Using STPA and CAST to Design for Serviceability and Diagnostics

Hannah Slominski

System Design & Management Program Masters Thesis, May 2020

Advisor: Nancy Leveson

Massachusetts Institute of Technology

“Why does it say paper jam, when there is no paper jam!?!”
-- *Samir Nagheenanajar (Actor: Ajay Naidu), Office Space 1998*

Motivation

Increased challenges meeting customer needs for equipment serviceability and support

- Increased product complexity
- Fast rate of technology change
- Technician shortages
- Increasing cost of machine unavailability

Motivation

Finally a method that accounts for emerging behavior and manages system complexity!

Curious about STPA applications beyond safety

- Security (Young & Leveson, 2013)
- Producibility (Ball, 2015)
- Quality (Goerges, 2013)
- Testing (Montes, 2016)

Purpose

Can STPA and CAST be used to improve product serviceability?

- Can it generate hardware and software serviceability requirements?
- Can it generate recommendations for the product development?
- Are any analysis modifications are required?

Can safety-STPA control structure be reused for serviceability?

Approach

CAST Case Study

- Existing diagnostic issue
- Analyzed full hierarchical control structure

STPA Case Study

- Future system early in conceptual phase, software-intensive
- Safety analysis, then serviceability analysis

Massachusetts Institute of Technology

https://www.suu.edu/aviation/maintenance/
https://www.tru.ca/trades/trades-programs/automotive-service-technician.html

Case Study 1: CAST Results

3 Physical Process Recommendations

6 Physical Process Control Recommendations

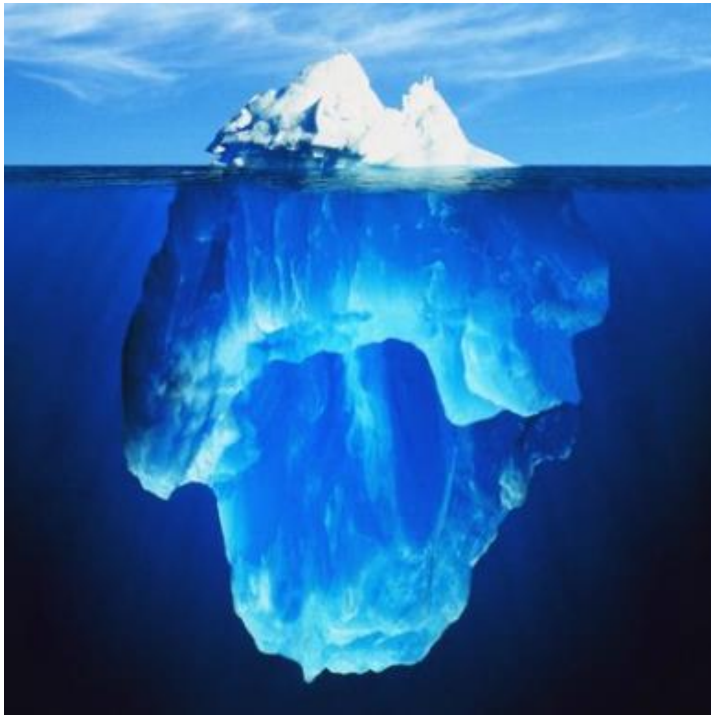
9 Product Support Recommendations

7 Product Design Recommendations

5 Product Test Recommendations

10 Management Recommendations

4 Key Systemic Factors



Key Insight –
Addressing the physical process and control is the tip of the iceberg

https://www.tokresource.org/tip-of-the-iceberg

Case Study 2: STPA Results

Analyzing just two UCA's generated:

16 Software, hardware and technical information requirements

10 Development process recommendations

Key Takeaway – STPA successfully generated serviceability requirements for a complex system in the conceptual design phase

https://www.tokresource.org/tip-of-the-iceberg

Terminology

STAMP Term	STAMP Definition	Proposed Service STAMP Term
Loss	A loss involves something of value to stakeholders. Losses may include any loss that is unacceptable to the stakeholders. (Leveson, 2011)	Loss
Accident	An accident is an unplanned and undesired loss event. (Leveson, 2011)	Loss Event
Hazard	A hazard is a system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to a loss. (Leveson & Thomas, 2018)	Hazard
Unsafe Control Action	An Unsafe Control Action (UCA) is a control action that, in a particular context and worst-case environment, will lead to a hazard. (Leveson & Thomas, 2018)	Unserviceable Control Action

Losses

Unplanned downtime due to inadequate serviceability (L-1)

Financial losses incurred through warranty costs (L-2)

Customer dissatisfied (L-3)

