Agenda for OSD/Army meeting on Cyber Resiliency Project

- 9:00am-9:30am – Overview of ongoing and potential UVA cyber attack resiliency projects - **Horowitz**
- 9:30am-10:30am – Army Project (RT-191) results – **Horowitz**
- 10:30am-11am – Silverfish Prototype Demonstration – **Sherburne**
- 11:15am-12:15am – Tool development project review (RT 172/196) – **Fleming**
- Lunch
- 1pm-1:30pm – Follow-on Army Project Possibilities (including potential static testing project) - **Horowitz**
- 1:30pm – Responses to Potential Interest from Dahlgren, TARDEC, DOT&E and NSA
- 2pm – End of meeting

Silverfish Prototype Overview & Demo

Tim Sherburne

13-Jun-2018

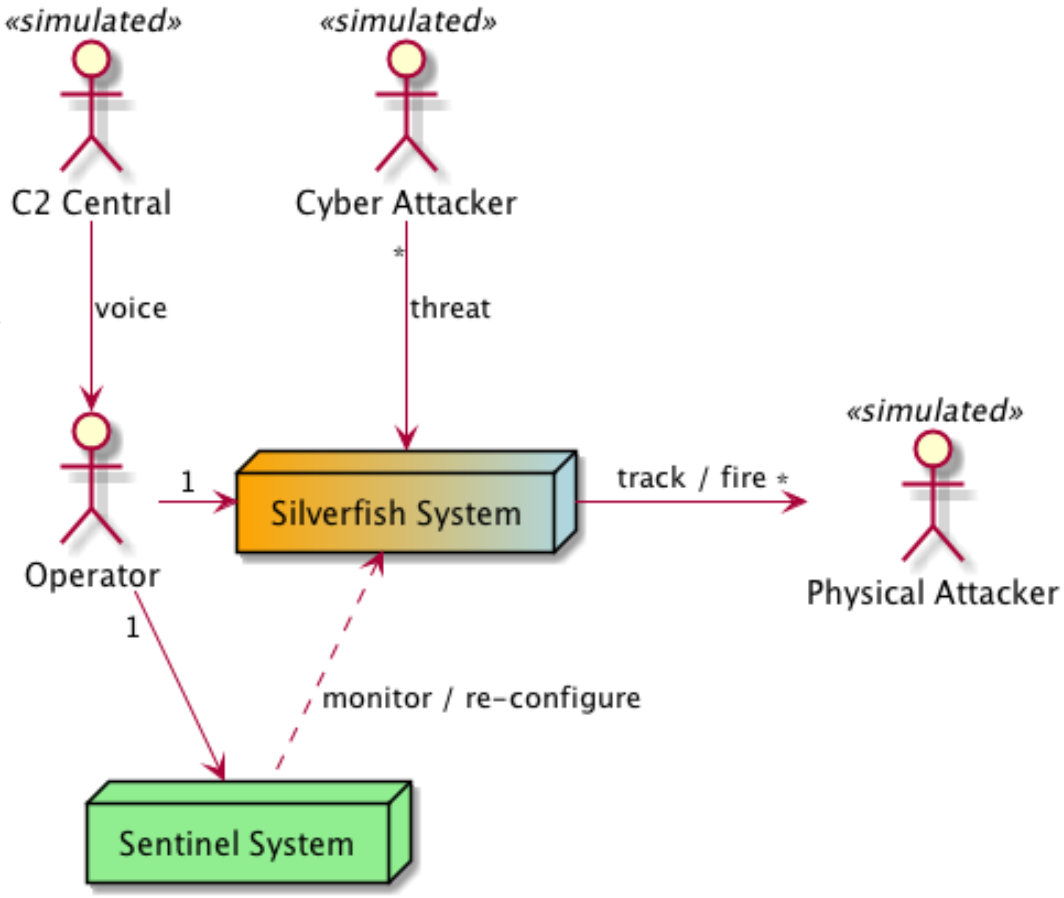
Topics

- Silverfish Requirements Review
- Prototype Architecture Overview
- UI Overview Demonstration
  - Fire Control Application
  - Situational Aware Application
- Cyber Attack / Resiliency – Use Case #1 Overview
- Cyber Attack / Resiliency – Demonstration
- What's Next?

