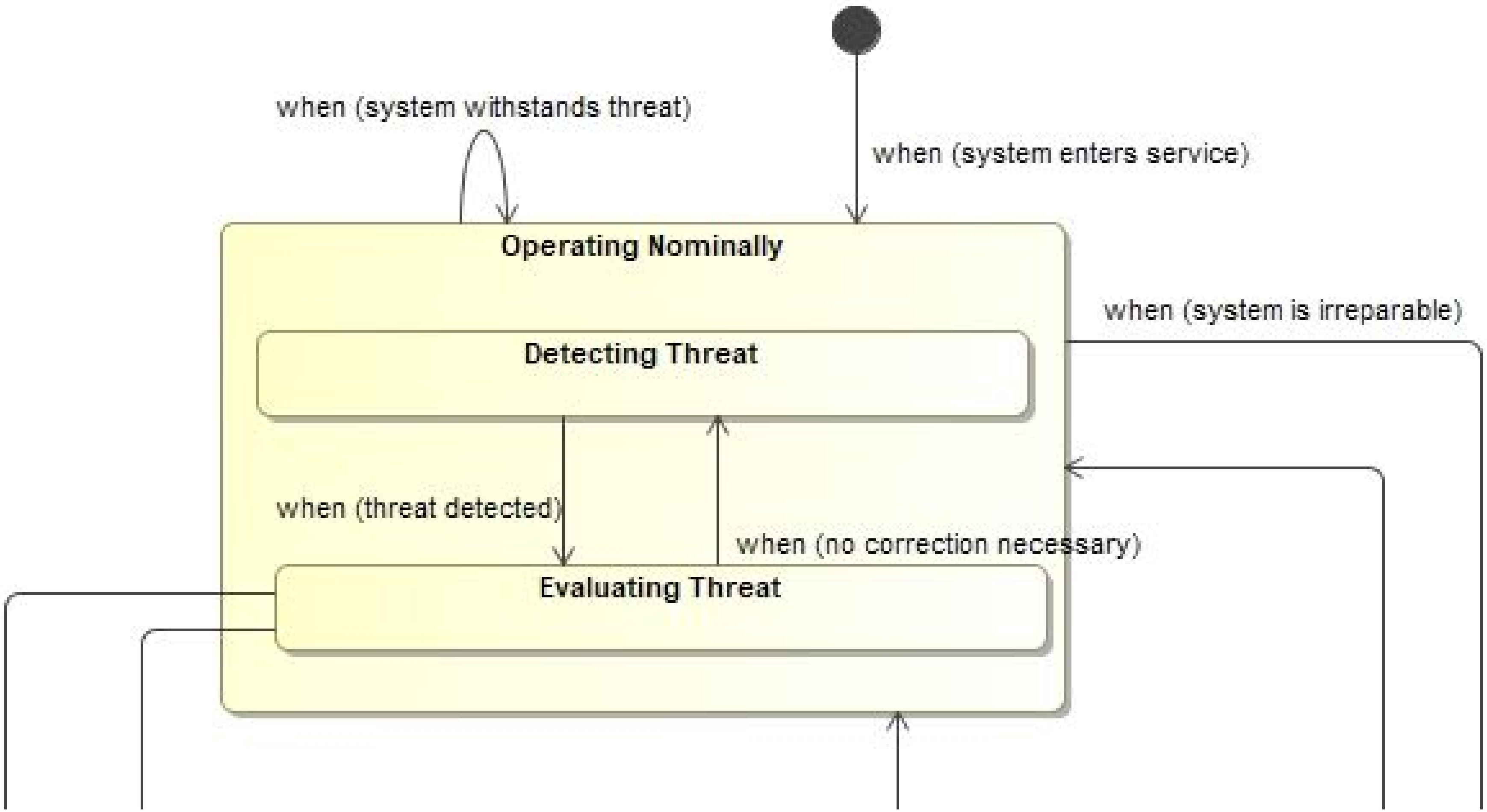
Resilience Principles

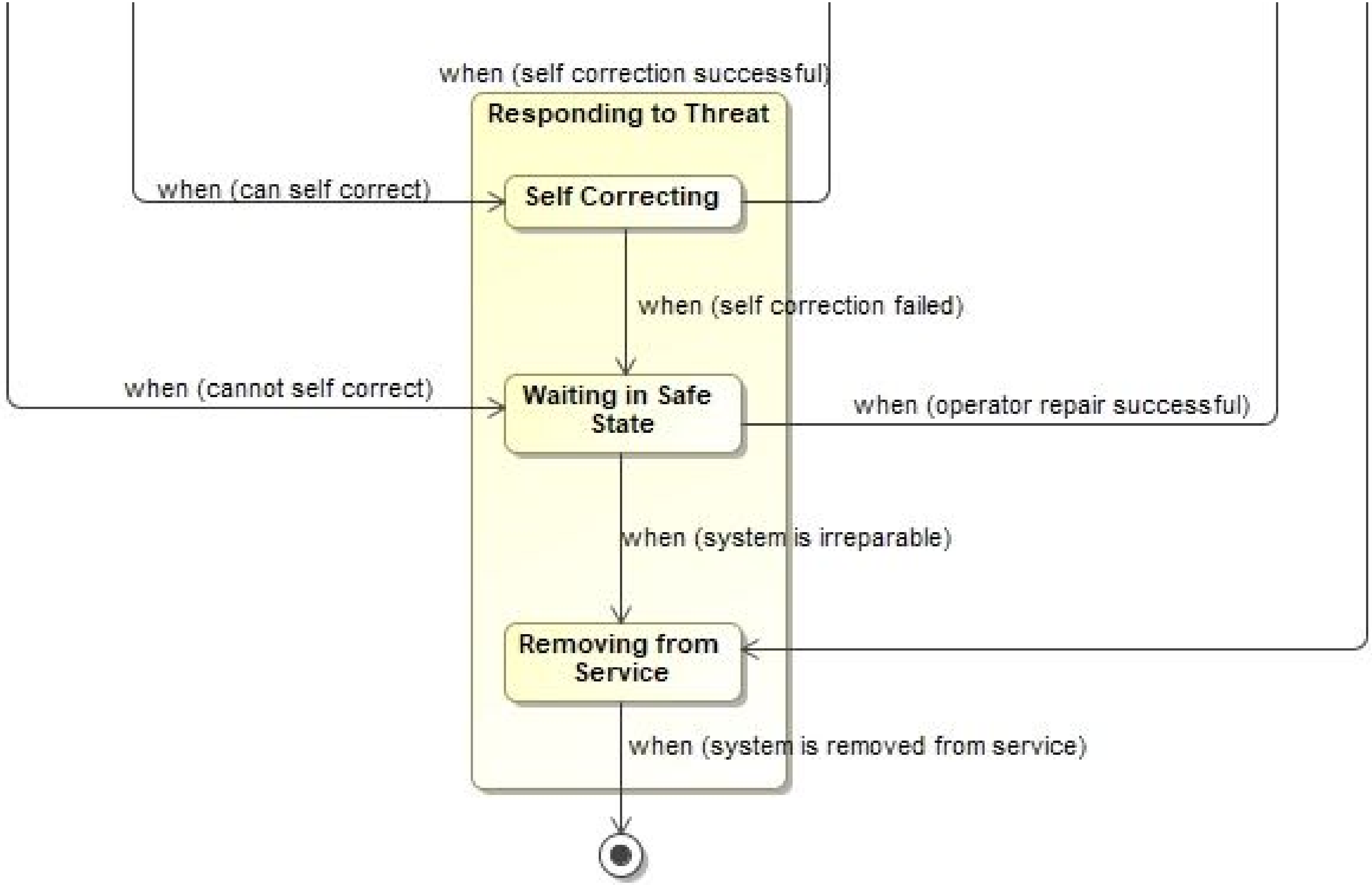


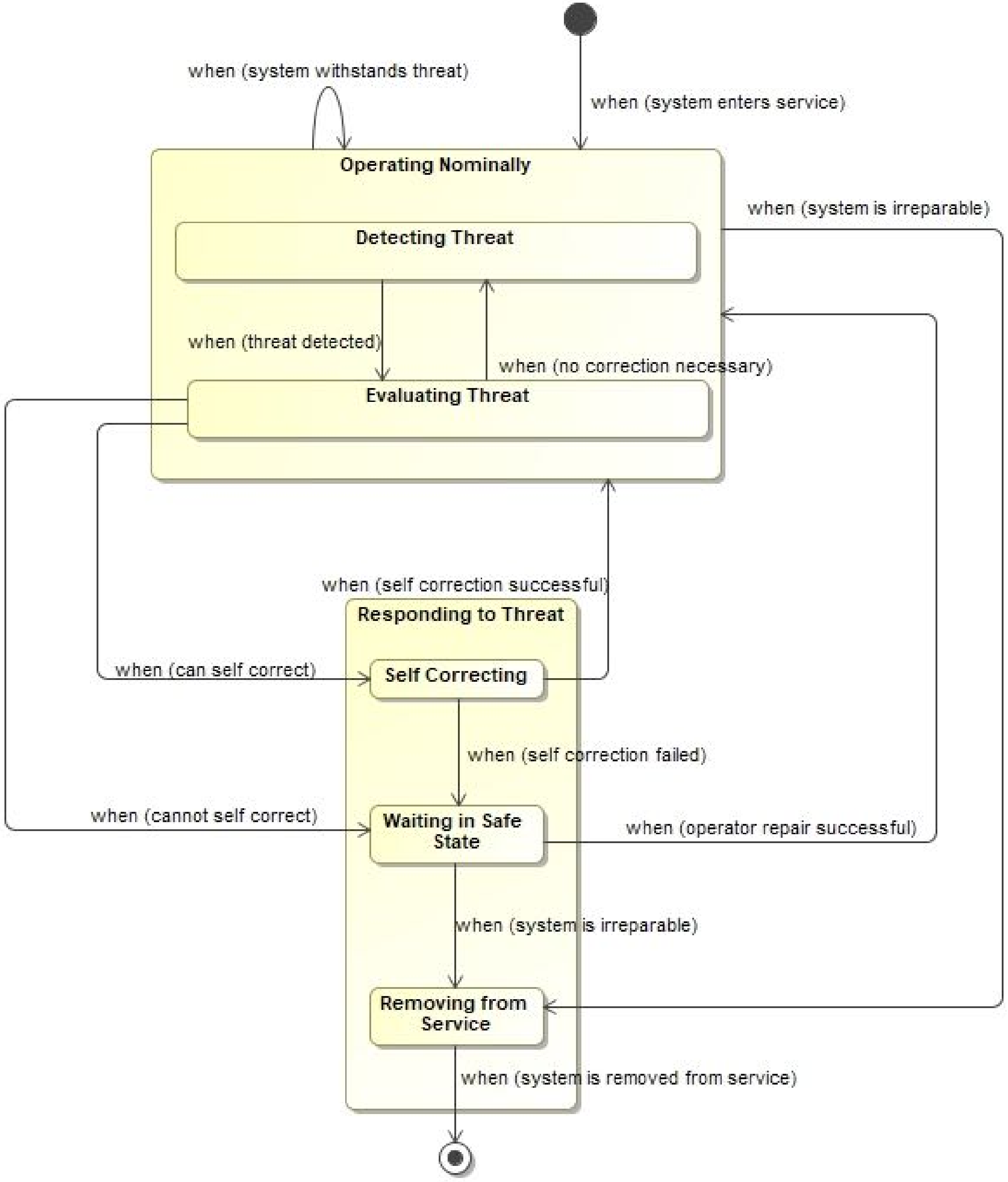
- Mitigation Questions
  - Detect and Avoid or Self Correct
    - Drift Correction
    - Inter-Node Interactions
    - Layered Defense
    - Loose Coupling
    - Reduce Hidden Interactions
    - Reorganization
  - Detect and Enter Safe State
    - Human-in-the-Loop
    - Layered Defense
    - Neutral State
    - Reduce Complexity
    - Reduce Hidden Interactions
    - Reorganization
  - Eliminate/Withstand Threat
    - Absorption
    - Functional Redundancy
    - Human-in-the-Loop
    - Layered Defense
    - Localized Capacity
    - Physical Redundancy
  - Restore System to Service
    - Human-in-the-Loop
    - Inter-Node Interactions
    - Layered Defense
    - Reduce Complexity
    - Reorganization
    - Repairability

Adapted from the work of Jackson and Ferris.


when (system withstands threat)
when (system enters service)
Operating Nominally
when (system is irreparable)
Detecting Threat
when (threat detected)