Key Takeaway – Leverage broad definition of a loss

A loss involves something of value to stakeholders. Losses may include any loss that is unacceptable to the stakeholders. (Leveson, 2011)

Hazard Examples

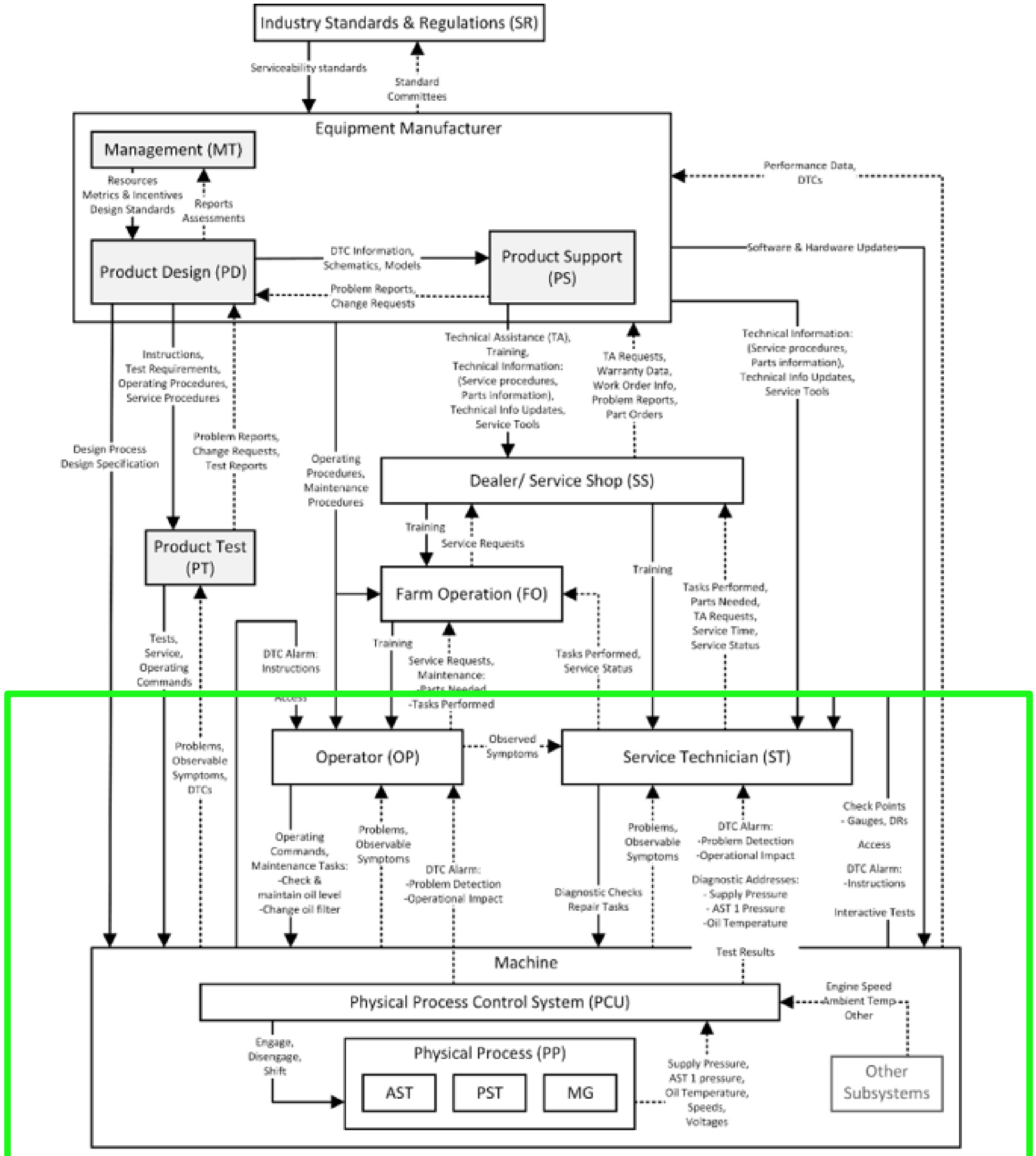
Operator takes the wrong action to mitigate the problem or ignores a service alarm (L-1, L-3)

Service technician does the wrong repair (L-1, L-2, L-3)