Silverfish Context Diagram

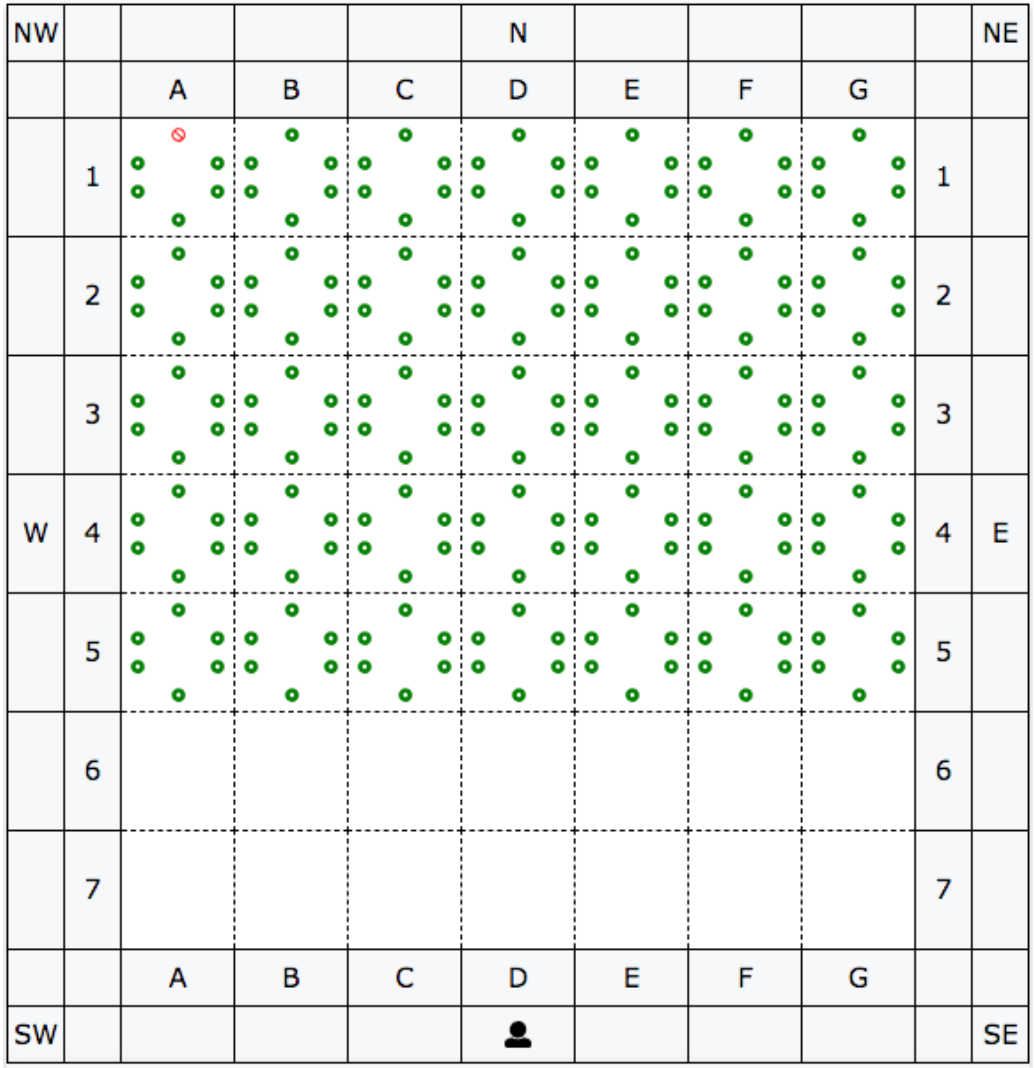
<u>Silverfish System:</u> ***Track*** and ***prevent*** adversarial vehicles (max speed 10 mph) or individuals (*physical attacker*) from trespassing into geographic areas that are close to strategically sensitive locations.

