A Systems Thinking Approach to Eliciting Cybersecurity Requirements for an Electric Snowmobile

Martin “Trae” Span

Dr. Jeremy Daily

Colorado State University

September 30, 2022

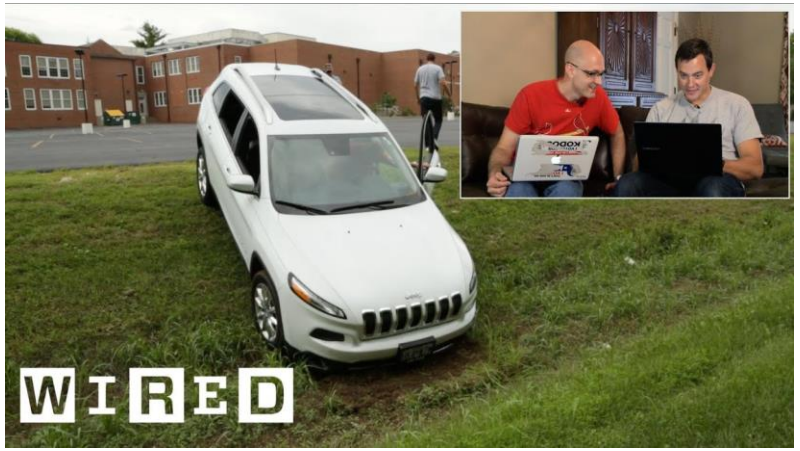
2022 INCOSE Western States Regional Conference – Golden, CO

Overview

- Problem Introduction
- Electric Snowmobile Example
- Proposed Value Added
- Future Work
- Questions

Problem Introduction

- Shift from Mechanical to Software based functionality [1]
- Cyber Physical Systems – Vehicles, Airplanes, Weapons Systems Vulnerable to Cyber Attacks: [2], [3], [4], [5]
- Acknowledged need to improve Cybersecurity by Design
  - ISACs for Vehicles [6], NDAA requirements for weapons systems [7]
- Need to Improve Requirements Elicitation Process for Security
  - Failure of checklist approach[8]– limits functionality and design trade space
- System Theoretic Process Analysis (STPA) [9], [10], [11]
  - Top-Down Systems Approach
  - Hazard Analysis technique to facilitate requirements for safe and secure complex system design



GAO 2021 Report on Weapon System Cybersecurity

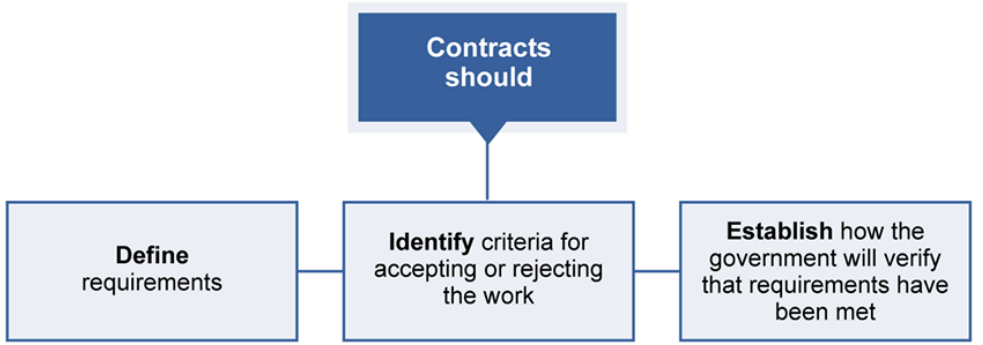
- Contracting for cybersecurity **requirements** is key.
- DOD guidance states that these **requirements** should be treated like other types of system **requirements**
- Specifically, cybersecurity **requirements** should be defined in acquisition program contracts, and criteria should be established for accepting or rejecting the work and for how the government will verify that **requirements** have been met.
- GAO found examples of program contracts omitting cybersecurity **requirements**, acceptance criteria, or verification processes. For example, GAO found that contracts for three of the five programs did not include any cybersecurity **requirements** when they were awarded.
- A senior DOD official said standardizing cybersecurity **requirements** is difficult and the department needs to better communicate cybersecurity **requirements** and **systems engineering** to the users that will decide whether or not a cybersecurity risk is acceptable.

What GAO Found

Since GAO's 2018 report, the Department of Defense (DOD) has taken action to make its network of high-tech weapon systems less vulnerable to cyberattacks. DOD and military service officials highlighted areas of progress, including increased access to expertise, enhanced cyber testing, and additional guidance. For example, GAO found that selected acquisition programs have conducted, or planned to conduct, more cybersecurity testing during development than past acquisition programs. It is important that DOD sustain its efforts as it works to improve weapon systems cybersecurity.

Contracting for cybersecurity requirements is key. DOD guidance states that these requirements should be treated like other types of system requirements and, more simply, "if it is not in the contract, do not expect to get it." Specifically, cybersecurity requirements should be defined in acquisition program contracts, and criteria should be established for accepting or rejecting the work and for how the government will verify that requirements have been met. However, GAO found examples of program contracts omitting cybersecurity requirements, acceptance criteria, or verification processes. For example, GAO found that contracts for three of the five programs did not include any cybersecurity requirements when they were awarded. A senior DOD official said standardizing cybersecurity requirements is difficult and the department needs to better communicate cybersecurity requirements and systems engineering to the users that will decide whether or not a cybersecurity risk is acceptable.