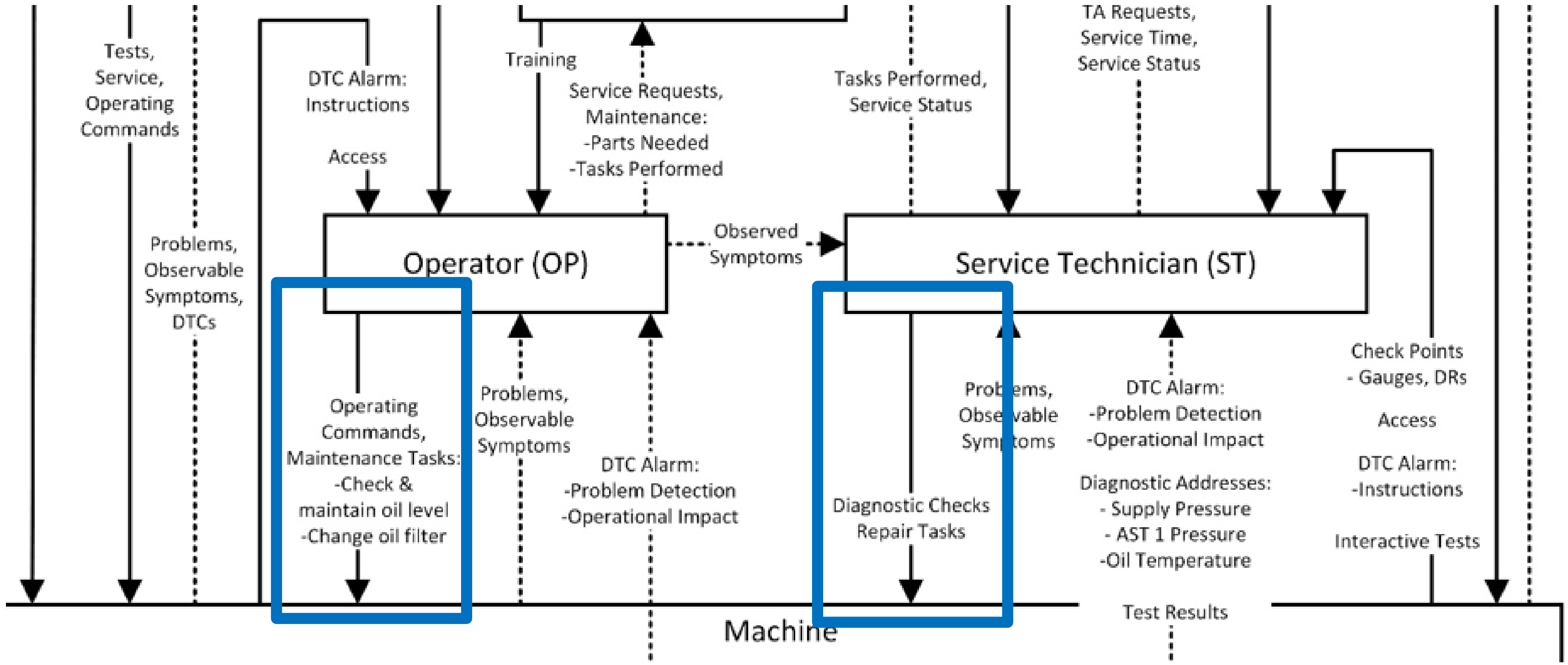
Machine falsely indicates a problem (L-1, L-2, L-3)

Repair & troubleshooting time exceeds <X> minutes (L-1, L-2, L-3)

https://www.centerforperformanceimprovement.com/blog/2018/6/12/top-5-ways-to-recruit-rockstar-automotive-technicians
https://jobs.autonation.com/



Industry Standards & Regulations (SR)
Serviceability standards
Standard Committees
Equipment Manufacturer
Management (MT)
Resources
Metrics & Incentives
Design Standards
Reports
Assessments
Product Design (PD)
DTC Information, Schematics, Models
Problem Reports, Change Requests
Product Support (PS)
Performance Data, DTCs
Software & Hardware Updates
Instructions, Test Requirements, Operating Procedures, Service Procedures
Problem Reports, Change Requests, Test Reports
Design Process
Design Specification
Operating Procedures, Maintenance Procedures
Technical Assistance (TA), Training, Technical Information: (Service procedures, Parts information), Technical Info Updates, Service Tools
TA Requests, Warranty Data, Work Order Info, Problem Reports, Part Orders
Technical Information: (Service procedures, Parts information), Technical Info Updates, Service Tools
Dealer/ Service Shop (SS)
Training
Service Requests
Product Test (PT)
Farm Operation (FO)
Training
Tasks Performed, Parts Needed, TA Requests, Service Time, Service Status
Tests, Service, Operating Commands
DTC Alarm: Instructions
Access
Training
Service Requests, Maintenance: -Parts Needed -Tasks Performed
Tasks Performed, Service Status
Problems, Observable Symptoms, DTCs
Operator (OP)
Observed Symptoms
Service Technician (ST)
Operating Commands, Maintenance Tasks: -Check & maintain oil level -Change oil filter
Problems, Observable Symptoms
DTC Alarm: -Problem Detection -Operational Impact
Diagnostic Checks Repair Tasks
Problems, Observable Symptoms
DTC Alarm: -Problem Detection -Operational Impact
Diagnostic Addresses: - Supply Pressure - AST 1 Pressure -Oil Temperature
Check Points - Gauges, DRs
Access
DTC Alarm: -Instructions
Interactive Tests
Test Results
Machine
Physical Process Control System (PCU)
Engine Speed Ambient Temp Other
Engage, Disengage, Shift
Physical Process (PP)
AST
PST
MG
Supply Pressure, AST 1 pressure, Oil Temperature, Speeds, Voltages
Other Subsystems