<u>Sentinel System:</u> Provide system resilience by ***monitoring*** to detect successful *cyber-attacks* and provide support for rapid ***reconfiguration*** of the attacked Silverfish system for continued operation with contained consequences.

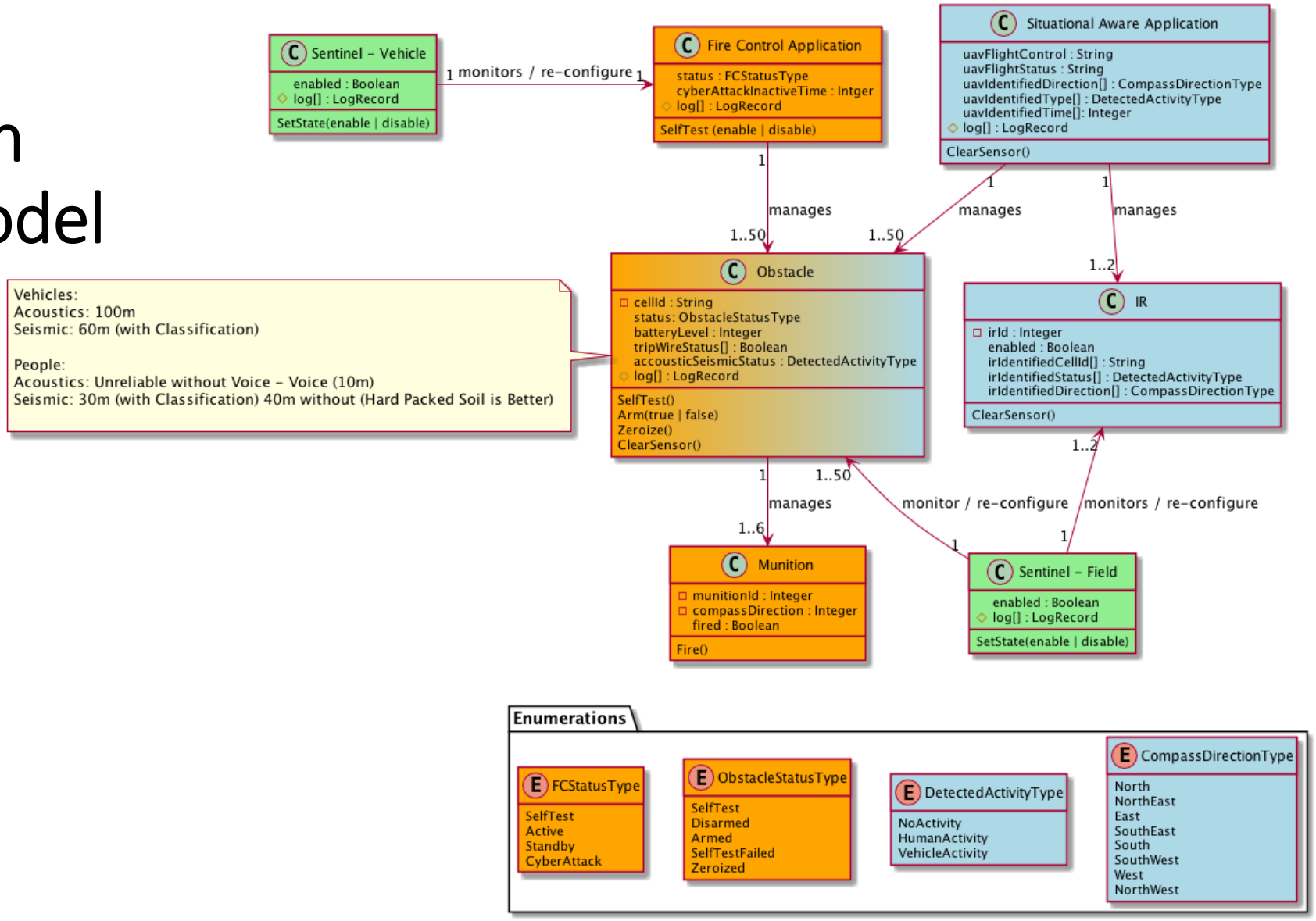


Silverfish Grid Layout

- <u>Prohibited Area:</u>
  - ~100 acres ≈ .16 sq. miles (.4 x .4)
- <u>Obstacle Deployment:</u>
  - ~50
  - 7x7 grid (A1-G7)
  - Aligned to Compass Coordinates
    - 🧍 is Operator Observation Point
- <u>Cell Grid:</u>
  - ≈ 300 ft. x 300 ft.
  - 6 Munitions per Cell (ready / fired state)
- <u>Vehicle Traversal:</u>
  - Max Speed = 10 mph ≈ 15 ft. / sec.
  - 20 seconds / grid
  - 2.3 minutes / protected area