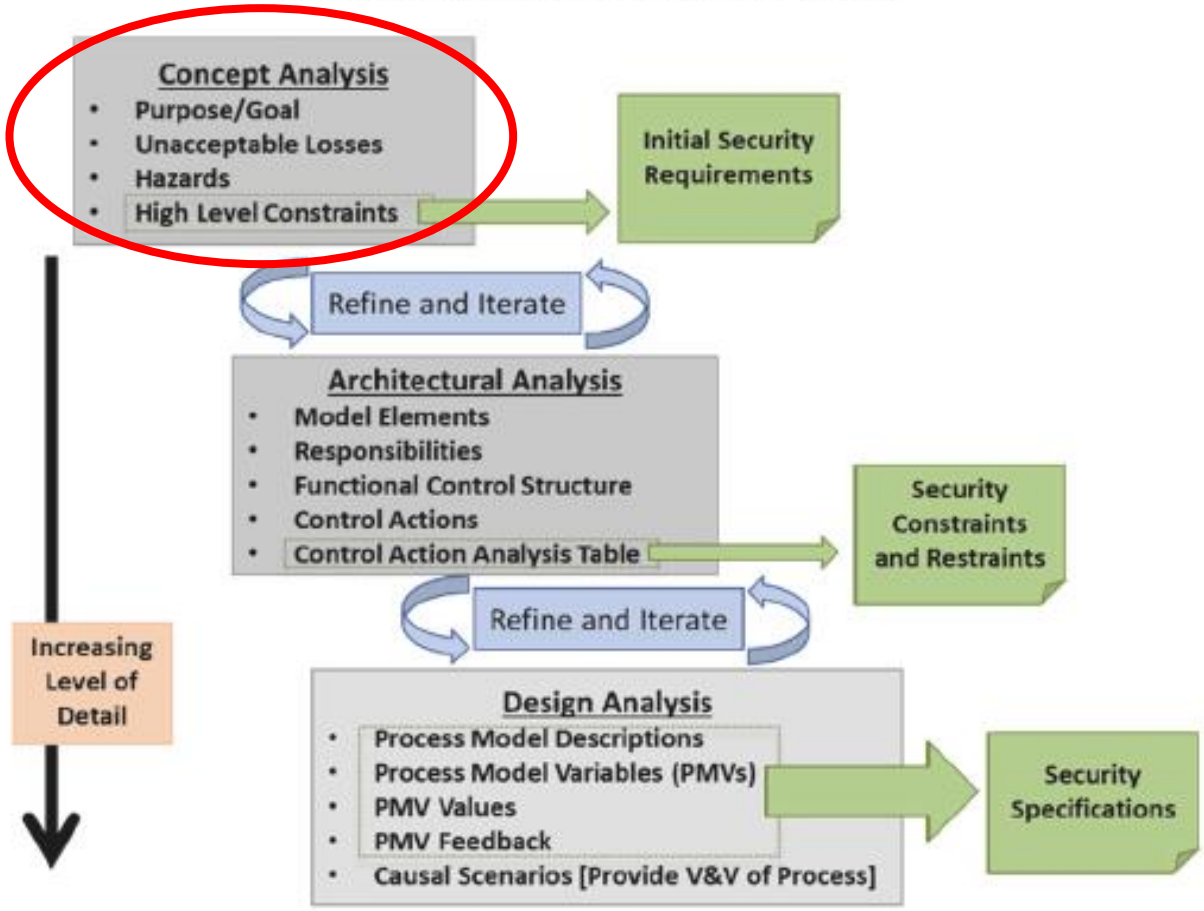
Incorporating Cybersecurity in Contracts



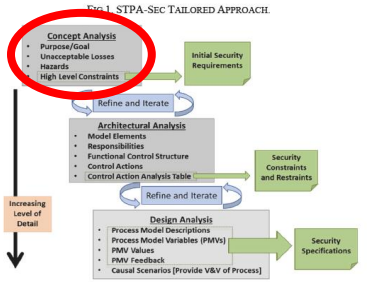
Source: GAO analysis of DOD information. | GAO-21-179

Concept Analysis

FIG 1. STPA-SEC TAILORED APPROACH.



Concept Analysis



A system to convey people and their gear across snow covered mountainous terrain

by means of charging, maneuvering, transporting, navigating

in order to Provide enjoyment and access to mountainous snow covered terrain

Can Snowmobiling Really Go Electric?

The beloved winter pastime has long been a massive polluter. Canadian startup Taiga Motors set out to transform the industry into something more environmentally friendly—and the big manufacturers are getting onboard.

Photo Credit: https://www.outsideonline.com/outdoor-adventure/snow-sports/taiga-motors-electric-snowmobile/

INCOSE | WSRC Western States Regional Conference

Loss/Hazards Mapping

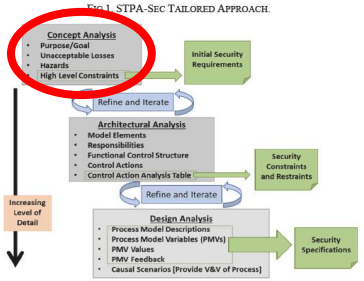
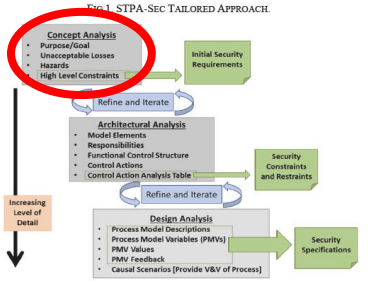


Photo Credit: Trae Span Original ☺

		Losses	
		L1: Loss of reputation/trust with stakeholders	**L2: Serious injury or Loss of life**
Hazards	**H1: Lack of range or controls displaying limited range**	**X**	**X**
	H2: Significant power loss	**X**	
	H3: Loss of navigation accuracy	**X**	**X**
	H4: Other capability degradation	**X**	**X**
	H5: Slow or Inaccurate Charging	**X**	

INCOSE | WSRC Western States Regional Conference

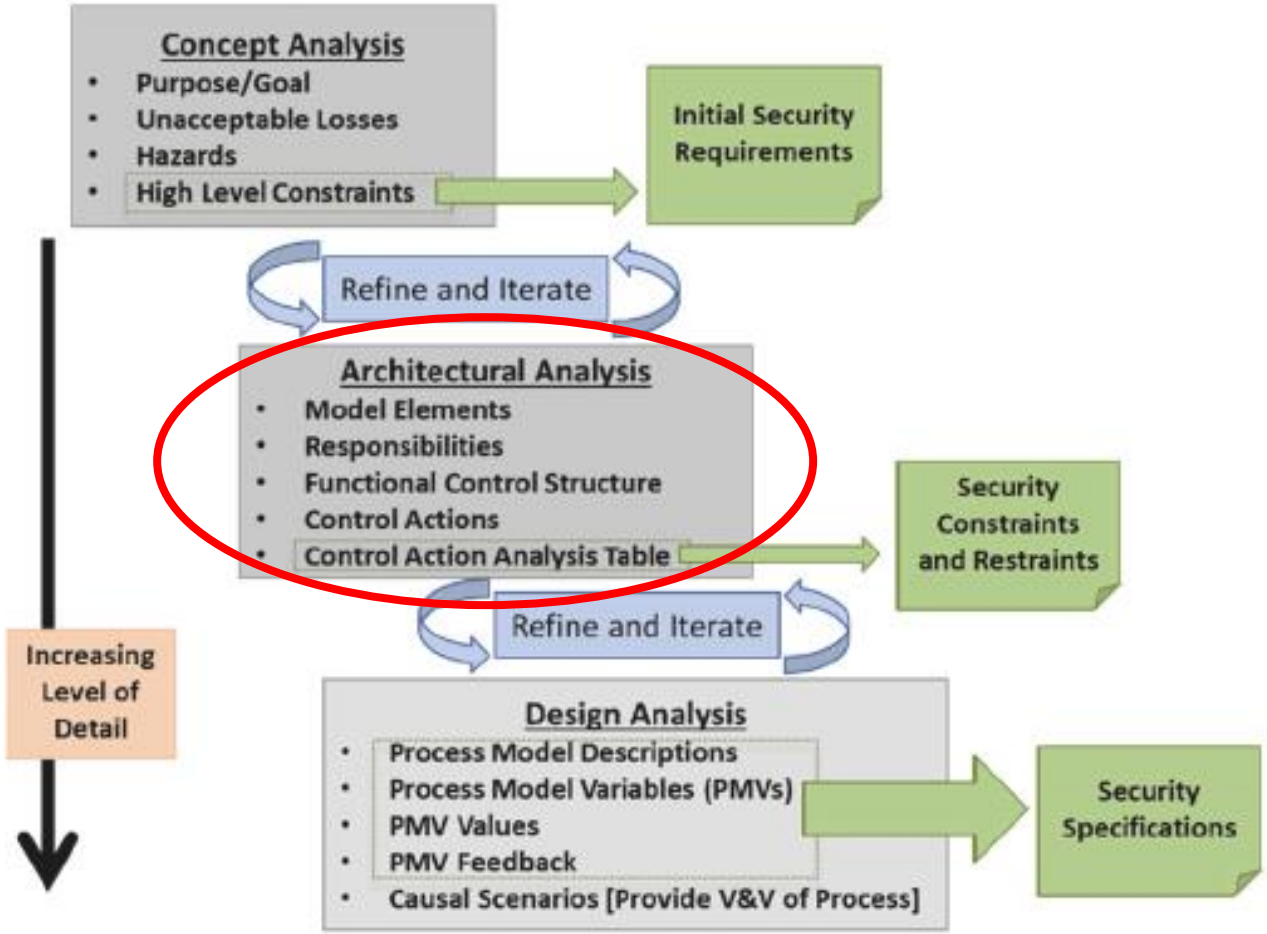
Initial Requirements (Constraints)