Key Takeaway – Service tasks are the controls

Table 3: Service Responsibilities - Physical Process Control System (PCU)

General Responsibilities	Specific
Monitor conditions	
Detect and decide when problems exist that require service action	X
Protect the machine from damage when problems are detected	X
Isolate problems and determine the repair required	X
Alarm the operator and technician to problems and communicate control action needed	X
Provide automatic troubleshooting aids: display relevant values, provide diagnostic tests and calibrations	X
Detect and decide when problems are fixed	

Table 4: Service Responsibilities – Operator (OP)

General Responsibilities	Specific
Operate the equipment in a way that does not lead to machine damage	
Monitor equipment condition and alarms	
Maintain the equipment: Applicable to loss event listed below	
Check and maintain hydraulic oil level	X
Change oil filter (when restricted or per regular interval?)	
Respond to problems that occur	
Follow DTC and operator manual instructions	X
Request service support	
Communicate observed symptoms to service technician	

Key Takeaway – Generated reusable general responsibilities and specific to the loss event. Reused in STPA case study

Table 12: Service Responsibilities - Operator (OP)

ID	Responsibilities	Feedback Needed
OP.R.1	Operate the equipment in a way that does not lead to machine damage or machine unavailability	TI DTC alarms, other system DTC alarms, TI disabled status, machine operating conditions, visual monitoring
OP.R.1.1	Manually control the function because TI is disabled	TI disabled status (if not observable without an indicator, machine must provide active feedback), visual monitoring
OP.R.2	Maintain the equipment	Maintenance required indicator
OP.R.2.1	Clean TI sensors	Sensor dirty status (if not observable from the operator seat), visual inspection

Key Takeaway – Some design requirements become apparent even before generating UCAs.

UCA Examples

PCU Control Action: Provide “replace component” code

- **UCA:** Physical process control unit (PCU) provides “replace component” code when component does not need replacement (H-1, H-2)

Technician Control Action: Replace component

- **UCA:** Service technician replaces component when it does not need replacement (H-2, H-6)

https://www.deere.com/en/our-company/john-deere-careers/dealer-technician-training/military-career-skills-program/

Conclusions

Successfully demonstrated STAMP applied to serviceability

- Same STPA and CAST steps
- Leverage broad definition of a loss
- Incremental process guides a service-friendly design

Generated hardware, software, and service instructions requirements simultaneously

Safety and Serviceability Alignment

STAMP elements:

- Reuse higher levels of control structure
- Different lower levels of control structure
- Different hazards and UCAs

Design considerations:

