Electrical, Computer, Software and Systems Engineering - Daytona Beach

College of Engineering

2014

# Keeping the Skies Safe

Massood Towhidnejad
*Embry-Riddle Aeronautical University*, towhid@erau.edu

Andrew J. Kornecki
*Embry-Riddle Aeronautical University*, kornecka@erau.edu

# Keeping the **skies** safe

**Professors Massood Towhidnejad** and **Andrew Kornecki** shine a light on how their lab is helping government and the aviation industry to enhance the safety and security of software-intensive systems

### Can you give a broad overview of the Next-Generation ERAU Advanced Research (NEAR) laboratory?

**MT:** The NEAR lab is an R&D facility supporting faculty, staff and students. Our team of researchers collaborates with the aerospace and aviation industries (private and government sector) on software engineering proof of concepts; rapid prototyping, modelling and simulation; data mining; and other related R&D projects.

### What expertise is represented in the lab?

**MT:** NEAR lab full-time staff include two PhDs – in Computer Engineering and Computer Science – four Masters of Software Engineering, a Master of Mechanical Engineering, a Master of Business Administration and a Master of Air Science. Our experience ranges from eight to 26 years, with an average of over 17 years. In addition to full-time staff, the lab has access to a large number of graduate and undergraduate students, and faculty members across the Embry-Riddle Aeronautical University.

### How can threats to the security and safety of systems in the aviation industry be analysed and understood?

**AK:** Safety is a critical factor for aviation. The progress of technology, particularly in electronics and computing, has changed the aviation industry. It is a popular saying in the community that modern aircraft are just computers with wings. An aeroplane is a large meta-system composed of multiple systems. Practically speaking, all these systems include some kind of processor and, considering aviation certification requirements, the amount of software is staggering and differs from what is needed for desktop software, for example.

Aircraft safety cannot be analysed any more based only on potential hazards and failures. Due to their increasing interconnectivity, modern computer systems are exposed to a variety of security threats. The complexity of the system itself may make it vulnerable, opening it to malicious actions that ultimately impact safety. Threat modelling assists software engineers in identifying and documenting potential security threats associated with a software product, providing development teams with a systematic way of discovering strengths and weaknesses in their software applications.

### Do you believe more should be done to counter threats to safety-critical systems in the future?

**AK:** The existing guidance in regulated industries (eg. aviation, space, medical, nuclear, transportation) seems to be adequate – assuming the system is not exposed to a malicious manipulation. Unfortunately, with the increasing interconnectivity of systems, such an assumption is unrealistic. Therefore, it is critical that safety professionals, including developers of safety-critical systems, are exposed to issues of security, while security professionals who typically focus on IT problems are aware of the safety implications of security violation.

### In what capacity have you been involved in the development of the Federal Aviation Administration (FAA)'s Next Generation Air Transportation System (NextGen)?

**AK:** One of the most dominant research areas at the NEAR lab is FAA's NextGen project. Our involvement has included contributing to human-in-the-loop simulation for the NextGen 4D flight management systems project.

Alongside software engineering graduate students, we defined software requirements for the AviationSimNet (ASN) Gateway – an intermediary between the NEAR lab's Real-Time Distributed Simulation (RTDS) and the nationwide airspace simulation system in the

FAA Technical Center – that provided logic for two-way communication and transfer messages between RTDS and ASN, as well as storage for the exchanged data.

We also developed and analysed safety and security requirements for the Gateway software based on the analysis of system assets, hazards, threats and attacks. This work related directly to ultimate real-life future implementation with a focus on communication security and the safety of the impacted aircraft in the simulation scenario. The fault tree model-based analysis, supported by a commercial tool, was a foundation to propose mitigations assuring the Gateway system's safety and security.

### One of your research objectives is to convince the world about the need for software engineering education. Why do you feel this is important?

**AK:** One major problem for the computing profession is the lack of a unified theory and approach to combine often dissimilar viewpoints: discrete and mathematical underpinnings of computer science, versus computer engineering, which focuses on building real systems considering spatial and material constraints of space, energy and time. Modern embedded systems include both viewpoints: microprocessors running software and programmable electronic hardware created with an extensive use of software. Rigorous discipline in terms of software engineering facilitates building real-world systems with good engineering practices and established processes.

The gap between science and engineering approaches is visible in education, where individual university departments tend to stay within their comfort zones, leading to stove-piping of academic programmes and limiting graduates to hearing only one side of the story.