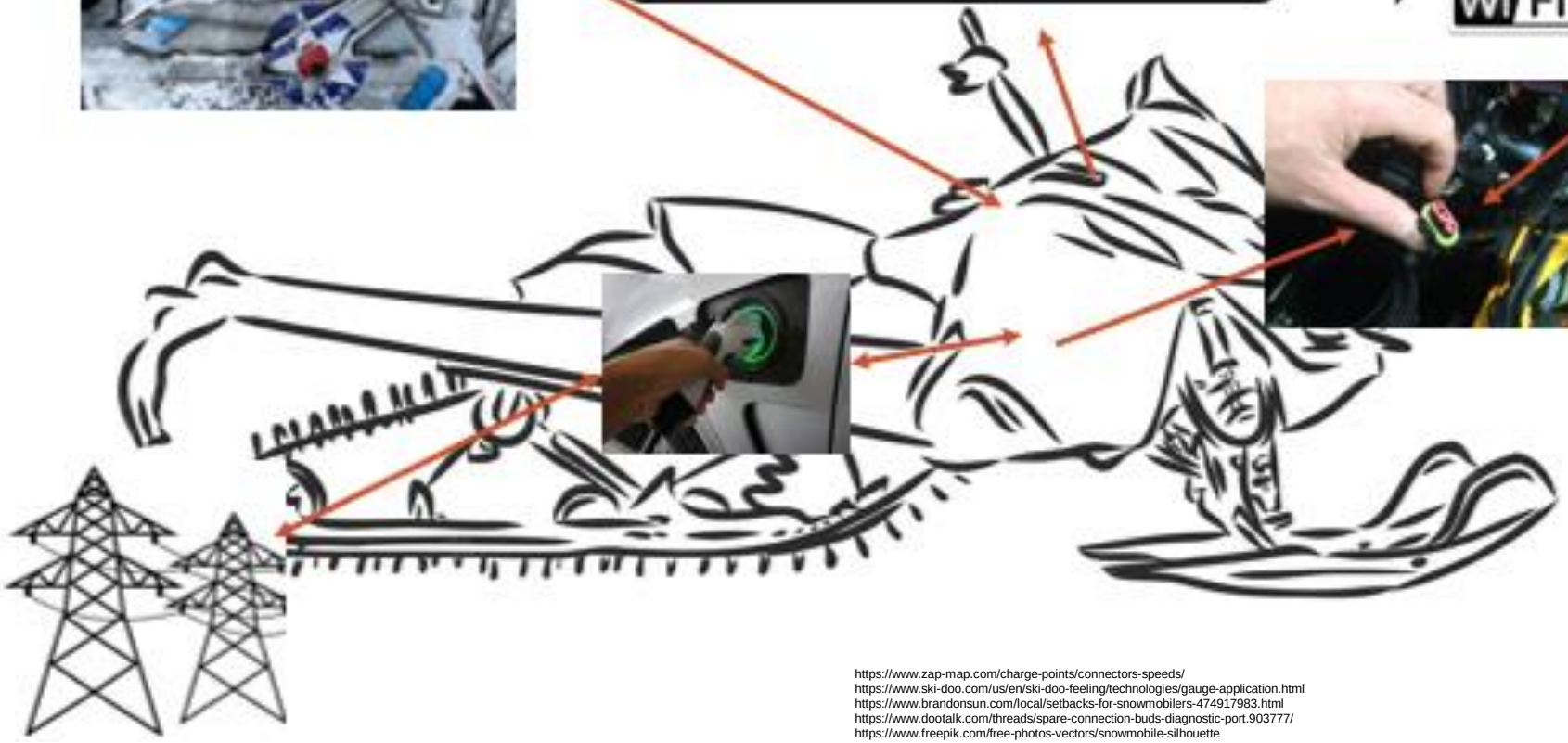
Hazards	Constraints
Lack of range or controls displaying limited range	HC-1.1 The system shall have redundant measure of computing range to display accurate and adjusted remaining range to the rider HC-1.2 The system shall conduct self tests on battery capacity and set a warning light when capacity or range calculations are below a minimum threshold
Significant power loss	HC-2.1 The system shall incorporate robust tamper and security protections to critical components and software for the drivetrain. HC-2.2 The system shall conduct real time status monitoring and set an indicator light if and when performance parameters exceed certain limits indicating a potential failure mode. HC-2.3 Key system performance metrics must be established and tested for the robustness of indicator lights.
Loss of navigation accuracy	HC-3.1 The system shall incorporate multiple sources of navigation aides and set an error message when not aligned. –E.G. Include a compass and barometric pressure sensor for altitude and heading and when over X Degrees or X ft off from GPS readings set an error message for degraded GPS navigation.
Other capability degradation	HC-4.1 The system shall identify safety critical functionality and prioritze power and onboard resources to maintaining that capability in the face of degradation events
Slow or Inaccurate Charging	HC-5.1 The system shall comply with applicable SAE Standards for electric vehicle charging HC- 5.2 The system shall monitor charging and display a fault if a charging error occurs

Architectural Analysis

FIG 1. STPA-SEC TAILORED APPROACH.

