Serendipity

Secure and dependable platforms for autonomy

Computer

Volvo Concept Lab

Mikael Sjödin
Prof. Datavetenskap

Mälardalens universitet

Serendipity

Computer

Secure and dependable platforms for autonomy

Mälardalens universitet

© AIRBUS S.A.S. 2017 - computer rendering by FIXION - photo by dreamstime.com - MMS 20171137 AIRBUS

**Autonomous,
connected,
heterogeneous,
time-sensitive,
cyber-physical systems,
systems-of-systems.**

Background: Dependable systems

- Redundancy-based fault tolerance,
- self-monitoring,
- self-healing, and
- self-reconfiguring.

Hypothesis

- Security and safety can be addressed in a uniform manner based on these features

Background: Dependable systems

- Redundancy-based fault tolerance,
- self-monitoring,
- self-healing, and
- self-reconfiguring.

Dependability: survive unintentional faults

Hypothesis

- Security and safety can be addressed in a uniform manner based on these features

Security: survive intentional faults

Serendipity

Computer

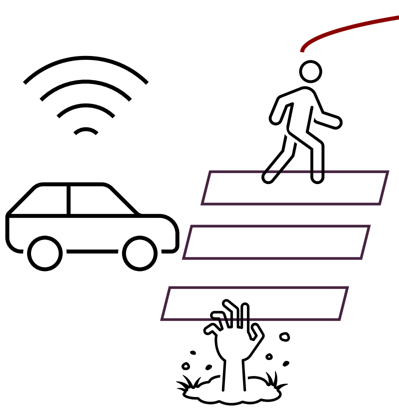
Secure and dependable platforms for autonomy

Mälardalens universitet

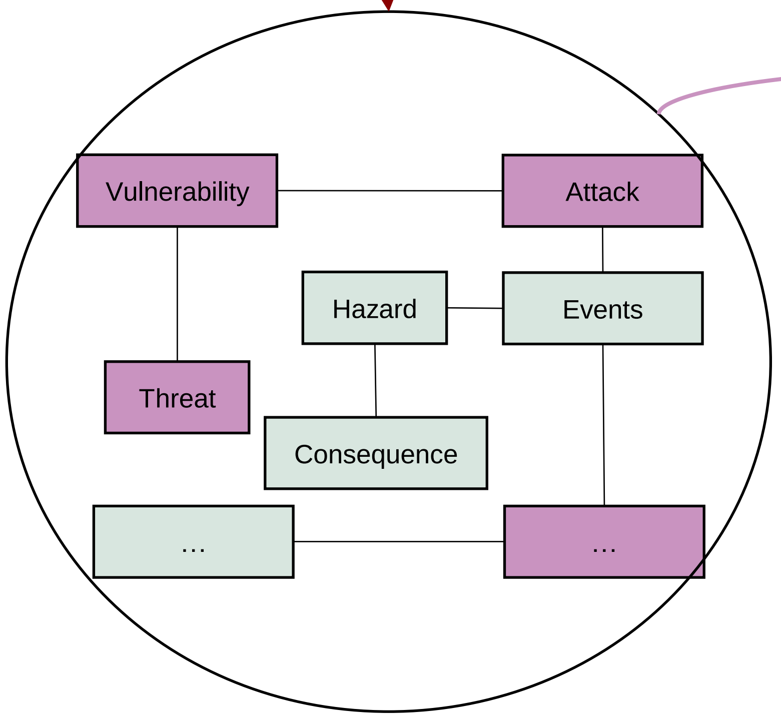
Key contributions (so far…)

- Ontology for safety and security
  - Joint requirements management for safety and security
- Automatic vulnerability detection
  - Identify for safety hazards and security vulnerabilities
- “Friendly Jamming” in wireless networks
  - Add a known jamming signal to prevent eavesdropping

From safety-security risk analysis through ontologies to safety-security requirements



1) Risk analysis of complex and high-collaborative systems to jointly targets both safety & security through…