when (no correction necessary)
Evaluating Threat
when (self correction successful)
Responding to Threat
when (can self correct)
Self Correcting
when (self correction failed)
when (cannot self correct)
Waiting in Safe State
when (operator repair successful)
when (system is irreparable)
Removing from Service
when (system is removed from service)


when (system withstands threat)
when (system enters service)
Operating Nominally
when (system is irreparable)
Detecting Threat
when (threat detected)
when (no correction necessary)
Evaluating Threat


when (self correction successful)
Responding to Threat
when (can self correct)
Self Correcting
when (self correction failed)
when (cannot self correct)
Waiting in Safe State
when (operator repair successful)
when (system is irreparable)
Removing from Service
when (system is removed from service)


when (system withstands threat)
when (system enters service)
Operating Nominally
Detecting Threat
when (system is irreparable)
when (threat detected)
when (no correction necessary)
Evaluating Threat
when (self correction successful)
Responding to Threat
when (can self correct)
Self Correcting
when (self correction failed)
when (cannot self correct)
Waiting in Safe State
when (operator repair successful)
when (system is irreparable)
Removing from Service
when (system is removed from service)

How does (should) the system handle threats?

- Can the system be designed such that the threat is eliminated? Can I add margin or redundancy?

- *Example: Reducing the weight of a device's lid so it does not injure a user's hand if it falls.*

- Inherent Safety by Design, "Defend;" Addresses Phases 1 and 2.

How does (should) the system handle threats?

- Can the system be designed to detect and avoid the threat to prevent loss of functionality or self-correct to restore full functionality if the threat cannot be avoided?

- *Example: Distribution of function between two, separate processors in a system. A "watch dog" monitors process parameters and interrupts the primary processor to prevent the system from entering an unsafe state.*

- Protective Measures, "Detect and Remediate;" Addresses Phases 1 and 2.