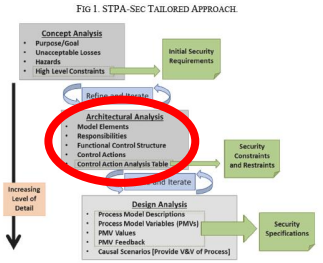


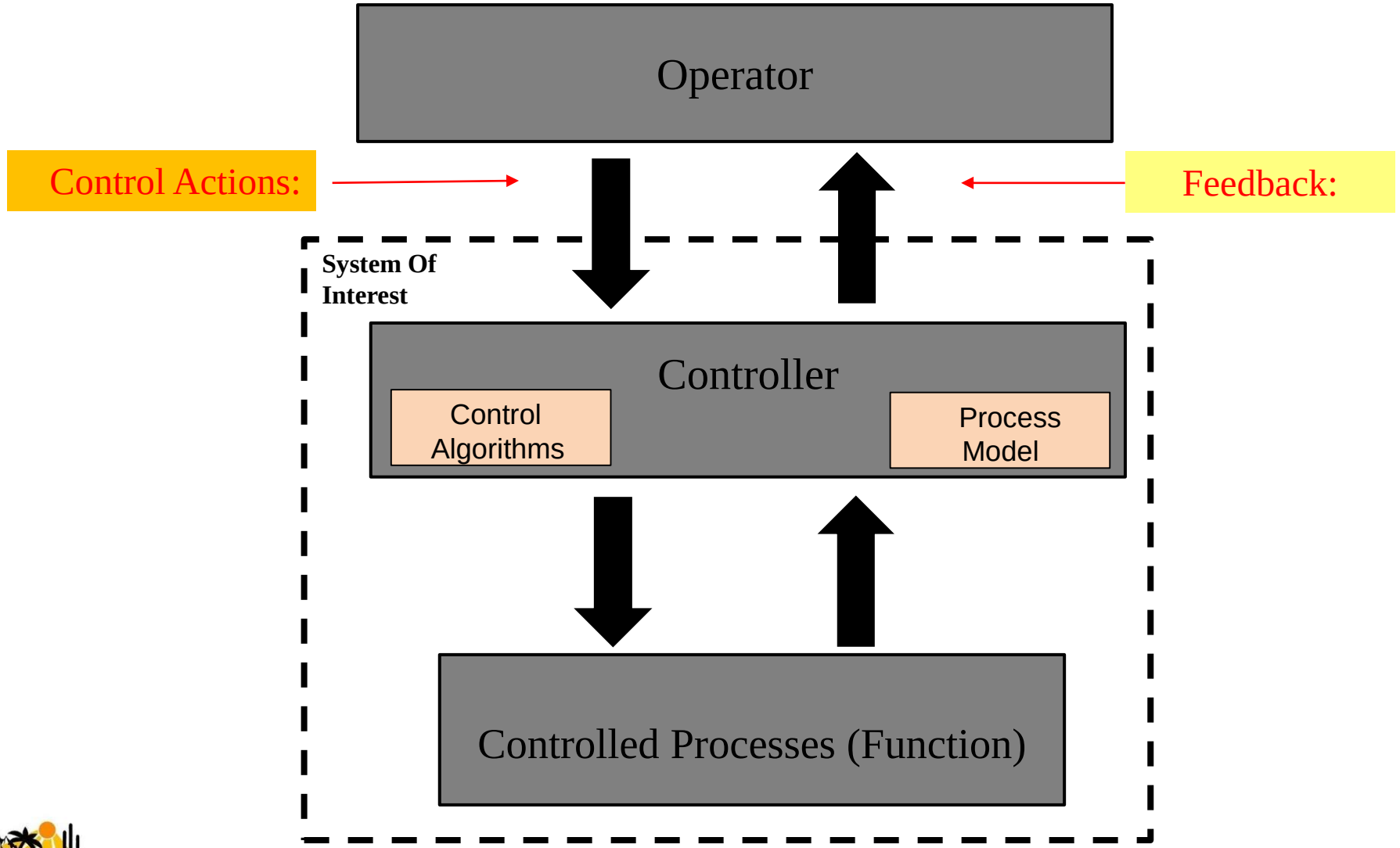
Simplified System Architecture Overview



https://www.zap-map.com/charge-points/connectors-speeds/
https://www.ski-doo.com/us/en/ski-doo-feeling/technologies/gauge-application.html
https://www.brandonsun.com/local/setbacks-for-snowmobilers-474917983.html
https://www.dootalk.com/threads/spare-connection-buds-diagnostic-port.903777/
https://www.freepik.com/free-photos-vectors/snowmobile-silhouette

Functional Control Structures (FCS)