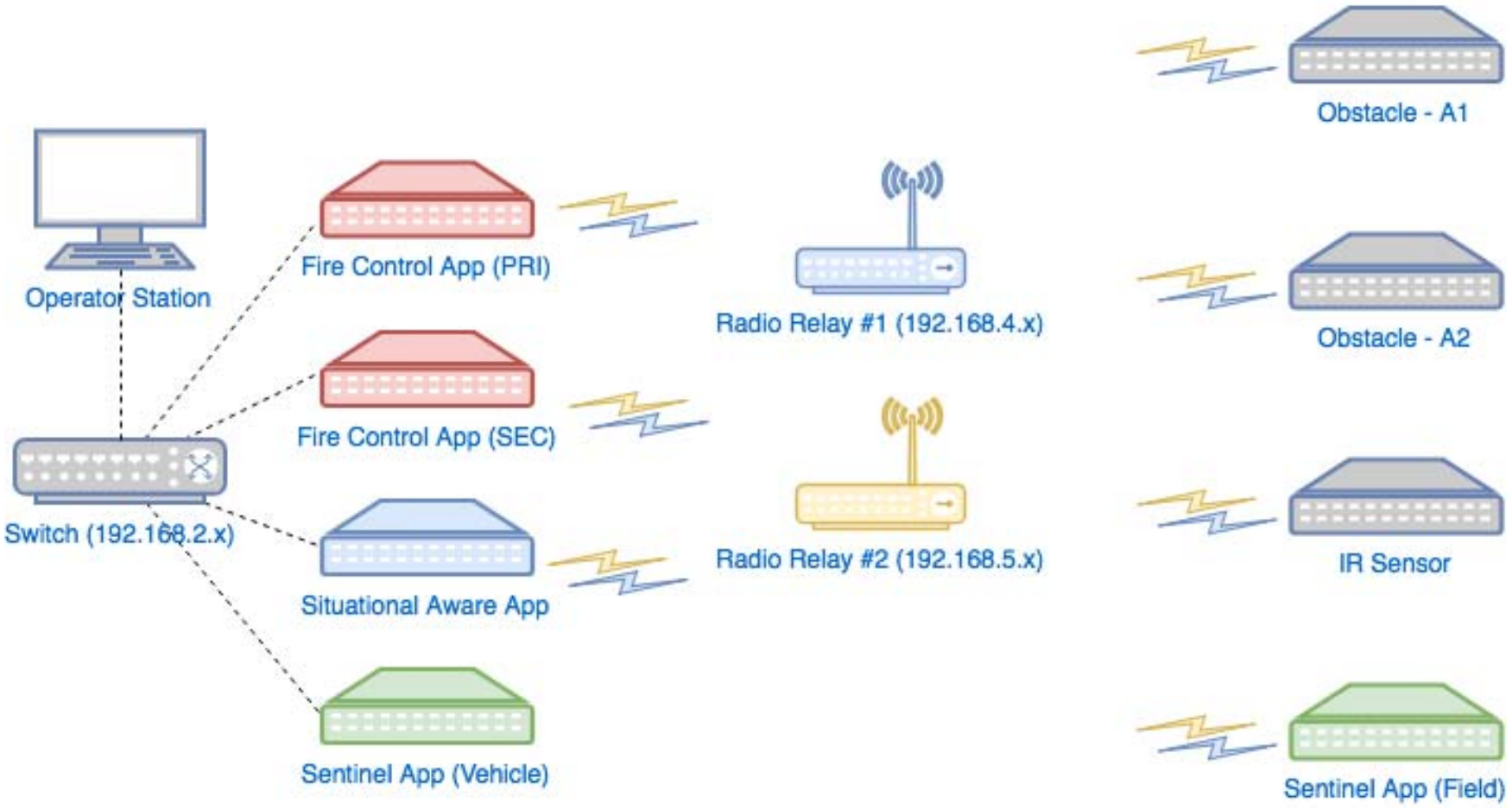


Silverfish Data Model

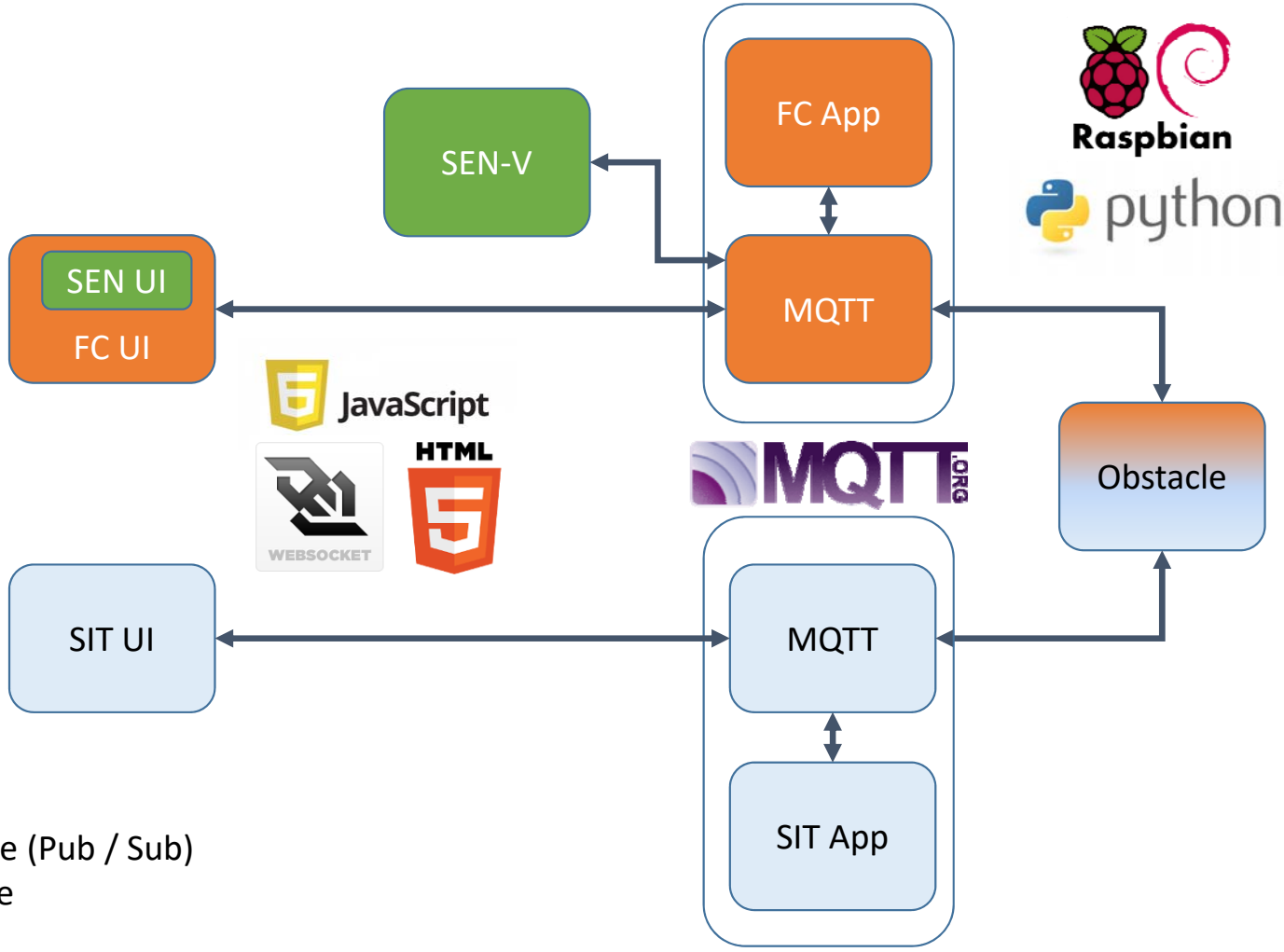