How does (should) the system handle threats?

- Can the system be designed to detect the threat and enter a safe state to wait for a user to restore the system to operation?

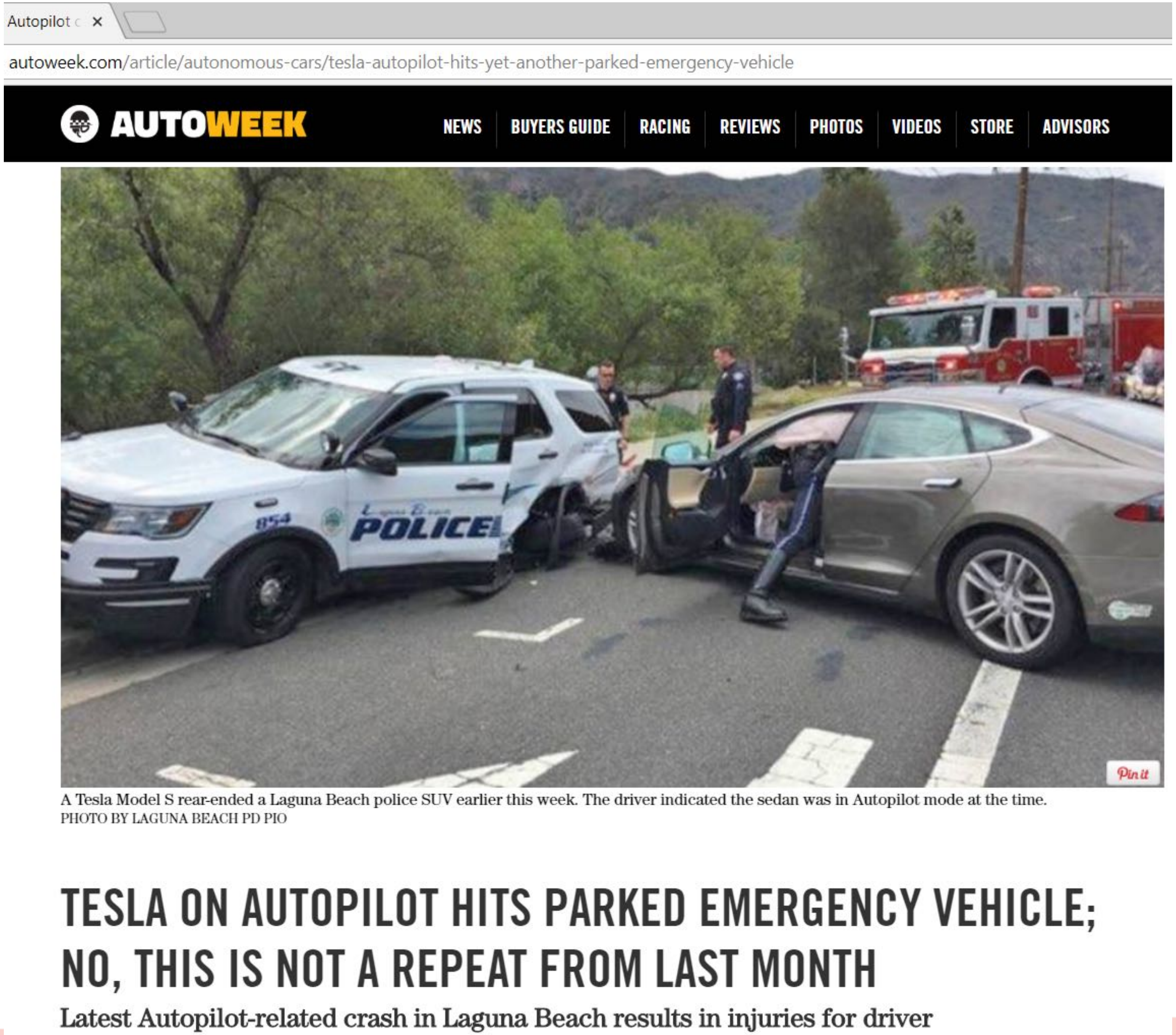
- *Example: The system detects a parameter is out of specification and pauses the function until an operator can resolve the anomaly.*

- Protective Measures, “Detect and Remediate;” Addresses Phases 1 and 2.

Are alarms inherently safe design?

Alarms are ***not*** inherently safe design.