Functional Viewpoint FCS

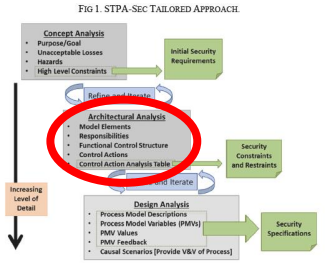
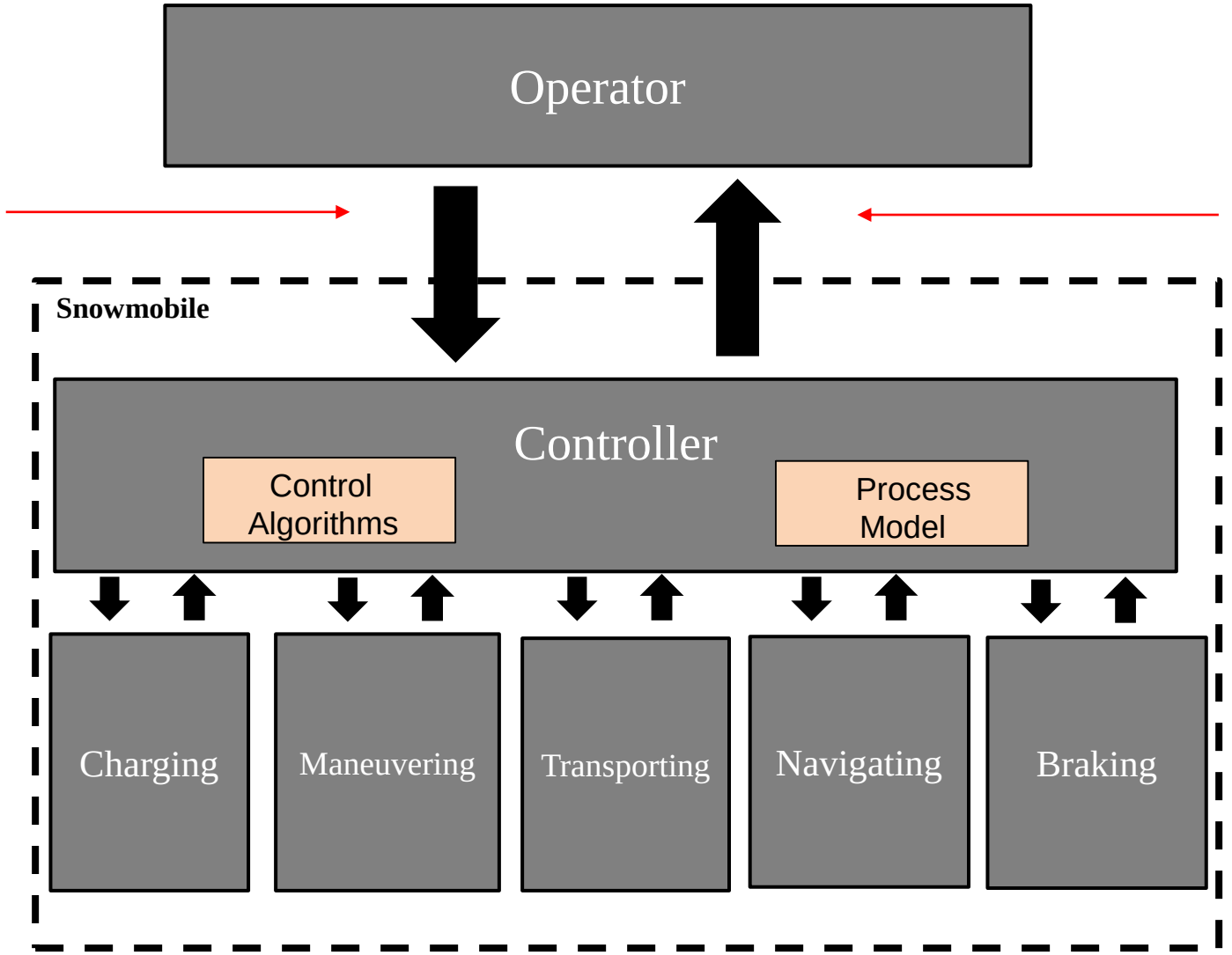


FIG 1. STPA-SEC TAILORED APPROACH

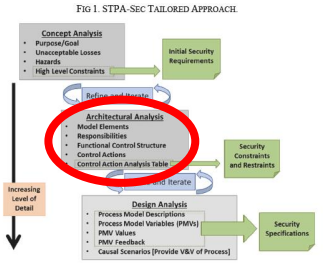
Control Actions:
Accelerate
Begin Charging
Search Destination
Route Navigation
Ect.



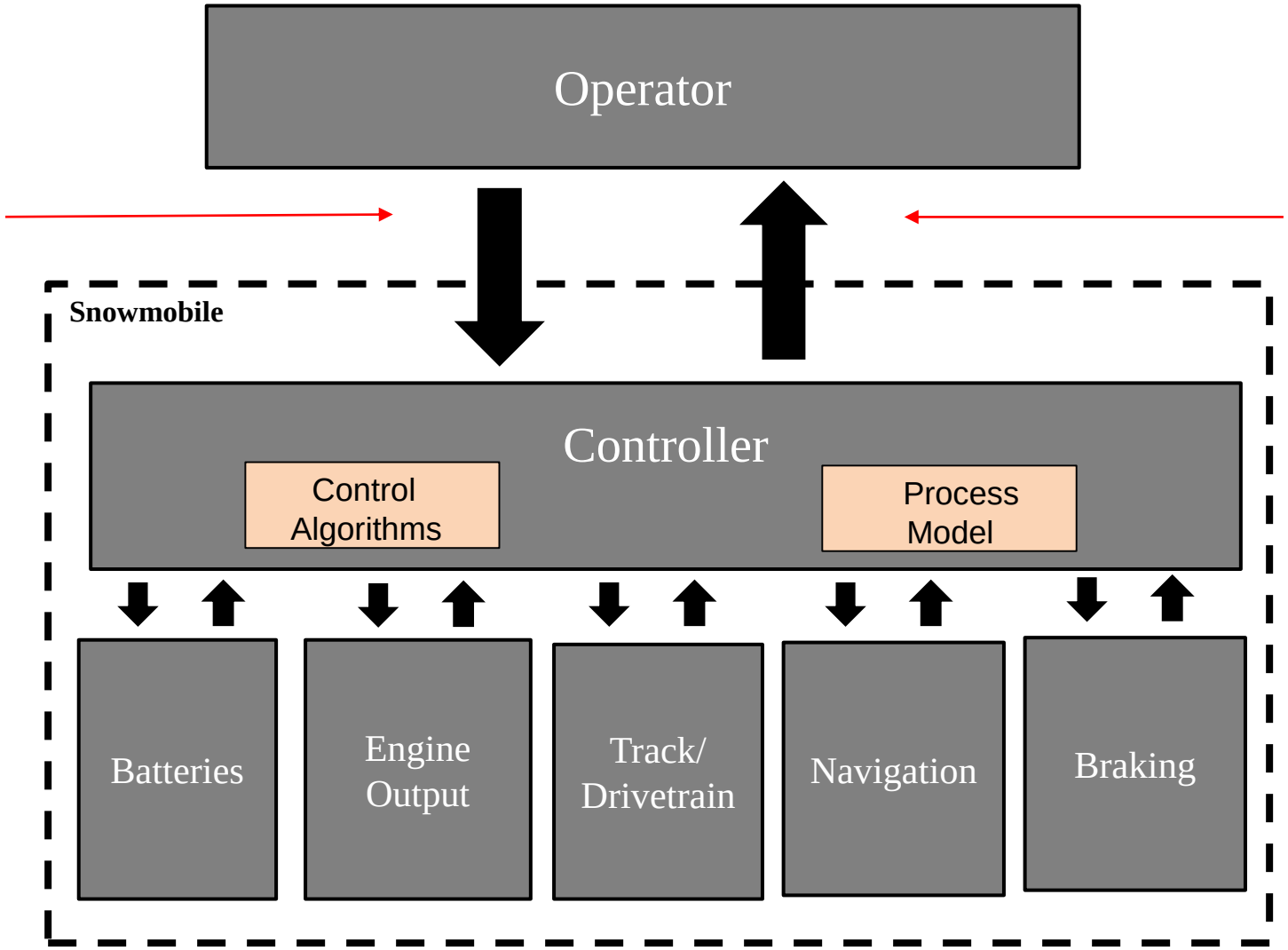
Feedback:
Track Speed
RPM
Battery Percentage
Estimated Range
Warning Lights
Current Position
Distance to Waypoint
Etc.