Prototype Architecture Overview

Silverfish Physical Architecture



Silverfish Software Architecture



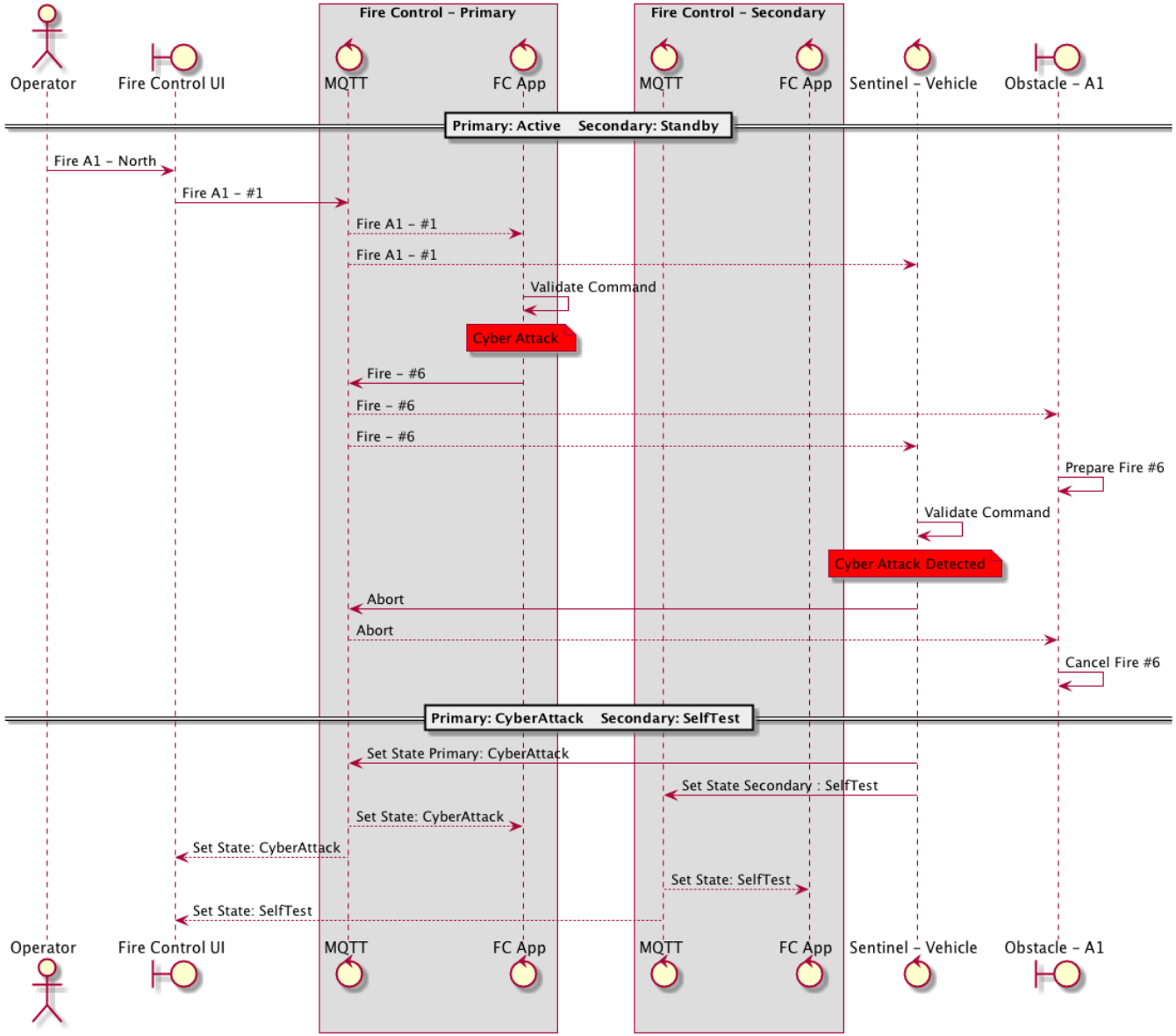
FC - Fire Control
MQTT – Message Queue (Pub / Sub)
SEN-V – Sentinel Vehicle
SIT – Situation Aware

