Modeling Cyber Situational Awareness in Air Traffic Control Center through System Dynamics Analysis

Mohd Ruzeiny Kamaruzzaman

mohd_ruzeiny.kamaruzzaman.mj5@is.naist.jp

iplab Laboratory for **Cyber Resilience**

Institute of Science and Technology — NAIST ®

Abstract

- The highly interdependent nature of dynamic systems in an Air Traffic Control Center (ATCC) necessitate its ecosystem to have a holistic yet focused approach that can provide effective and reliable cyber situational awareness. The taken approach shall determine whether the desired state of operability can be achieved. This research aims to propose a novel technique to obtain cyber situational awareness in the air traffic management setup by analyzing the behavior of interdependent complex systems through specific simulation techniques. The outcome of the simulated scenarios may deduce sets of systems behavior in assessing cyber situational awareness.

Background & Motivation

1.

Increasing cyber systems convergence resulting in new risk dimensions and threats

Digitalization of traditional legacy systems that were based mostly on radio communications into data packets over internet protocol have made information dissemination more efficient and reliable. However challenges surrounding ensuring information security and other technological drawbacks need to be addressed appropriately.

2.

Complexity in monitoring Interdependent Information Infrastructures in a dynamic ecosystem

Interdependent information infrastructures form complex systems that require holistic yet focused approach in monitoring existing cyber interdependencies. Furthermore, behavioural changes in these systems under certain conditions bring complexity in monitoring overall systems performance into higher level. Studying the conditions that would cause such behaviours and predicting its impacts towards mission performance can be used as the benchmark in obtaining situational awareness at a specific time point.

3.
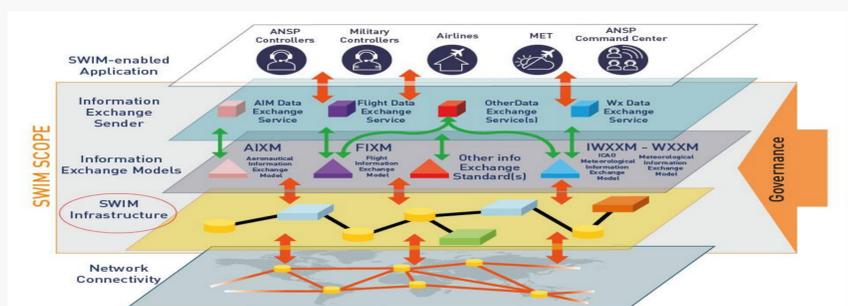
Modeling situational awareness in line with the Systems Wide Information Management (SWIM) concept

Innovations and breakthroughs are more practical when complementing the SWIM initiative. Situational awareness capability should comprise the multi layer architectures of SWIM and the involvement of various internal and external stakeholders within the information exchange domain.

Proposed Idea and Methodology

- Modeling the interdependent systems behavior using suitable approach (i.e. System Dynamics)

  - the chosen modeling technique will simulate a type of failure such as disruption to the network environment which is hosting the ATCC.
  - outcome of the simulated scenarios will be analyzed. For example systems behaviors such as resilience level in the form of time until outage / redundancy switches in.

- Further tests to the earlier simulated outcomes will be run using algorithms related to mission performance evaluation in determining systems' baseline and the deviations under certain induced circumstances. Among the anticipated findings after this test has concluded would be a series of behavior changes under specific criteria in a time series.

- The new model would be further tested to propose a situational awareness concept on the information exchange that is in accordance with the SWIM initiative.

Conclusion and Future Work

This research would offer contributions unique to the field of air traffic management by providing **simulation data of events** that can be used for future studies in other important areas such as cyber incident response. Second, **a new model for obtaining cyber situational awareness**. Lastly a **situational awareness concept in line with SWIM**.