INCOSE | WSRC Western States Regional Conference

Physical Viewpoint FCS



Control Actions:
Accelerate
Charge
Search Destination
Route Navigation
Brake
Ect.



Feedback:
Track Speed
RPM
Battery Percentage
Estimated Range
Warning Lights
Current Position
Distance to Waypoint
Etc.

INCOSE | WSRC Western States Regional Conference

Control Action Analysis

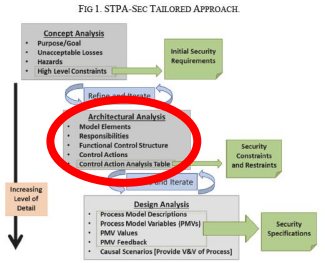


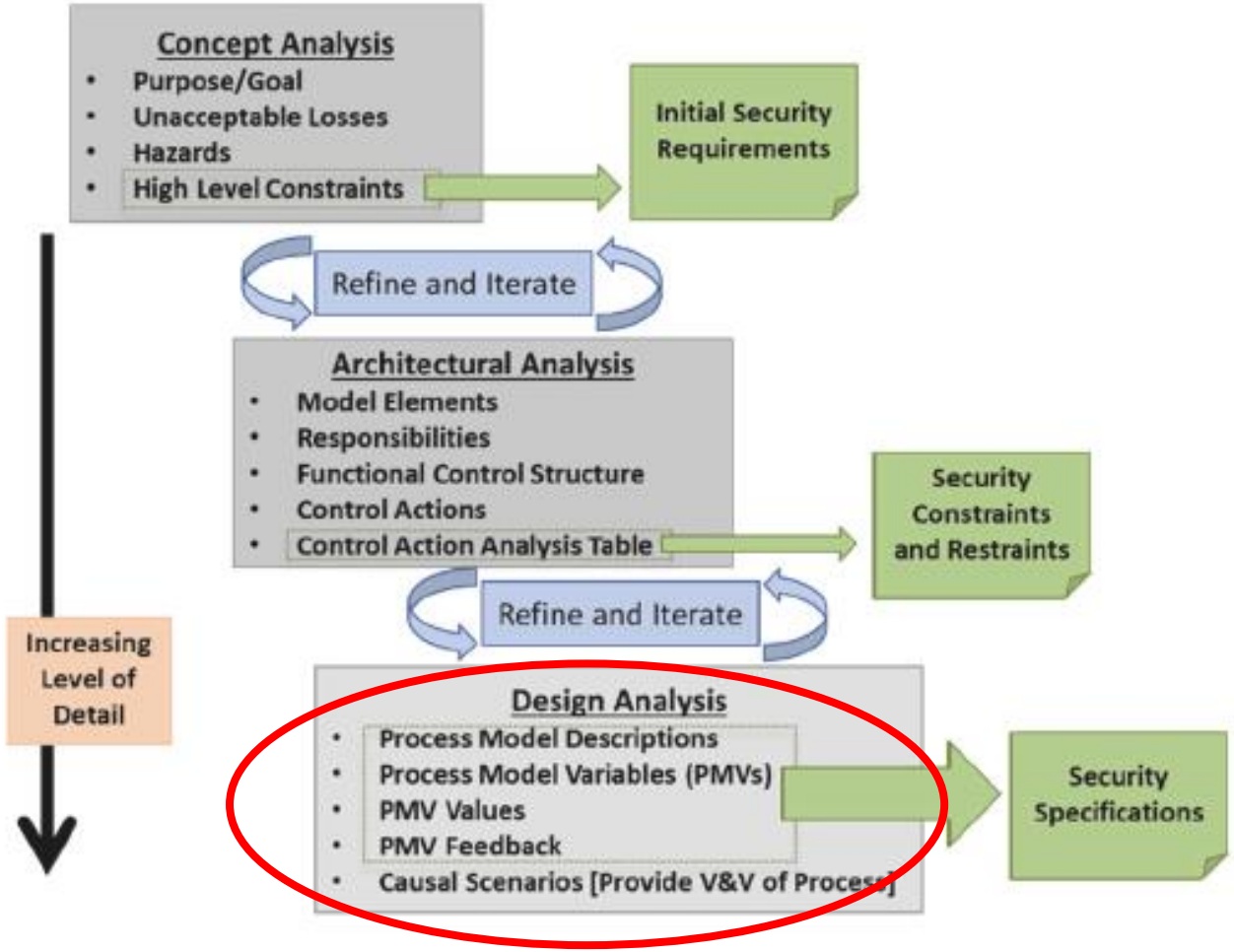
FIG 1. STPA-SEC TAILORED APPROACH

Hazards				
H1: Lack of range or controls displaying limited range	H2: Significant power loss	H3: Loss of navigation accuracy	H4: Other capability degradation	H5: Inaccurate or Slow Charging

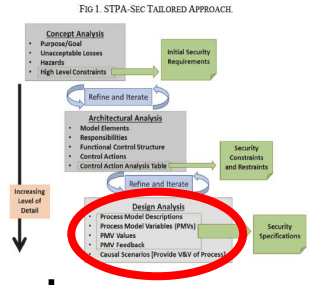
Control Action	Not providing causes Hazard	Providing Causes Hazard	Too Early/too late, wrong order	Stopping too soon/applying too long
Accelerate (1)	UCA-#1a : Not Providing Acceleration is Hazardous if operator requires it to traverse terrain safely [H2, H4]	UCA-#1b : Providing Acceleration is Hazardous if in conditions require precise navigation with deceleration [H2, H4]	UCA-#1c : Providing acceleration too late or too early is Hazardous if in a critical phase of terrain navigation [H2, H4]	UCA-#1d : Providing acceleration too short or too long is Hazardous if in a critical phase of terrain navigation [H2, H4]
Charge(2)	UCA-#2a : Not Providing charge is Hazardous if the user requires a charge to continue riding [H-1, H4]	UCA-#2b : Providing Charge is Hazardous if the batteries are in a condition where charging may cause damage (too hot or too cold) [H2, H4, H5]		UCA-#2c : Charging too long is hazardous if it damages the batteries [H2, H4, H5]
Search Destination (3)	UCA-#3a : Not Providing Search Destination is hazardous if the user requires navigation to return to a safe location [H-3]			
Route Navigation (4)	UCA-#4a : Not Providing Route Navigation is Hazardous if the user needs to adjust their path to avoid obstacles [H3]	UCA-#4b : Providing Route Navigation is Hazardous if display distracts the user in a critical maneuver in hazardous conditions [H3]	UCA-#4c : Not Providing Route Navigation in a timely manner is Hazardous if the user needs to adjust their path to avoid obstacles [H3]	
Brake (5)	UCA-#5a : Not Providing Brake is Hazardous if operator requires it to traverse terrain safely [H2, H4]	UCA-#5b : Providing braking is Hazardous if in conditions require precise navigation without braking [H2, H4]	UCA-#5c : Providing braking too late or too early is Hazardous if in a critical phase of terrain navigation [H2, H4]	UCA-#5d : Providing braking too short or too long is Hazardous if in a critical phase of terrain navigation [H2, H4]

Design Analysis

FIG 1. STPA-SEC TAILORED APPROACH.



