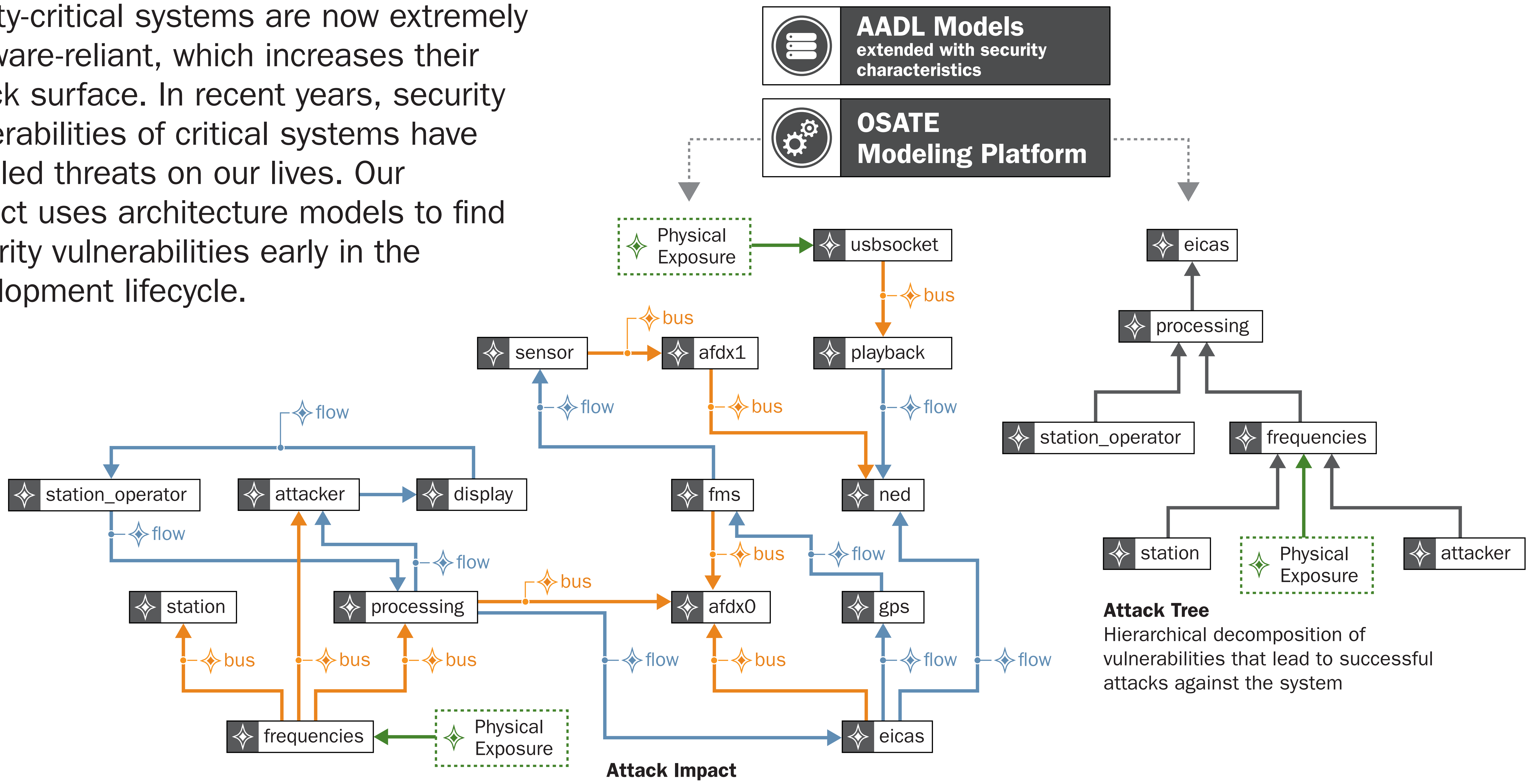
Automated Assurance of Security Policy Enforcement

Detecting and fixing architecture-related vulnerabilities early in the lifecycle

Safety-critical systems are now extremely software-reliant, which increases their attack surface. In recent years, security vulnerabilities of critical systems have enabled threats on our lives. Our project uses architecture models to find security vulnerabilities early in the development lifecycle.



Attack Impact
Exhibits all components' vulnerabilities and their impact within the architecture

Attack Tree
Hierarchical decomposition of vulnerabilities that lead to successful attacks against the system

After the Jeep hack in 2015, Fiat-Chrysler issued a massive recall of 1.4 million cars. In the medical domain, the FDA advised hospitals to stop operating the Symbiq Infusion System due to potential tampering. With estimates targeting more than 20 billion connected devices by the end of 2020, the number of vulnerabilities, and their impact, will continue to grow. Vulnerabilities are no longer only a matter of code but strongly related to the system architecture.

The SEI team is working on solutions using the semantics of the Architecture Analysis & Design Language (AADL) and its extensions to detect vulnerabilities in software architectures. We are developing an AADL extension to capture security concerns in software architecture as well as new analysis tools that produce security reports from an AADL architecture.

What vulnerabilities can we detect?

The latest reports show that vulnerabilities are no longer related only to code (e.g., buffer overflow, semantic code) but are tightly coupled to the architecture: in component connections (e.g., use of encryption), shared resources (e.g., processing or memory), or configuration directives (e.g., use of encryption). We extended the AADL core language to provide the capability to detect common architecture-related vulnerabilities. With security expertise from the SEI CERT Division, we identified AADL modeling patterns for architecture-related vulnerabilities. We also identified patterns to capture and recognize Common Vulnerabilities and Exposures (CVE) in AADL architecture models.

A collaborative effort for safer systems

We initiated collaboration with the following projects or standardization bodies:

SAE AS-2C: As the technical lead of the AADL standard, the SEI team collaborates with the standardization committee and will propose a new security annex for the standard.

The Open Group: The SEI is working with the Open Group and its Real-Time Embedded Systems Forum on a MILS standard for developing secure systems.

The MITRE CVE: With security knowledge from the CERT Division, the SEI team mapped architecture-related CVEs into AADL to detect security vulnerabilities in architecture models.

How are vulnerabilities reported?

The SEI research team developed AADL architecture analysis tools to detect vulnerabilities and show their impact. The tools currently generate two analysis reports from AADL models:

Attack Impact: This comprehensive report provides the architecture vulnerabilities for each component and shows how they are propagated using connections and shared resources. This analysis method is similar to Failure Modes and Effects Analysis.

Attack Tree: A hierarchical tree represents the relationships between contributors (architecture elements and vulnerabilities) of a compromised component. This analysis method is similar to Fault-Tree Analysis.

These tools are integrated with the AADL modeling tool OSATE and are available under the open source Eclipse Public License for download.

Making an impact

We have demonstrated our approach through case studies from the automotive and avionics domains. We retro-engineered automotive architectures to show how our approach and tools can detect security issues such as the one reported in the Jeep hack. For the avionics domain, we demonstrated our approach in the System Architecture Virtual Integration (SAVI) consortium and showed how attacks against the Automatic Dependent Surveillance-Broadcast (ADS-B) protocol could impact airplanes and ground station security.

Contact: Julien Delange | jdelange@sei.cmu.edu