UI Overview Demonstration

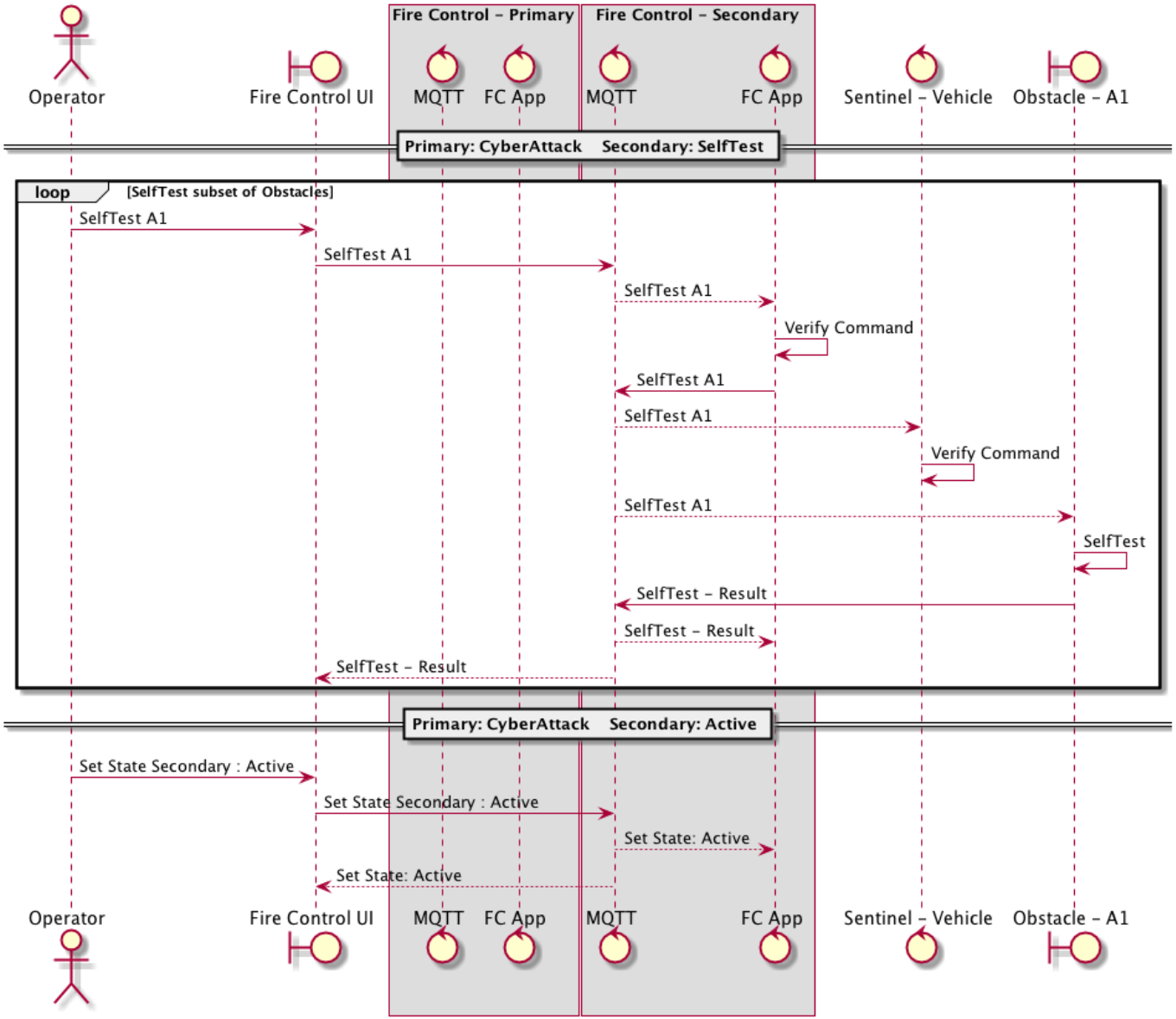
Silverfish Cyber Attack Use Case #1

Cyber Attack Use-case	Attack Target	Attack Method	Description	Detection Method / Corrective Action
1.1 Inappropriate Firing via Manipulated Operator Commands	Fire Control Application Software	Insider – SW Developer	During design and manufacture, a SW Developer introduces software to the Fire Control Application that redirects Operator fire commands, when deployed at a specific geographic location. With this Cyber-attack knowledge, a Physical attacker could gain access to a protected area. The Fire Control Application includes Primary and Secondary instances which are based on independent design and manufacture so as to minimize the likelihood of the same Cyber Attack affecting both.	*Design Pattern: Changing Control Input* Detection Method The Sentinel Application within the Vehicle monitors the Fire Control Application for consistency between Operator requested actions and the actions that will be delivered to the Obstacles via the Radio Relay Interface. Corrective Action The Sentinel detects the attack and takes the following actions: • The misfire is aborted. • The Primary Fire Control Application is taken out of service and put into a "CyberAttack" state. • The Secondary Fire Control Application is put into a "SelfTest" state. To gain confidence with the reconfigured system, the Operator takes the following actions: • Individually test one or munitions. • Multi-Select a group of munitions for test. • If and when confidence is restored, Activate the Resiliency Mode (disable the "Self Test" of the Secondary Fire Control Application) and continue operation.

UC #1 – Sequence Diagram – Part 1



UC #1 – Sequence Diagram – Part 2



Cyber Attack / Resiliency – Demonstration

What's Next

- Key Results / Insights to date:
  - To be published in Final Report:
    - Human Factors / System Design Tradeoffs
    - Sentinel Interfaces & Timing / System Design Tradeoffs
- Next Use Cases - Preview

Silverfish Cyber Attack Use Case #2

Cyber Attack Use-case	Attack Target	Attack Method	Description	Detection Method / Corrective Action