Vulnerability

Attack

Hazard

Events

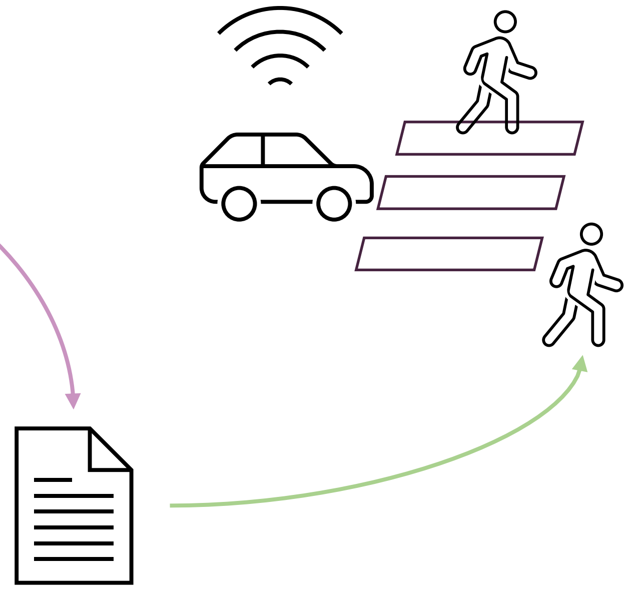
Threat

Consequence

…

…

2) … a combined safety/security ontology to elicit….

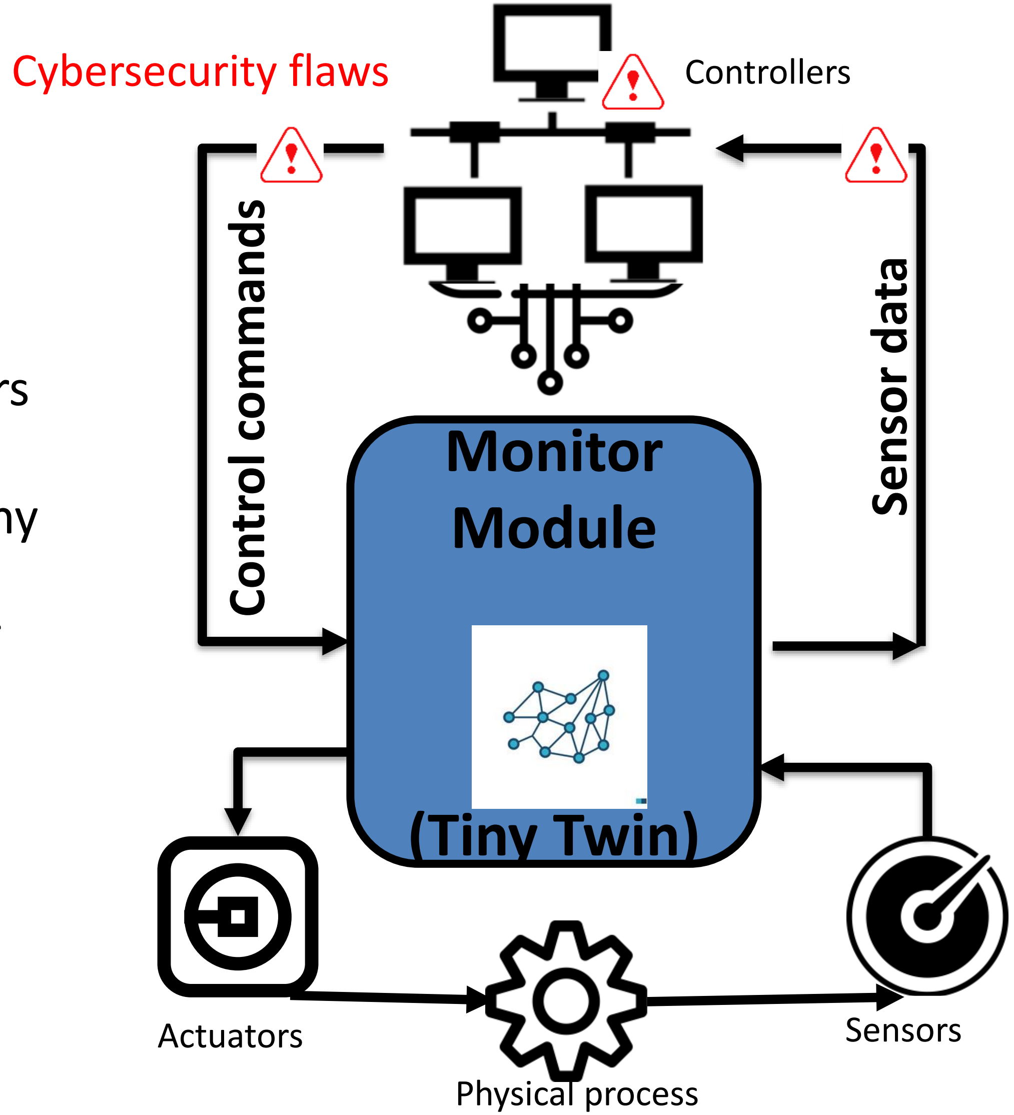


3) ..safety/security requirements that ….