Deriving Requirements



- Due to the extensive nature of complex systems, we adapted a streamlined methodology (STPA Handbook)

- Based on the CA Analysis:
  - System Constraints: Derive specific system behaviors that must be satisfied to prevent Unsafe CAs
  - Causal Scenarios: Describes the causal factors that may lead to the Unsafe CAs and to hazards.

N. Leveson and J. Thomas, "An STPA Primer," 9 September 2013. [Online]. Available: http://sunnyday.mit.edu/STPA-Primer-v0.pdf.
Reule, Ryyan T., et al. "STPA-Sec Analysis for DevSecOps Reference Design." INCOSE International Symposium. Vol. 31. No. 1. 2021.

Derived Requirements

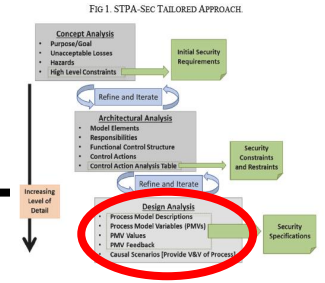
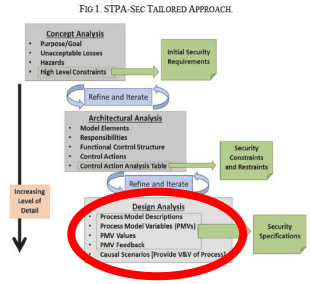


FIG 1. STPA-SEC TAILORED APPROACH

Control Action	Not providing causes hazard	Providing causes hazard	Too early/too late, wrong	Stopping too soon/applying too long
Accelerate (1)	UCA-#1a : Not Providing Acceleration is Hazardous if operator requires it to traverse terrain safely [H2, H4]	UCA-#1b : Providing Acceleration is Hazardous if in conditions require precise navigation with deceleration [H2, H4]	UCA-#1c : Providing acceleration too late or too early is Hazardous if in a critical phase of terrain navigation [H2, H4]	UCA-#1d : Providing acceleration too short or too long is Hazardous if in a critical phase of terrain navigation [H2, H4]

	Not providing causes hazard	Providing causes hazard	Too early/too late, wrong	Stopping too soon/applying too long
Constraints (Requirments)	SC-1.1 Acceleration performance must be continuously montiored and if degradation is detected a system warning light should be illuminated SC-1.2 If acceleration degradation exceeds a certain thresholds for severity or repetitiveness the system should be placed into a limp mode and notify the operator. SC-1.3 As a safety critical control action the acceleration command should be a part of safety critical security testing.	SC-1.4 More than one sensor should detect throttle position and disagreement between sensors should result in the lower value being selected	SC 1.4 applies	SC 1.4 applies

Causual Scenario



Control Action 1: Acceleration

Causal Scenario: A malicious actor gains access to the throttle control tables and inverts the percentage of acceleration commanded when the angle of attack exceeds 15 degrees. This security requirement added through STPA supports the necessity of an independent backup sensor for acceleration and code to default to the lower value

Acceleration Control Action

Unacceptable Losses

Loss of Reputation/Trust With Stakeholders

Serious Injury or Loss of Life

Hazazrds

H1: Lack of Range

H2: Significant Power Loss

H3: Loss of Navigation Accuracy

H4: Other Capability Degredation

Hazardous Control Action

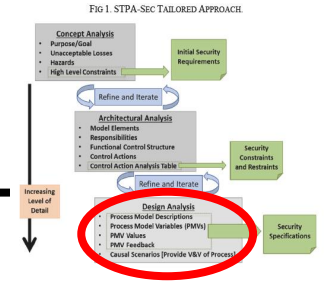
UCA-#1b : Providing Acceleration is Hazardous if in conditions require precise navigation with deceleration [H2, H4]

Security Requirement

SC-1.4
More than one sensor should detect throttle position and disagreement between sensors should result in the lower value being selected. An Engine warning light should be illuminated

INCOSE | WSRC Western States Regional Conference

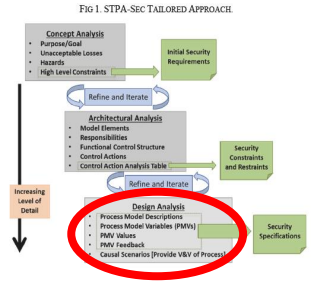
Derived Requirements



Control Action	Not providing causes hazard	Providing causes hazard	Too early/too late, wrong	Stopping too soon/applying too long
Brake (5)	UCA-#5a : Not Providing Brake is Hazardous if operator requires it to traverse terrain safely [H2, H4]	UCA-#5b : Providing braking is Hazardous if in conditions require precise navigation without braking [H2, H4]	UCA-#5c : Providing braking too late or too early is Hazardous if in a critical phase of terrain navigation [H2, H4]	UCA-#5d : Providing braking too short or too long is Hazardous if in a critical phase of terrain navigation [H2, H4]

	Not providing causes hazard	Providing causes hazard	Too early/too late, wrong	Stopping too soon/applying too long
Constraints (Requirments)	SC-5.1 Operator should be reminded to verify braking system operation SC-5.2 The braking system should be specified as a 'high reliability' component (specific metrics to be defined further into design)	SC-5.3 The braking system should not automatically engage on decelleration (no regenerative braking when letting off the throttle)	SC 5.2 applies	SC 5.4 The snowmobile should NOT autonomously decide when to apply or release the brakes.

