BAE SYSTEMS

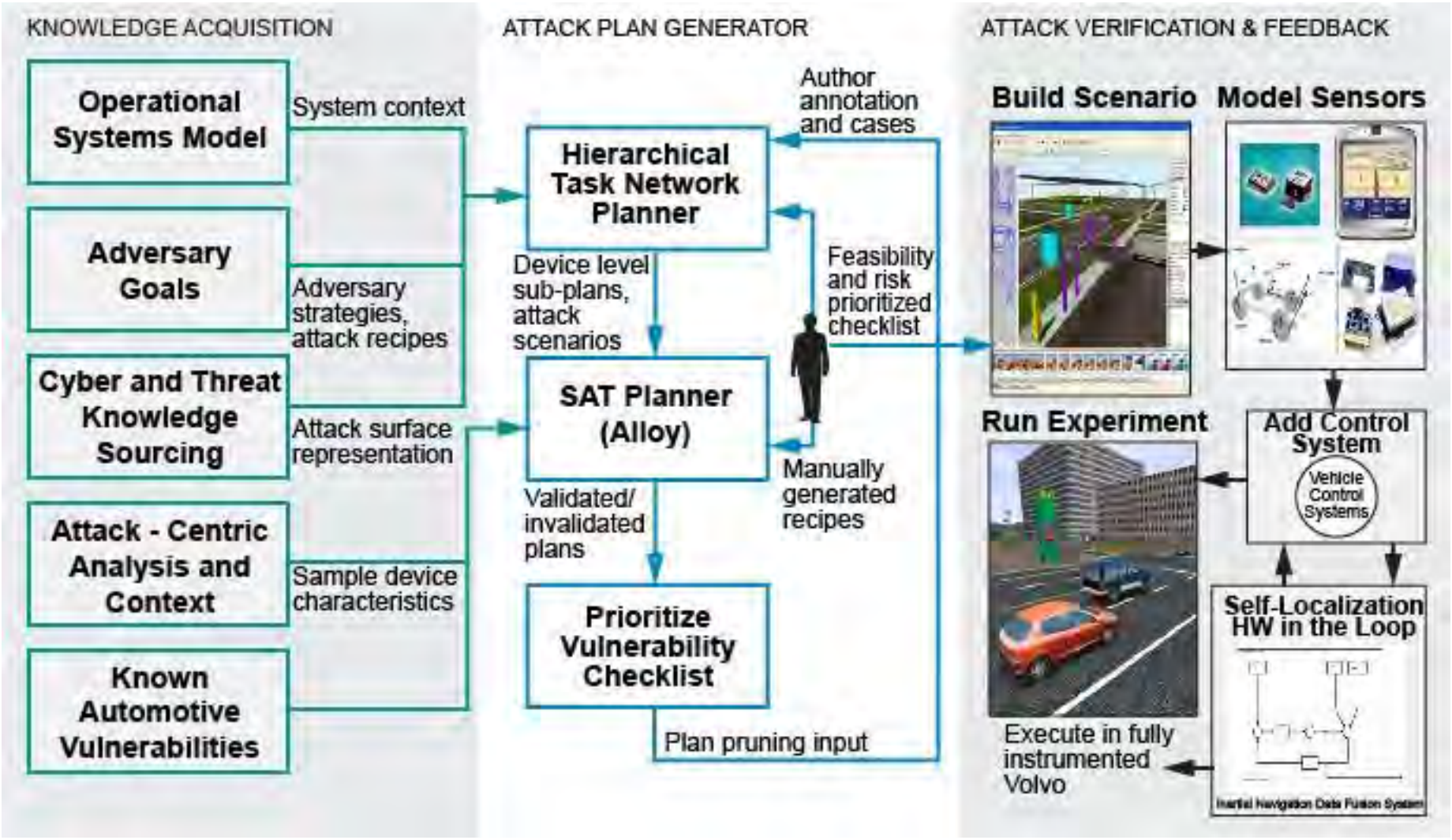
Applied Vulnerability Detection System

J. Smith, B. Krikeles, D. Wittenberg and M. Taveniku

April 14, 2015

BAE SYSTEMS

Generate, verify, and prune to manage and prioritize possible attack point vulnerabilities



BAE SYSTEMS

Data from multiple external sources seeds a goal-oriented attack plan generation process

KNOWLEDGE ACQUISITION

Characterizing systems based on their exposed services versus their marketed functions.

How services and vulnerabilities relate to attack objectives.

Operational Systems Model

System context

Adversary Goals

Adversary strategies, attack recipes

Externally available services reside on Device Layer 0.