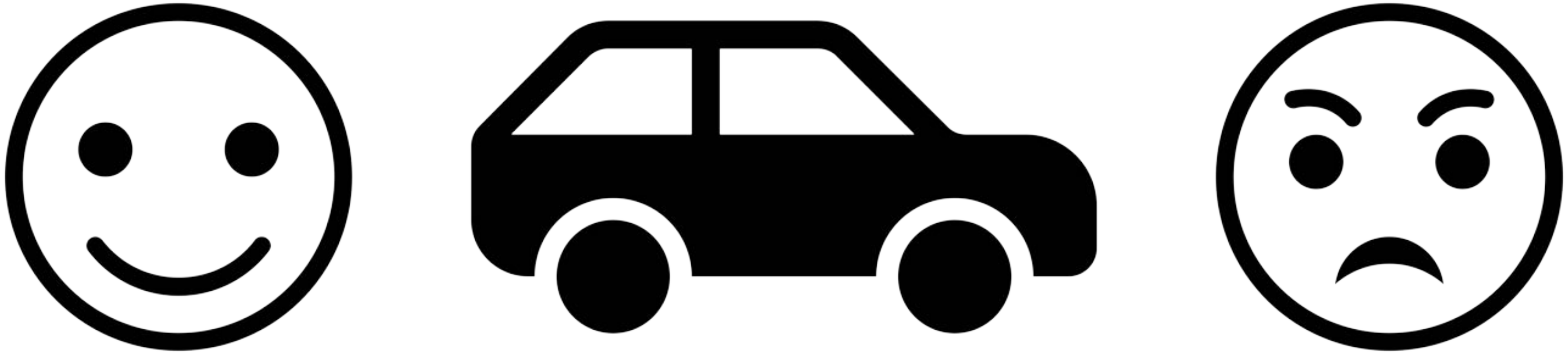
ADY™
+ SPAR
DY™ PRIMER
EVLON
www.drewcareyshow.com
© 2000 Warner Bros.



A Tesla Model S rear-ended a Laguna Beach police SUV earlier this week. The driver indicated the sedan was in Autopilot mode at the time.
PHOTO BY LAGUNA BEACH PD PIO