# Gateway to **next-generation research**

Investigations underway at the Embry-Riddle Aeronautical University's **Next-Generation ERAU Advanced Research laboratory** are helping to create a new national airspace system for the US Federal Aviation Administration while simultaneously improving overall knowledge in software engineering

THE MODERN CONVENIENCES people enjoy in their everyday lives, from automobiles to mobile phones and televisions, all rely on embedded software to function properly. The technology also has applications in essential sectors such as the military, banking, medicine and transport. In the aviation industry in particular, software-intensive systems are both critical and abundant. Modern aircraft use embedded software and dedicated hardware for autopilot flight control, displays, navigation, communication, engine control and much more. Any issues with these systems – even a minor fault – could have a major impact on overall aircraft safety.

To ensure the safety of such critical systems, hazard analysis is conducted to determine their development requirements, testing and management. This is the precise area in which the Next-Generation ERAU Advanced Research (NEAR) laboratory is able to contribute its considerable expertise.

## A PATH TO SAFETY

The NEAR lab is based at Embry-Riddle Aeronautical University (ERAU) in Florida, USA. The lab researchers have experience working in industry, with their backgrounds including aviation, software engineering and business. To complement the expertise of the full-time staff, the lab often cooperates with university faculty specialising in air traffic control, human factors, a variety of engineering domains, and airline, military and private aviation.

The lab undertakes studies, technical evaluations and human-in-the-loop and hardware-in-the-loop simulations to analyse and develop solutions to issues faced by the aviation industry. The researchers make use of the lab's real-time simulation environment, which allows them to link to external simulators, such as AviationSimNet, the national aviation simulation environment, the Federal Aviation Administration (FAA)'s live aircraft position data feed, and weather data. Professor Massood

Towhidnejad, Director of the NEAR lab, explains the value of having such a facility in-house: "This allows the lab to establish simulation scenarios where the simulation components – eg. aircraft simulator and air traffic controller – could potentially be distributed across the nation, while the participating aircraft are a combination of real and simulated aircraft affected by different weather phenomena".

The state-of-the-art facilities at the NEAR lab provide the researchers with the tools they need to conduct research into airspace safety, control, capacity and efficiency. For example, their research has led to new insights that have helped to improve airport capacity and efficiency as well as reduce in-flight fuel costs and streamline ground operations. As a result, the lab has been hired by a number of high-profile players in aviation, including the FAA, NASA, National Oceanic and Atmospheric Administration (NOAA) and Boeing.

## IN FOCUS

Some focus areas for the NEAR lab's recent research have included hardware and software certification for real-time safety-critical systems, analysing potential threats to cyberphysical systems, and looking at Bayesian belief networks (BBNs) enhanced with rough sets (RSs) as adequate tools to solve computational problems with insufficient information.

A BBN is a statistical model representing the joint probability distribution of a set of random variables with explicit independence assumptions, all described through a graph. The graph's nodes represent variables and arcs represent probabilistic dependency relations among the variables. This allows the system to be diagnosed or analysed even when some data are missing. "With my colleague, Dr Janusz Zalewski from Florida Gulf Coast University, we recently showed that BBNs and RSs can be combined to enhance the process of reasoning under uncertainty in case of missing values of

certain attributes of objects," reveals NEAR lab member Professor Andrew Kornecki. "RSs helps make BBNs more valuable in case of the occasional lack of evidence for real-time decision making or active safety diagnostics, with information being supplied to the nodes during operation."

The applications for this research are of significant value to the aviation industry: "Using well-established techniques, supported by commercial tools, we are able to assess the security and safety characteristics of selected systems and identify methods leading to certification of systems in aviation," Kornecki highlights.

## RETHINKING AIRSPACE

One of the major research areas that the NEAR lab is involved in is the FAA's Next Generation Air Transportation System (NextGen) project. NextGen will culminate in a new, satellite-based national airspace system for the US by 2025. The system will mean a number of improvements in the way airspace is managed. For example, controllers will be able to monitor and manage aircraft with greater safety margins, planes will fly closer together, take more direct routes and runway congestion will be reduced.

The changes will result in noticeable improvements for passengers, such as quicker flight times and fewer delays. On a wider scale, it will also lead to significant economic and environmental gains. It is estimated that over the next five years, NextGen will reduce aviation fuel consumption by 1.4 billion gallons and cut emissions by 14 million tonnes. By decreasing gridlock, both in the air and on the ground at airports, it is expected that the new system will save the US economy around US $22 billion each year in lost economic activity.