Attack surface representation

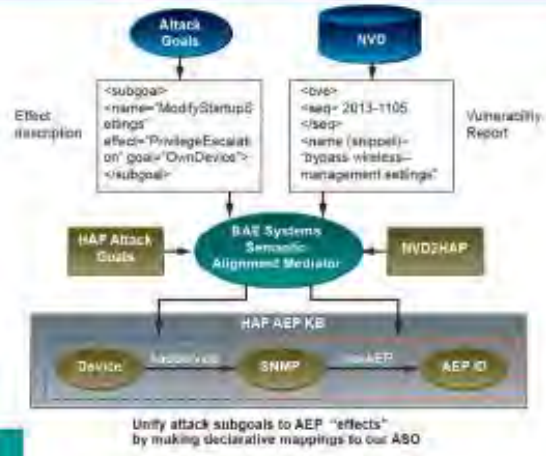
Transforming existing data into attack-centric representations.

Cyber and Threat Knowledge Sourcing

- ID and auto-capture data sources
- Use a BAE Systems mediation solution to process data source records and attach new semantic "Weakness" and "Effect" descriptions
- Transform data sources into a standardized Attack and Exposure Point (AEP) record based on a new Attack Surface Ontology (ASO)

Attack - Centric Analysis and Context

- Construct a new AEP device view that aligns with how an adversary seeks to expose the device's attack surface
- Unify disparate device scanning techniques into an automated framework that populates a common Device Characterization Ontology for analysis by the planner
- Infer adversary goals from data collected on the attacks that adversaries have already conducted against other systems based on attack patterns derived from the Common Attack Pattern Enumeration and Classification (CAPEC)

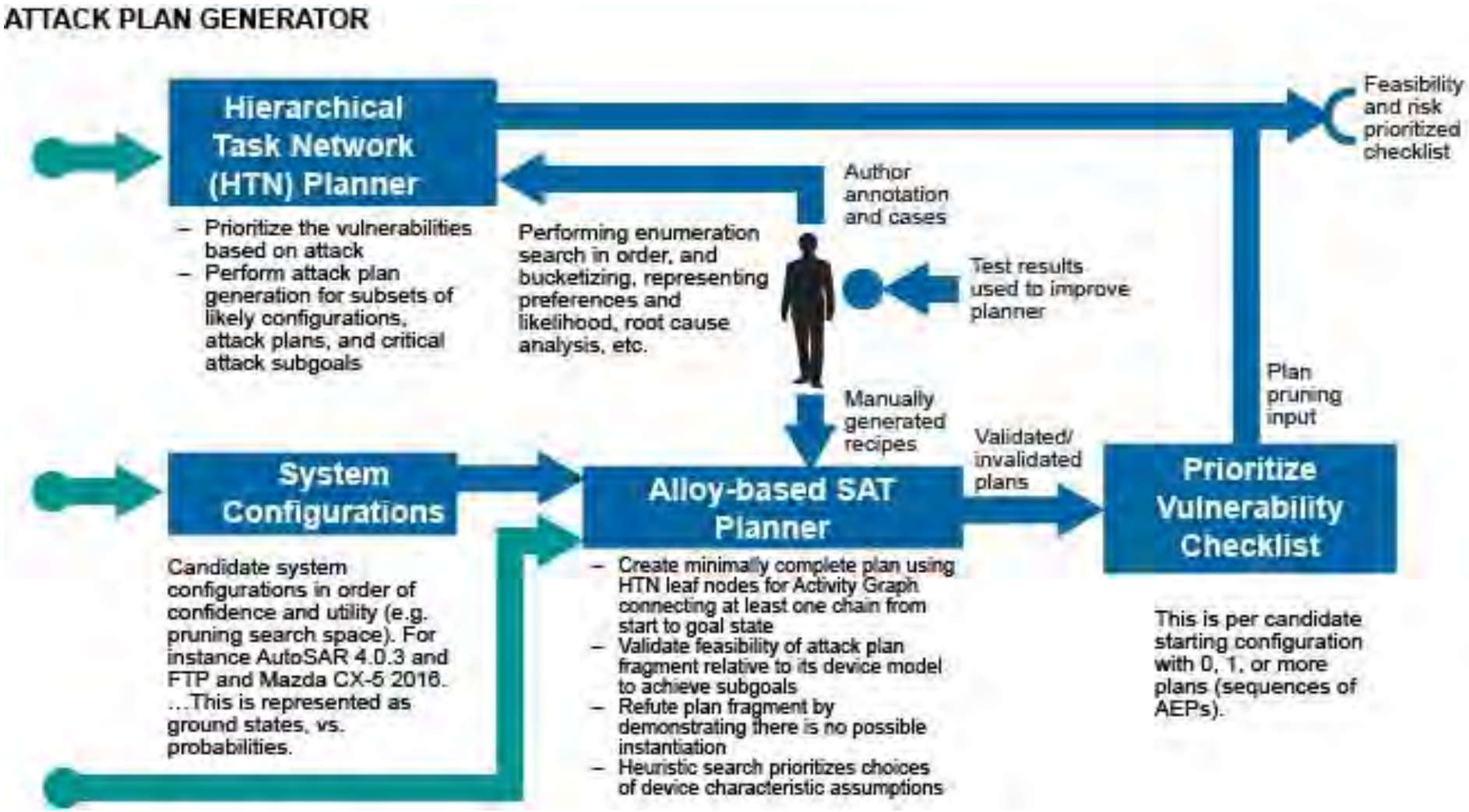


Known Automotive Vulnerabilities

Includes services that an attacker can misuse.