TESLA ON AUTOPILOT HITS PARKED EMERGENCY VEHICLE; NO, THIS IS NOT A REPEAT FROM LAST MONTH

Latest Autopilot-related crash in Laguna Beach results in injuries for driver

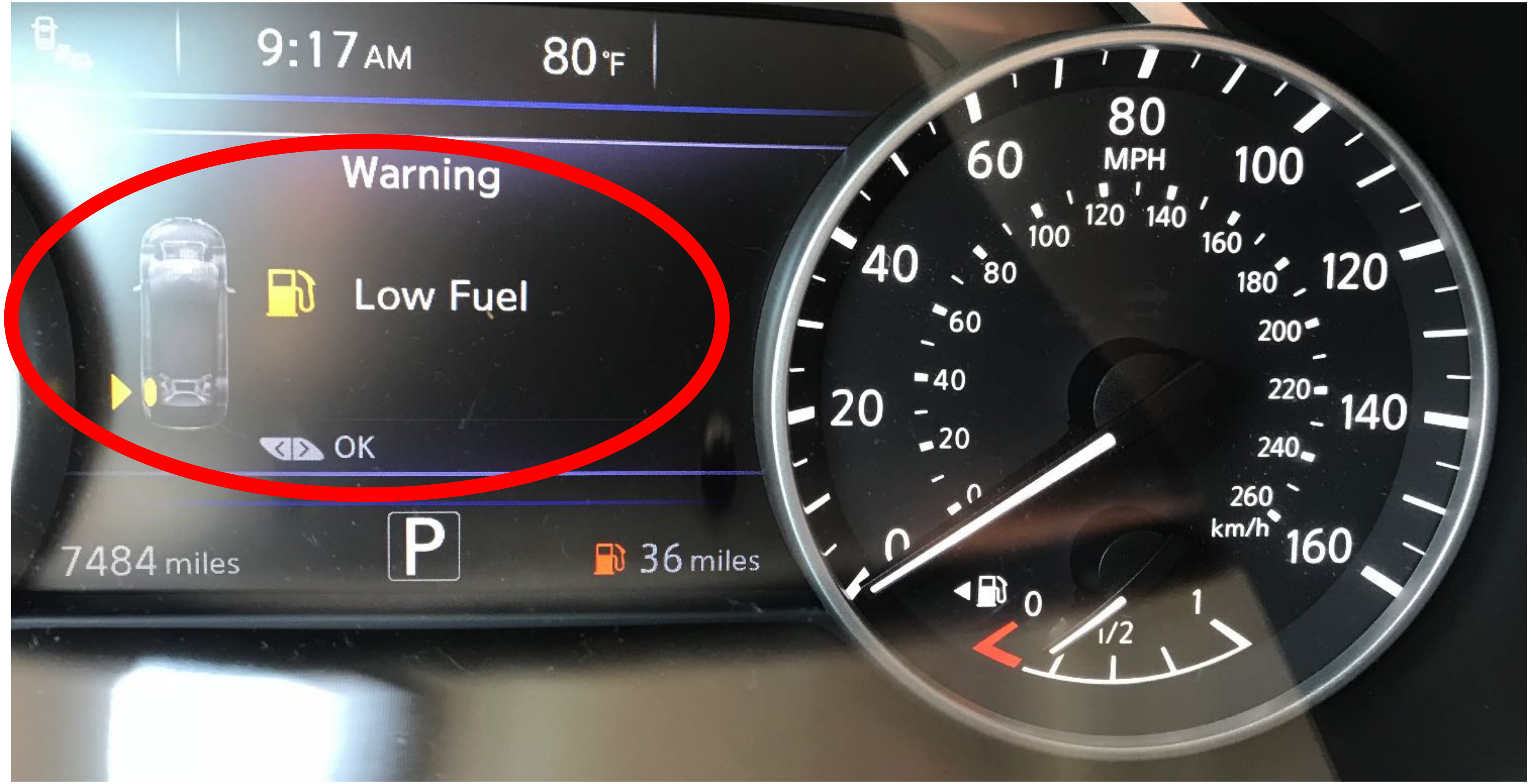


How does (should) the system handle threats?

- What is the path by which the system can be returned to its nominal, operating state after the threat has been resolved? What should happen if the system cannot be returned to service?

- *Example: System provides context-specific troubleshooting tips to help the operator resolve the problem.*

- Protective Measures & Info for Safety, "Recover;" Addresses Phase 3.

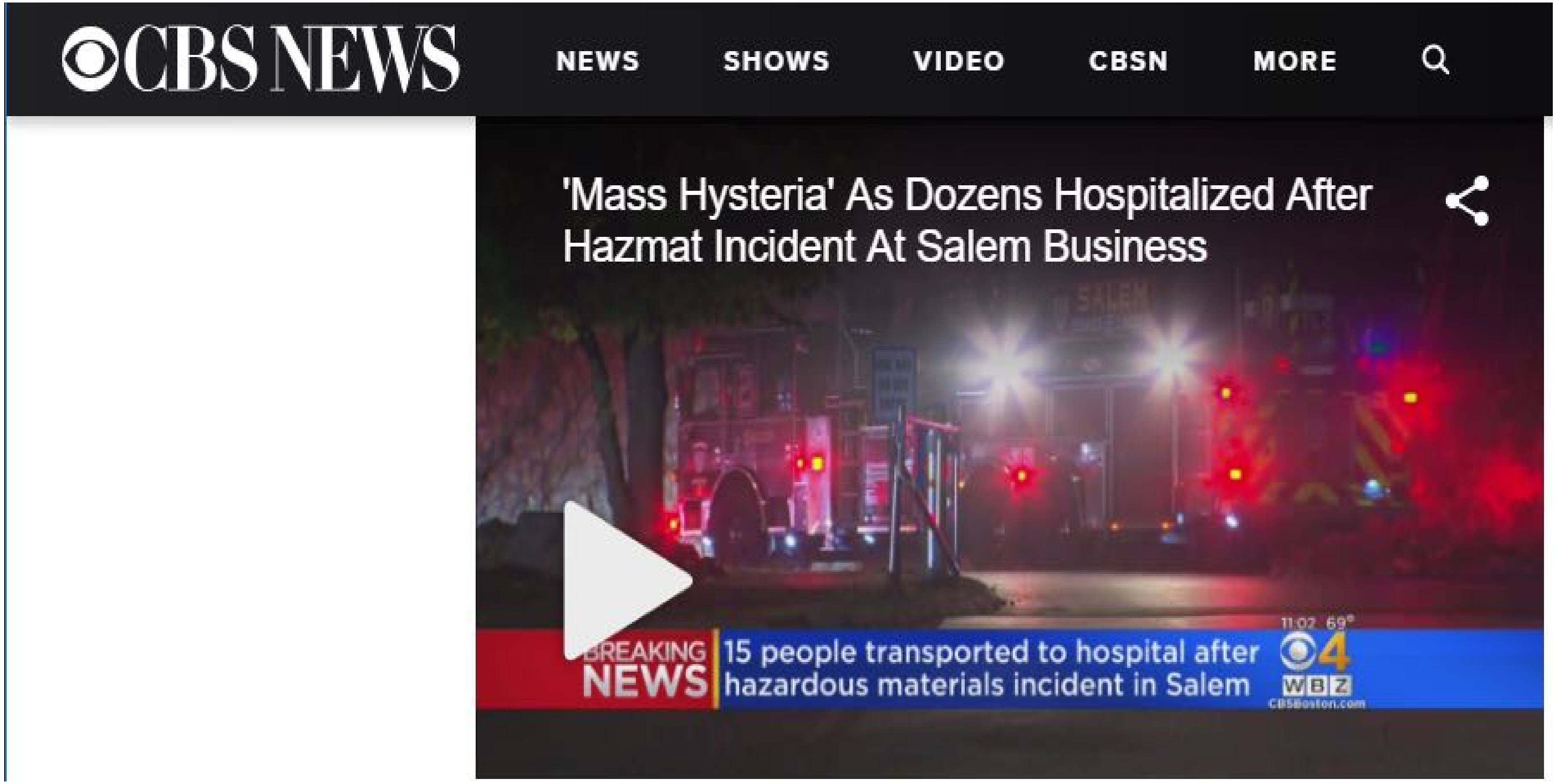

9:17 AM
80°F
Warning
Low Fuel
OK
7484 miles
P
36 miles
MPH
km/h
0
1/2
1

We still haven’t addressed the most important question:

How do I get to “As Low As Possible?”