## SIGNIFICANT CONTRIBUTION

However, such a major overhaul is no simple task, and requires expert knowledge and major research. To support the NextGen project, the NEAR lab is making contributions through a number of research efforts. The ERAU is tasked with managing the FAA's Florida Testbed, located at Daytona Beach International Airport. As the technical arm of the ERAU, the NEAR lab

# INTELLIGENCE

## NEXT-GENERATION ERAU ADVANCED RESEARCH (NEAR) LAB

### OBJECTIVES

• To provide safety and security measures for software-intensive systems

• To explore the feasibility of system property-based dependability assessment

• To assess the impact of adding security countermeasures on system performance

• To convince the world about the need for software engineering education

### CURRENT AND PREVIOUS COLLABORATORS

**American Airlines • Barco • Boeing, Inc. • County of Volusia • CSC • Daytona Beach International Airport • Delta Airlines • Embry-Riddle Aeronautical University** (ERAU) **• ENSCO Inc. • Federal Aviation Administration** (FAA) **• Frequentis • General Electric • Harris Corporation • JetBlue Airlines • Jeppesen • Lockheed Martin Corporation • Mosaic ATM • Sensis Corporation • The Volpe Center**

### CURRENT FUNDING

FAA • Boeing Company • ERAU • Mosaic ATM • National Oceanic and Atmospheric Administration (NOAA)

### CONTACT

**Professor Massood Towhidnejad**
Director, NEAR lab

Embry-Riddle Aeronautical University
Electrical, Computer, Software and Systems
Engineering Department
College of Engineering
Lehman Engineering Center
Room 354 Daytona Beach
FL 32114, USA

**T** +1 386 226 6891
**E** towhid@erau.edu

**www.near.aero**
**http://faculty.erau.edu/korn/**
**www.near.aero/current/bio_massoodt.html**

**PROFESSOR MASSOOD TOWHIDNEJAD** completed his PhD in Computer Engineering in 1990. He is the Director of the NEAR lab, and Professor of Software Engineering in the Department of Electrical, Computer, Software, and Systems Engineering at ERAU. His research interests include software engineering, software quality assurance and testing, autonomous systems, and air traffic management.

**PROFESSOR ANDREW J KORNECKI** completed MSEE (1970) and PhD (1974) degrees, with the AGH University of Science and Technology in Krakow, Poland. He joined ERAU in 1985 and in 1995, resulting from a National Science Foundation grant, he designed and implemented the ERAU Real-Time Laboratory. His recent area of research focuses on dependable software-intensive systems in regulated industries such as aviation.

**EMBRY-RIDDLE**
Aeronautical University

plays a pivotal part in furthering this facility. "We perform almost any technical activities that are needed in order to maintain and operate FAA's laboratory facility," Towhidnejad describes. "This includes the initial hardware and software infrastructure, necessary system maintenance, software development for interfacing the systems in the lab, and more."

NEAR lab researchers are also directly involved in a variety of NextGen projects. "Typically these projects require the expertise of a number of different industry partners in combination with personnel from the FAA and NEAR lab," Towhidnejad explains. For example, in one project – the Aircraft Access to System Wide Information Management (SWIM) – NEAR lab members serve as the technical leaders responsible for the work carried out by their industrial partners. Other projects investigate unmanned systems, 4D flight management systems, aircraft arrival management systems and real-time exchange of flight data. "The NEAR lab has also been employed as a subcontractor for a number of NextGen-related work being conducted by other industries," Towhidnejad adds.

## WINGS FOR THE FUTURE

The NEAR lab is not only a research facility, it is also committed to educating aspiring students. One way the lab aims to train up and coming professionals is by addressing the divide between the different computing and engineering fields. "Considering how to close the gap between hardware and software constitutes a significant paradigm shift in the education of the future cadre of dependable system developers," Towhidnejad notes.

The idea is to link up studies in computer science, computer engineering and software engineering to create an all-encompassing curriculum for software engineering education. Although these three fields all take different approaches, they are all important to the creation of reliable embedded systems. The NEAR lab has published papers advocating software engineering education, and has outlined key concepts that should be included in an undergraduate programme. "The proliferation of software-intensive cyberphysical systems in everyday life forces industry to hire engineers familiar with time-critical reactive dependable systems, those who understand the issues of safety and security and the intricacies of hardware-software interaction," explains Kornecki.

By contributing their expertise to influence important projects and industry players, combined with the lab's focus on nurturing the next generation of engineers, the NEAR lab is securing the future of aviation and shaping the skies of tomorrow.



Software engineering students at work.