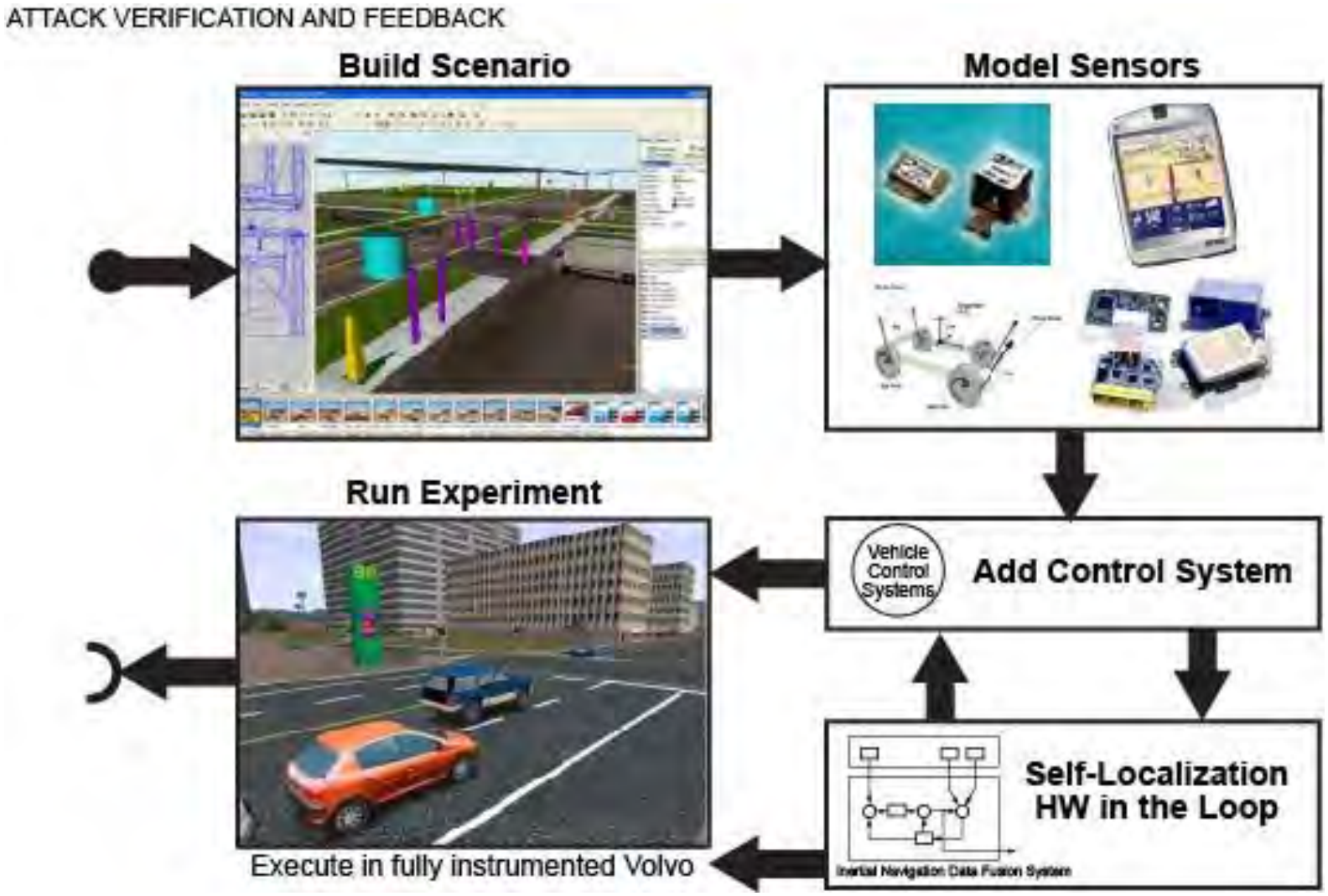
BAE SYSTEMS

The identified attack space is reduced by using a vulnerability-based feasibility analysis