- Operator's responsibility to monitor alarms

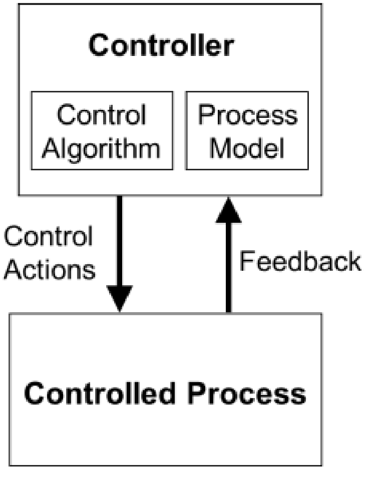
Other Insights

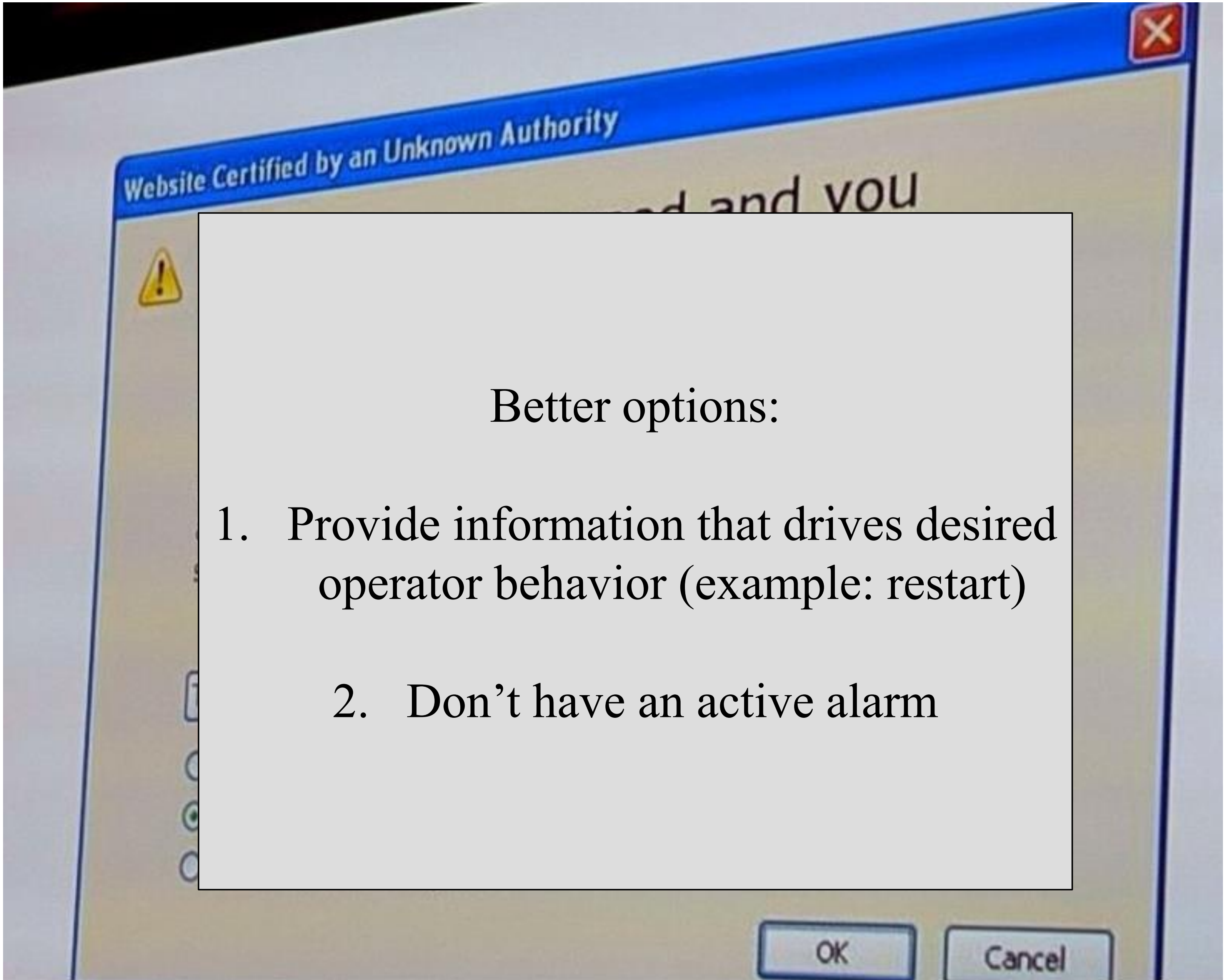
Reliability $\neq$ Machine Availability

Other Insights

Use service information to <u>drive desired human behavior</u>

vs. identify a "root cause"





Better options:

1. Provide information that drives desired operator behavior (example: restart)

2. Don't have an active alarm

Q&A

References

Ball, A. J. (2015). *Identification of Leading Indicators for Producibility Risk in Early-Stage Aerospace Product Development*. Massachusetts Institute of Technology.

Goerges, S. L. (2013). *System theoretic approach for determining causal factors of quality loss in complex system design* (Massachusetts Institute of Technology). https://doi.org/10.1115/DETC201434156

Leveson, N. G. (2011). *Engineering a Safer World: Systems Thinking Applied to Safety*. MIT Press.

Leveson, N. G., & Thomas, J. P. (2018). *STPA Handbook*. Retrieved from http://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf

Montes, D. R. (2016). *Using STPA to Inform Developmental Product Testing*.

Young, W., & Leveson, N. (2013). Systems thinking for safety and security. *Proceedings of the 29th Annual Computer Security Applications Conference*, 1–8. https://doi.org/10.1145/2523649.2530277