2.2 Prevent or corrupt transmission of situational awareness data	Radio Relay	External	During operation of the Silverfish network, a Cyber Attacker gains access to the Radio Relay network and injects false sensor report messages. The Silverfish network includes Primary and Secondary Radio Relay instances which are based on independent design and manufacture so as to minimize the likelihood of the same Cyber Attack affecting both.	*Design Pattern: Introspection* Detection Method The Sentinel Application within the Field monitors network traffic and maintains a profile of “normal” traffic loads based on current field state. Corrective Action The Sentinel detects a higher than normal level of sensor reporting activity based on the current Obstacle’s sensor state. The Sentinel disables the Primary Radio Relay network changing its state to “TamperDetected” thereby notifying the Operator of the Cyber Attack. The Sentinel attempts to activate the Secondary Radio Relay network by running a set of self-test actions. If the self-tests pass, the Sentinel Activates the Secondary Radio Relay network thereby notifying the Operator of the Corrective action.

Silverfish Cyber Attack Use Case #3

Cyber Attack Use-case	Attack Target	Attack Method	Description	Detection Method / Corrective Action
2.1 Delays in situational awareness	Acoustic / Seismic Sensor	Insider	During deployment of the obstacle network, a Cyber Attacker inappropriately installs the Obstacle Sensors so as to affect proper reporting.	*Design Pattern: Data Consistency* Detection Method The Sentinel Application within the Vehicle monitors Sensor Activity for consistency (Seismic, Acoustic, IR & UAV). Corrective Action The Sentinel Application detects ongoing inconsistencies of Seismic and Acoustic sensor data from multiple Obstacles as compared to the IR and UAV sensor reports. The Sentinel "votes" the Obstacle sensor reports as "bad" and sets the Obstacle Situational Reporting state to "TamperDeteced" thereby notifying the Operator of the Cyber Attack. The Situational Aware Application continues to operate in a "reduced" state based on IR and UAV sensor reports. The Situational Aware application recommends that an additional Corrective action would be for the Operator to relocate the vehicle to a better vantage point for manual observation.