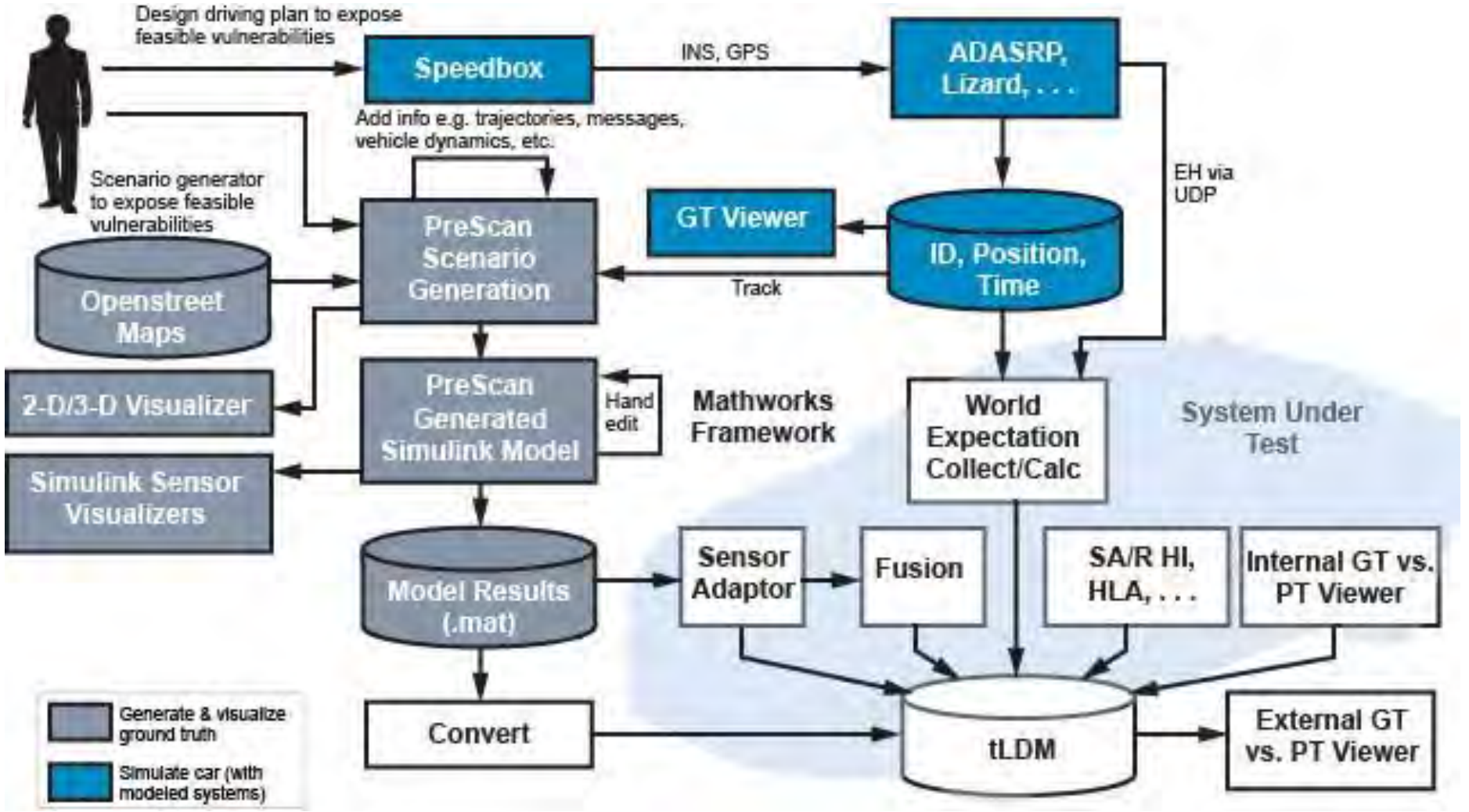
BAE SYSTEMS

PreScan simulations verify attack plans and identify exhibiting an emergent system-level vulnerability