Photo Credit: Lain A. Wanless https://www.flickr.com/photos/reemul/7338644262

The case for “As Low As Possible”

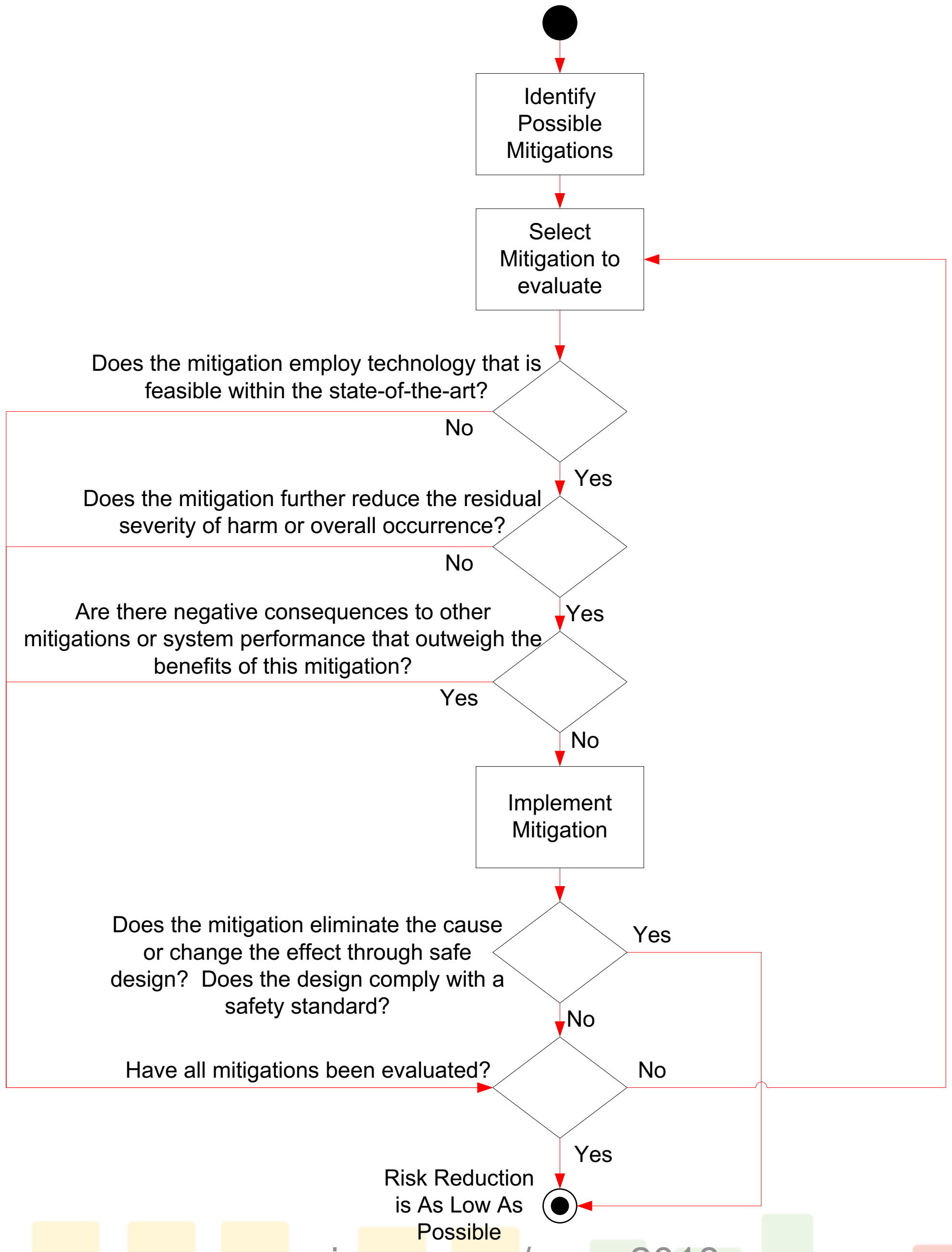


'Mass Hysteria' As Dozens Hospitalized After Hazmat Incident At Salem Business

BREAKING NEWS

15 people transported to hospital after hazardous materials incident in Salem

https://www.cbsnews.com/news/thermal-circuits-e-cigarette-plant-chlorine-leak-salem-massachusetts-hazmat-sick-workers/



Identify Possible Mitigations

Select Mitigation to evaluate

Does the mitigation employ technology that is feasible within the state-of-the-art?