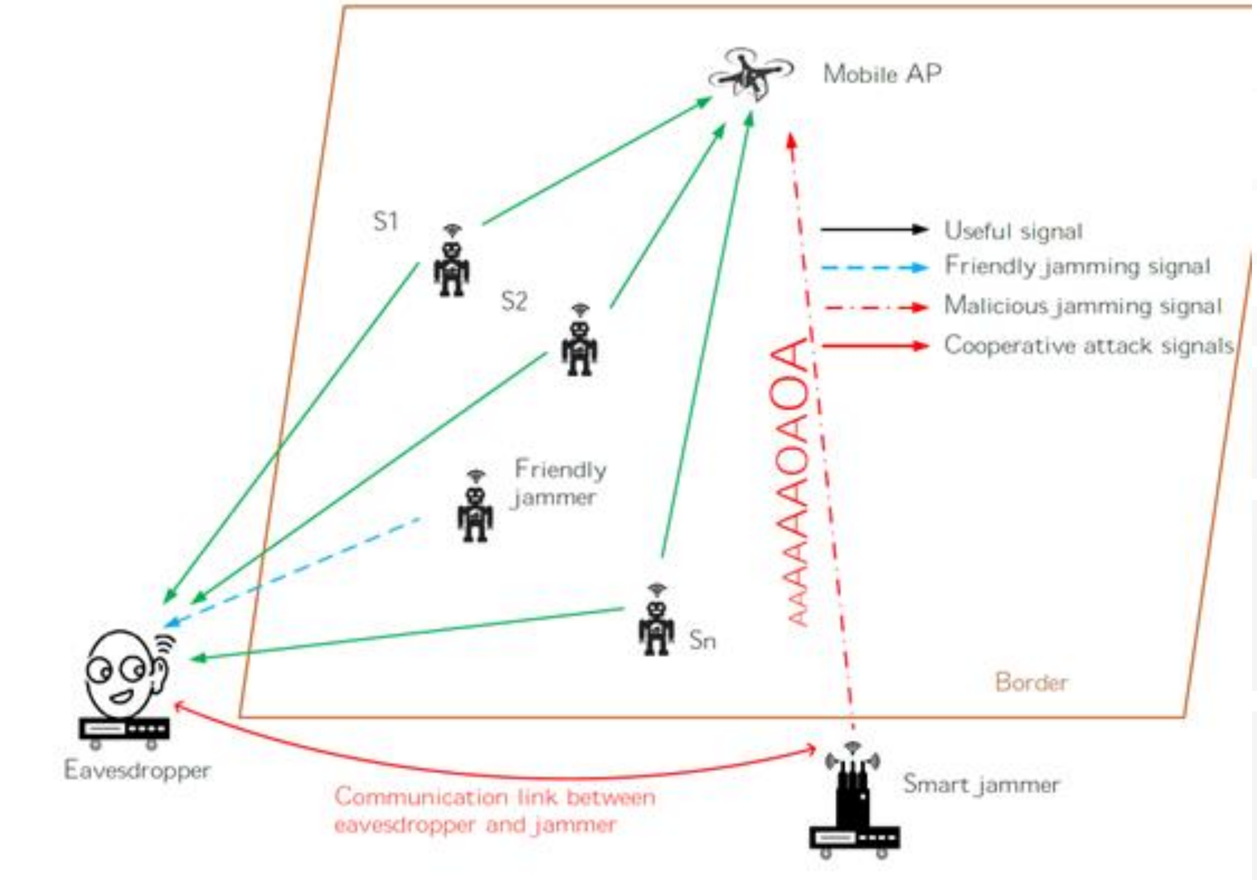
4) .. make the system secure and safety

Automatic Vulnerability Detection

1. Monitor employs a **Tiny Digital Twin** to track the expected behaviour of the system
2. **Listens** to input/output of the controllers
3. **Drops** faulty commands if identifies a mismatch between the transitions in Tiny Twin and input/output
4. Provides a **report** that shows sources of the attacks



Friendly jamming



Threats: eavesdropping and jamming

- Eavesdropping can make jamming attacks more efficient
- Using a friendly jammer to mask friendly transmissions
- Secrecy performance measure: adjusted communications such that eavesdroppers experience outages
- Adjusted the framework for secrecy performance analysis to include the use of untrusted relay nodes.

Serendipity

Computer

Secure and dependable platforms for autonomy

Mälardalens universitet

A380
plus
A380 AIRBUS
© AIRBUS S.A.S. 2017 - computer rendering by FIXION - photo by dreamstime.com - MMS 20171137
AIRBUS

Mikael Sjödin
Prof. Datavetenskap

mikael.sjodin@mdu.se