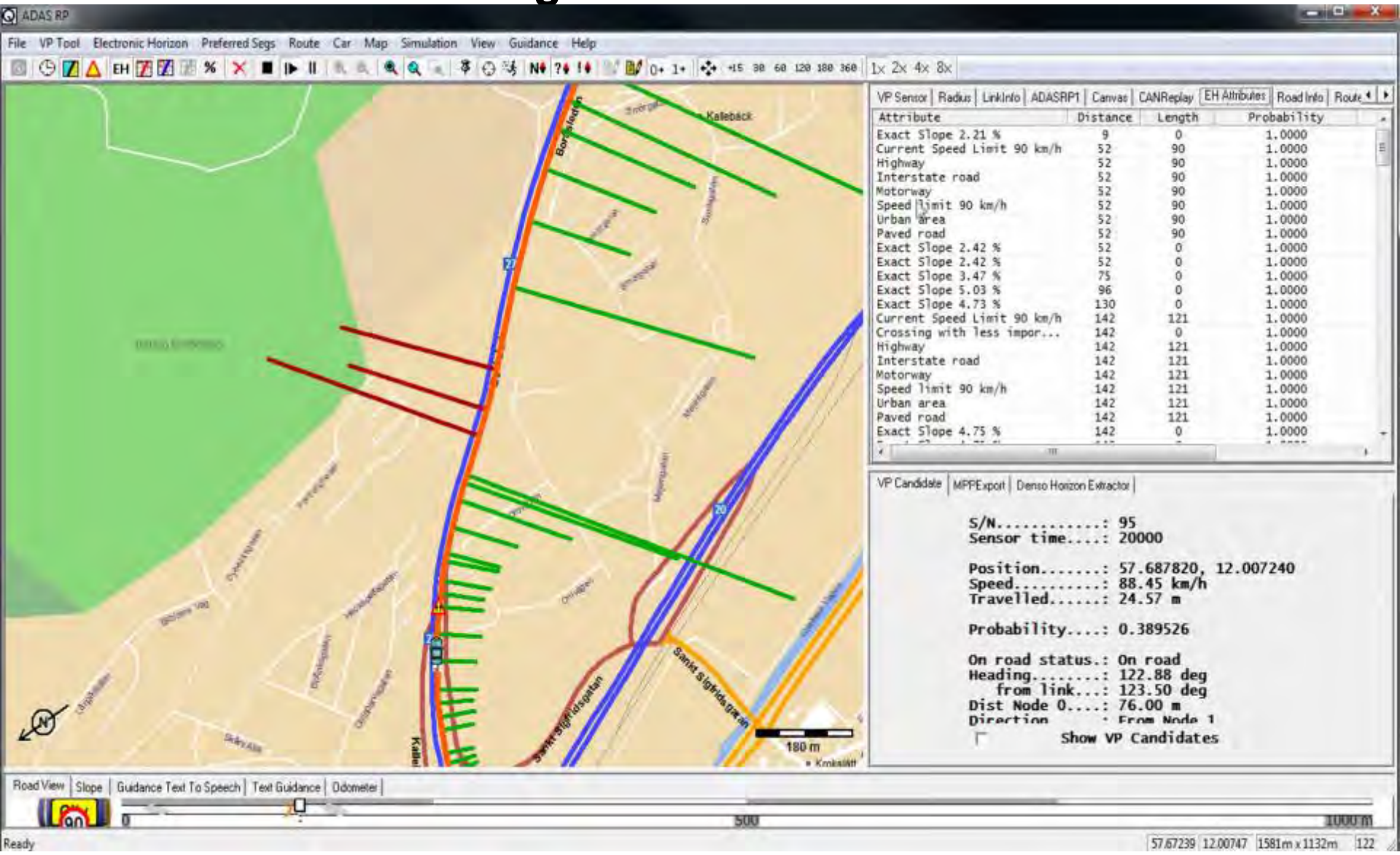
BAE SYSTEMS

Ground truth is used to calibrate PreScan simulations



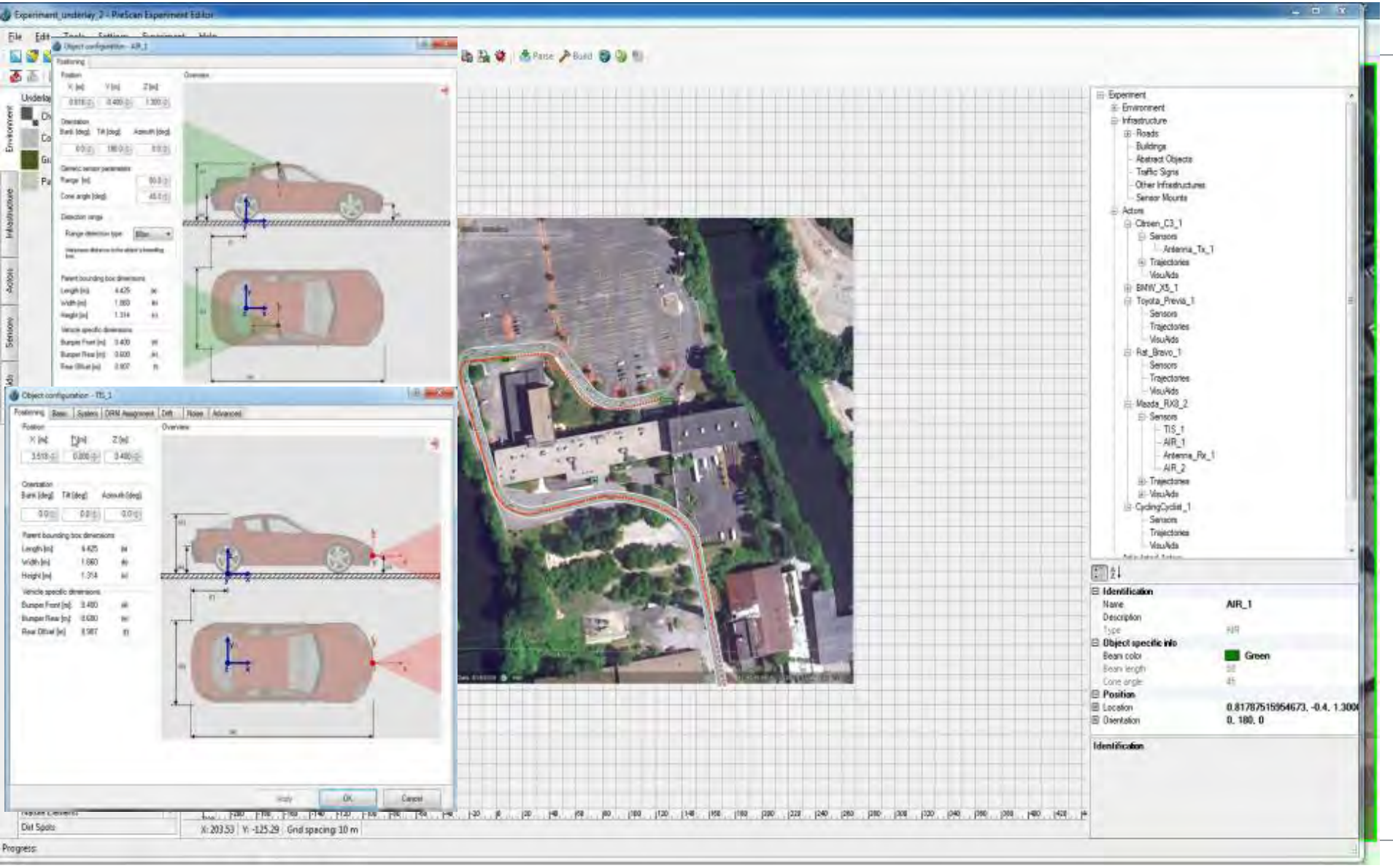
Generate and visualize ground truth, verify simulation scenario against actual