No

Yes

Does the mitigation further reduce the residual severity of harm or overall occurrence?

No

Yes

Are there negative consequences to other mitigations or system performance that outweigh the benefits of this mitigation?

Yes

No

Implement Mitigation

Does the mitigation eliminate the cause or change the effect through safe design? Does the design comply with a safety standard?

Yes

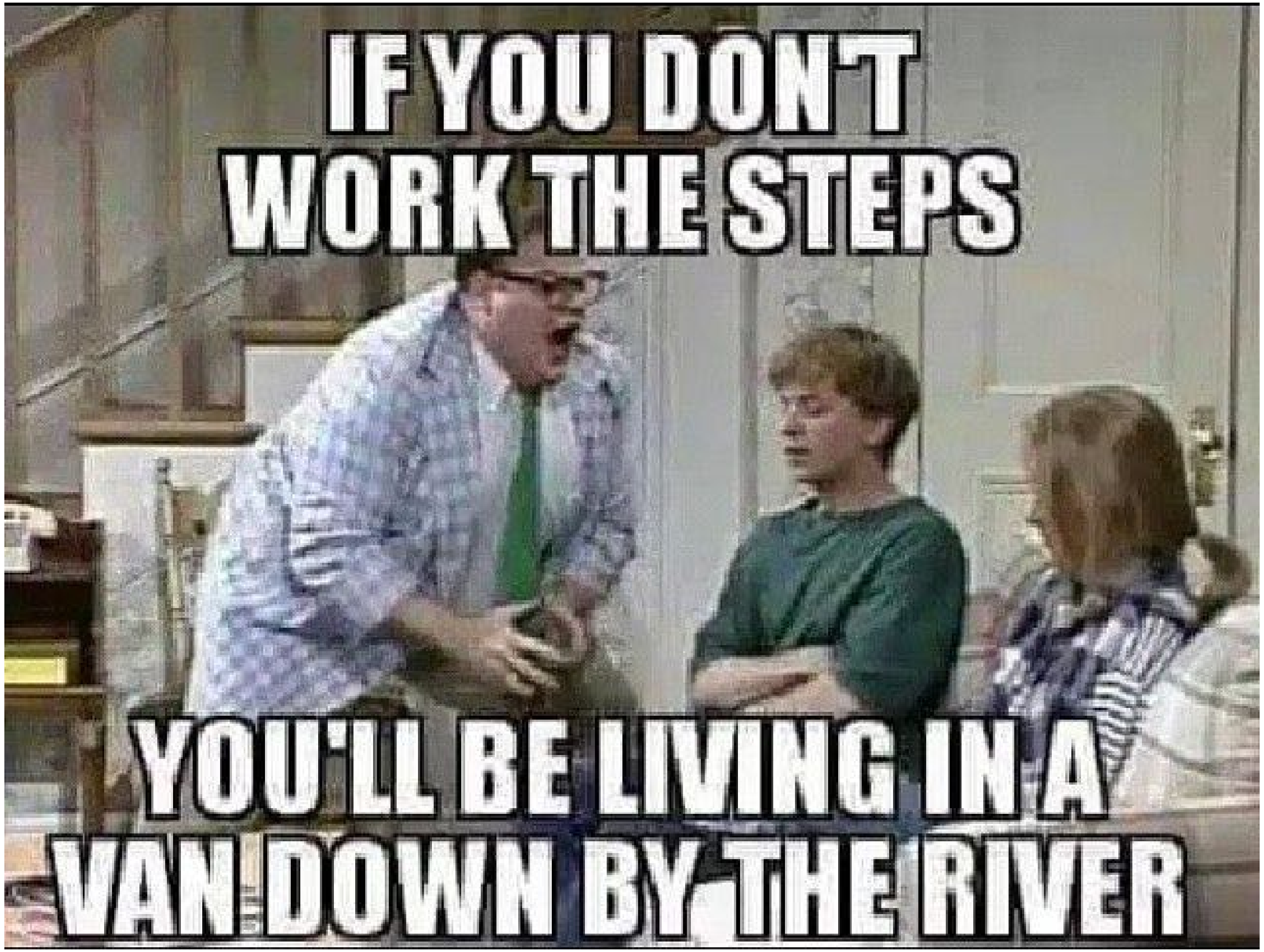
No

Have all mitigations been evaluated?

No

Yes

Risk Reduction is As Low As Possible


IF YOU DON'T
WORK THE STEPS
YOU'LL BE LIVING IN A
VAN DOWN BY THE RIVER

28th Annual **INCOSE**
international symposium

Washington, DC, USA
July 7 - 12, 2018

www.incose.org/symp2018

Questions?

How does (should) the system handle threats?

What does the system need to do to maintain its performance in the presence of threats?

Use case study of Salem plant illness

- Risk management work didn’t adequately answer the last question about how to return to service.