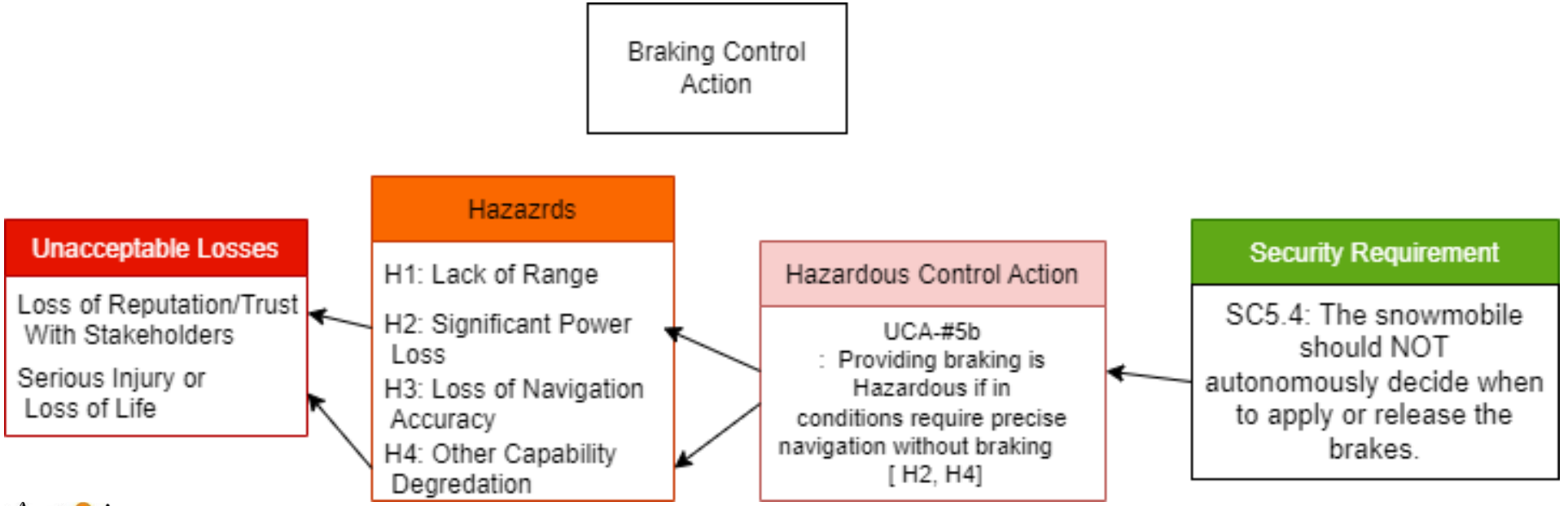
Causual Scenario



Control Action 5: Brake

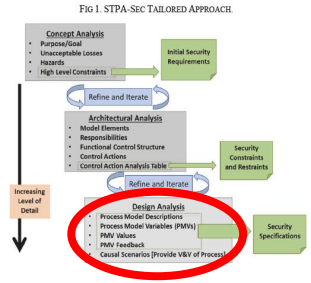
Causal Scenario: A software failure, either accidental or malicious, applies brakes when not commanded by the rider. This could easily harm the rider if done at high speeds.

This causal scenario supports a requirement to NOT include regenerative or software controlled braking. This analysis supports a requirement of mechanical only braking.

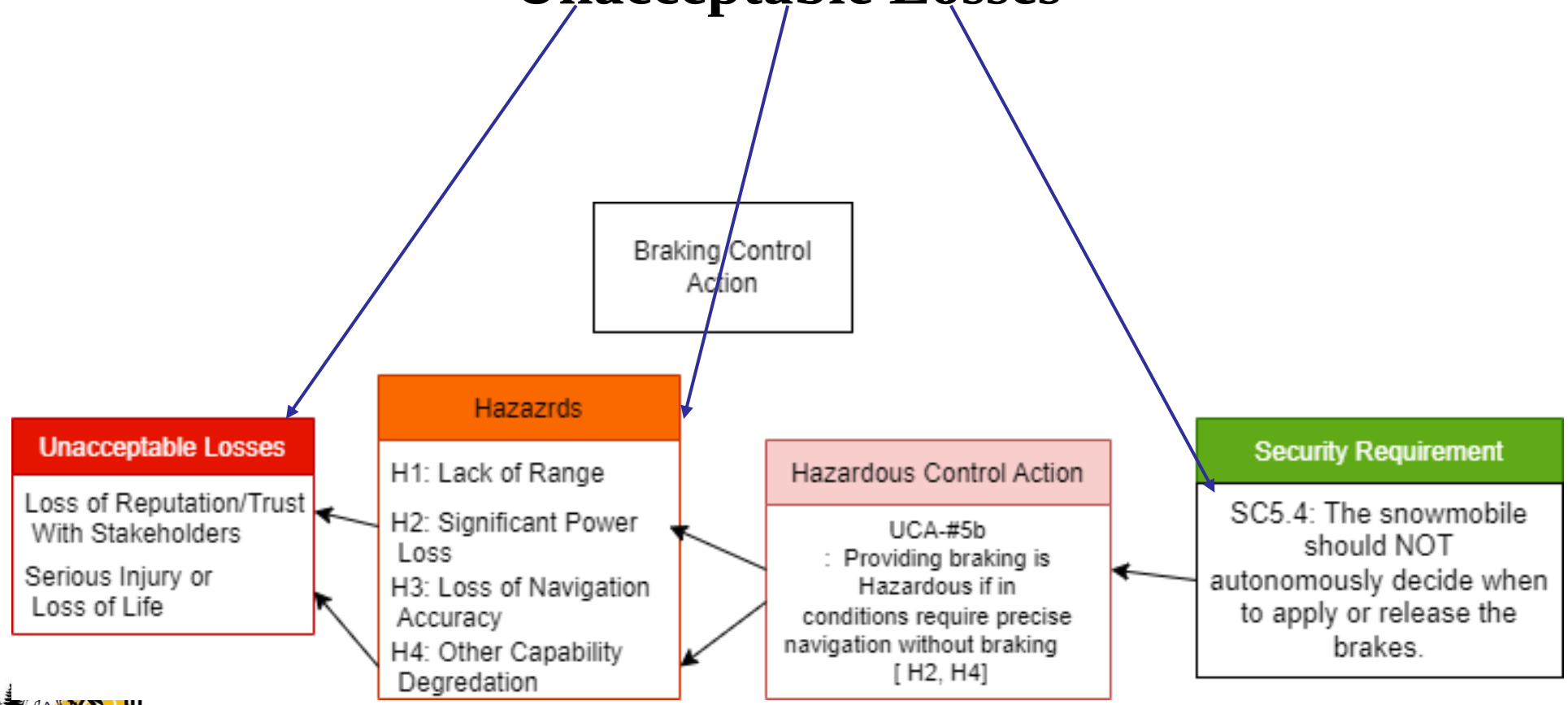


INCOSE | WSRC Western States Regional Conference

STPA-Sec Value Added



Traceability From Specific Security Requirements to System Level Unacceptable Losses



INCOSE | WSRC Western States Regional Conference

Future Work

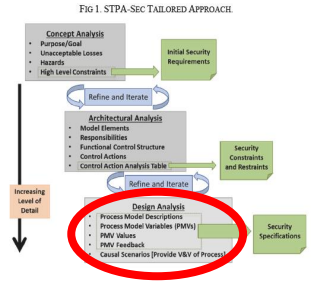


FIG 1. STPA-SEC TAILORED APPROACH

- Possible Extensions?
  - Add a Risk Priority Assessment approach to the cyber requirements?
- How do you integrate this with SysMl models?
- Can I use this approach for security policy elicitation?
- Show the impacts of performing this assessment at various levels of abstraction

Questions?

Simplified System Architecture Overview