BAE SYSTEMS



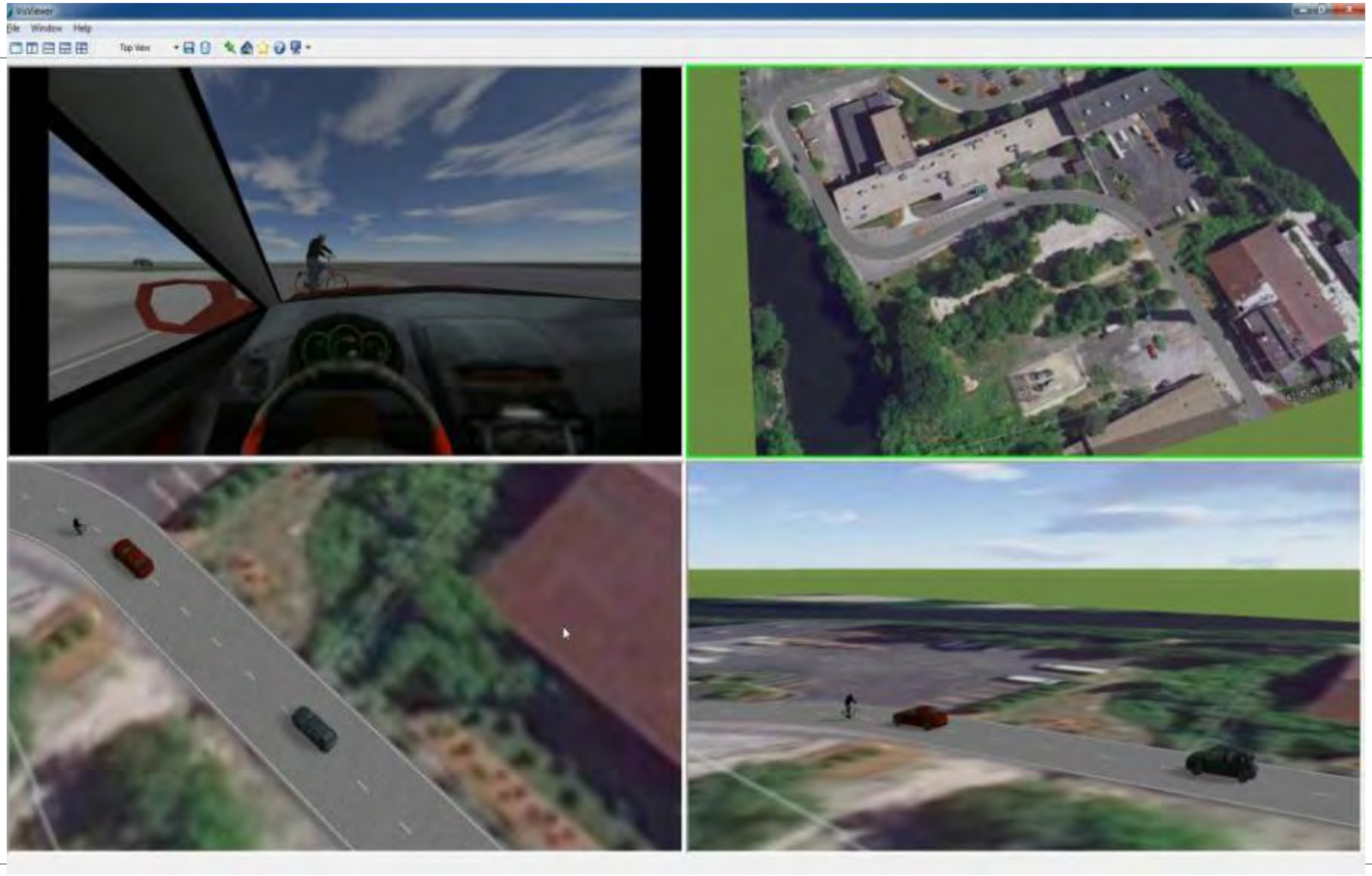
Model car sensors and additional obstacles for vulnerability analysis

BAE SYSTEMS



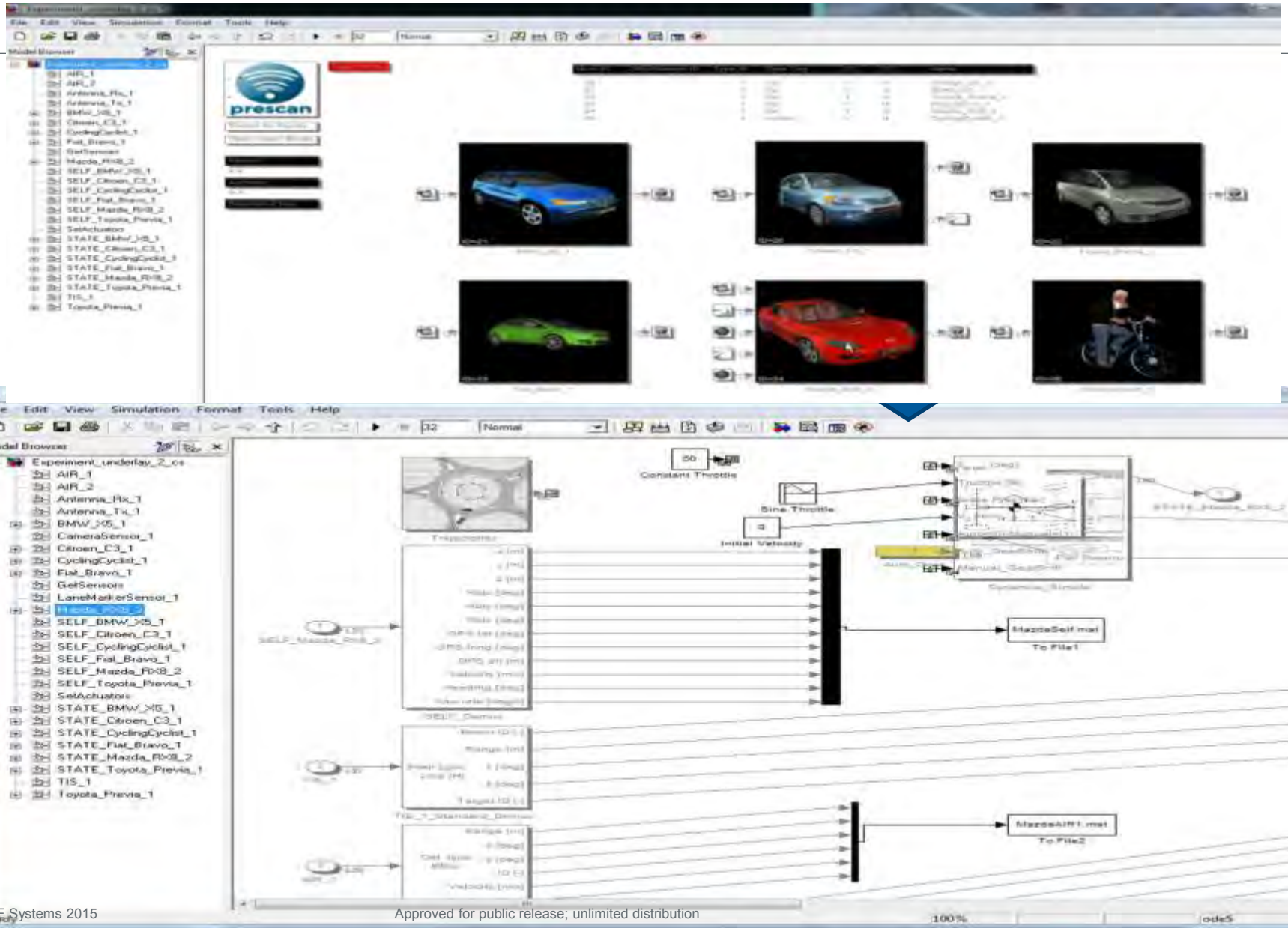
Run simulation to visualize and generate Simulink

BAE SYSTEMS



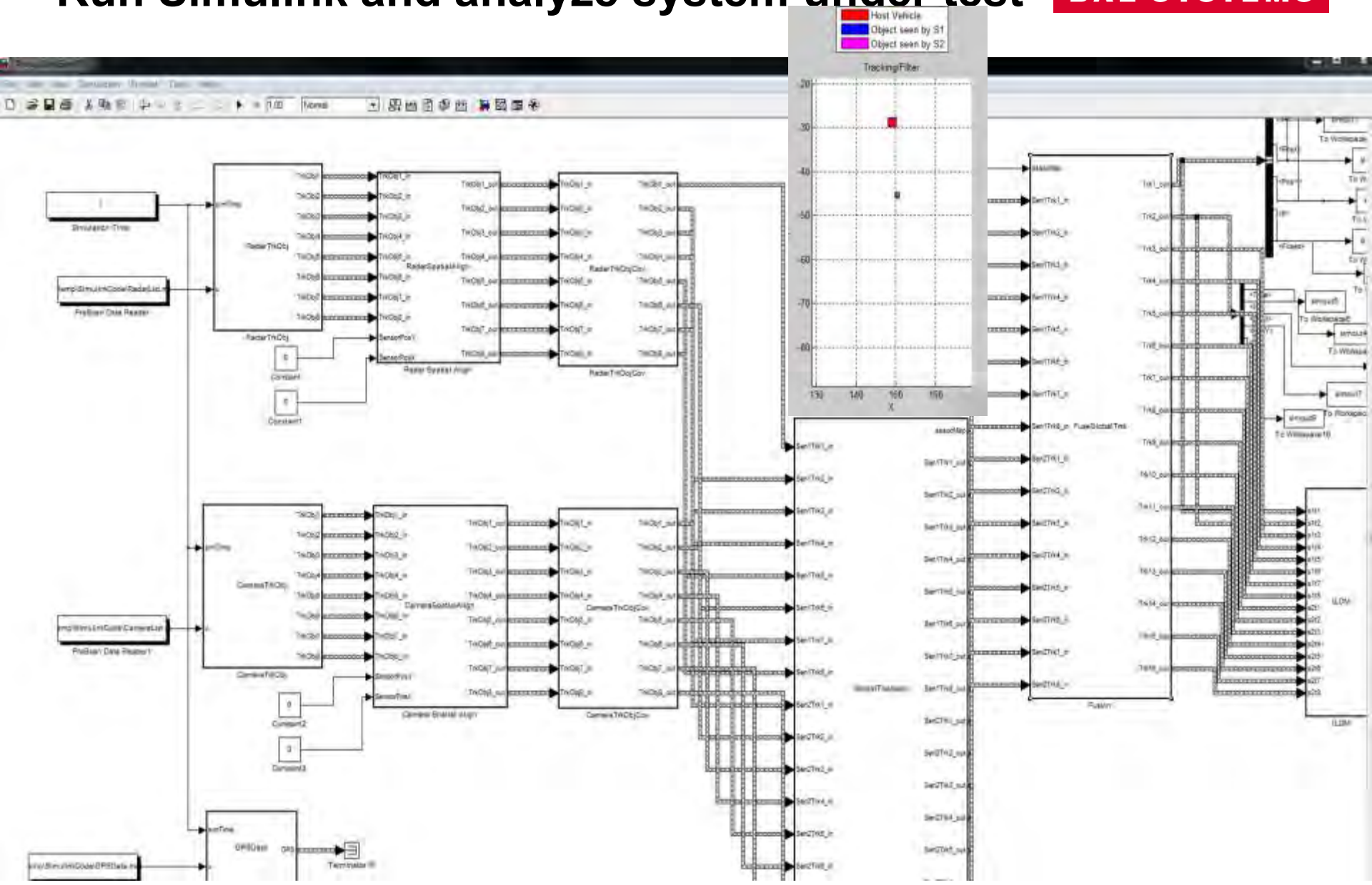
Edit Simulink adding fault injection and dynamic model changes

BAE SYSTEMS



Run Simulink and analyze system under test

BAE SYSTEMS



BAE SYSTEMS

Summary: The system equips users to…

- Automatically detect emergent vulnerabilities in complex CPS
- Approach from the attacker's point of view
- Automatically ingest public and private lists of vulnerabilities and organize them into a standardized Attack Point database
- Generate the set of composite device-level attack scenarios
- Reduce the cardinality of the generated attack space by evaluating the feasibility of each attack against device characteristics and constraints
- Discard unlikely or infeasible attacks and prioritizes the remainder by risk size and likelihood of occurrence
- Use prioritized vulnerability list to confirm or rule out each candidate attack and feeding back to refine planning