MÄLARDALEN UNIVERSITY
SWEDEN

Incorporating Attack Modeling into Safety Process

Amer Šurković[1], Dzana Hanić[1], *Elena Lisova*[1], Aida Čaušević[1], Kristina Lundqvist[1], David Wenslandt[2], and Carl Falk[2]
[1] Mälardalen University, Västerås, Sweden
{asc17003, dhc17002}@student.mdh.se and
{elena.lisova, aida.causevic, kristina.lundqvist}@mdh.se
[2] Knightec AB, Sweden
{david.wenslandt, carl.falk}@knightec.se

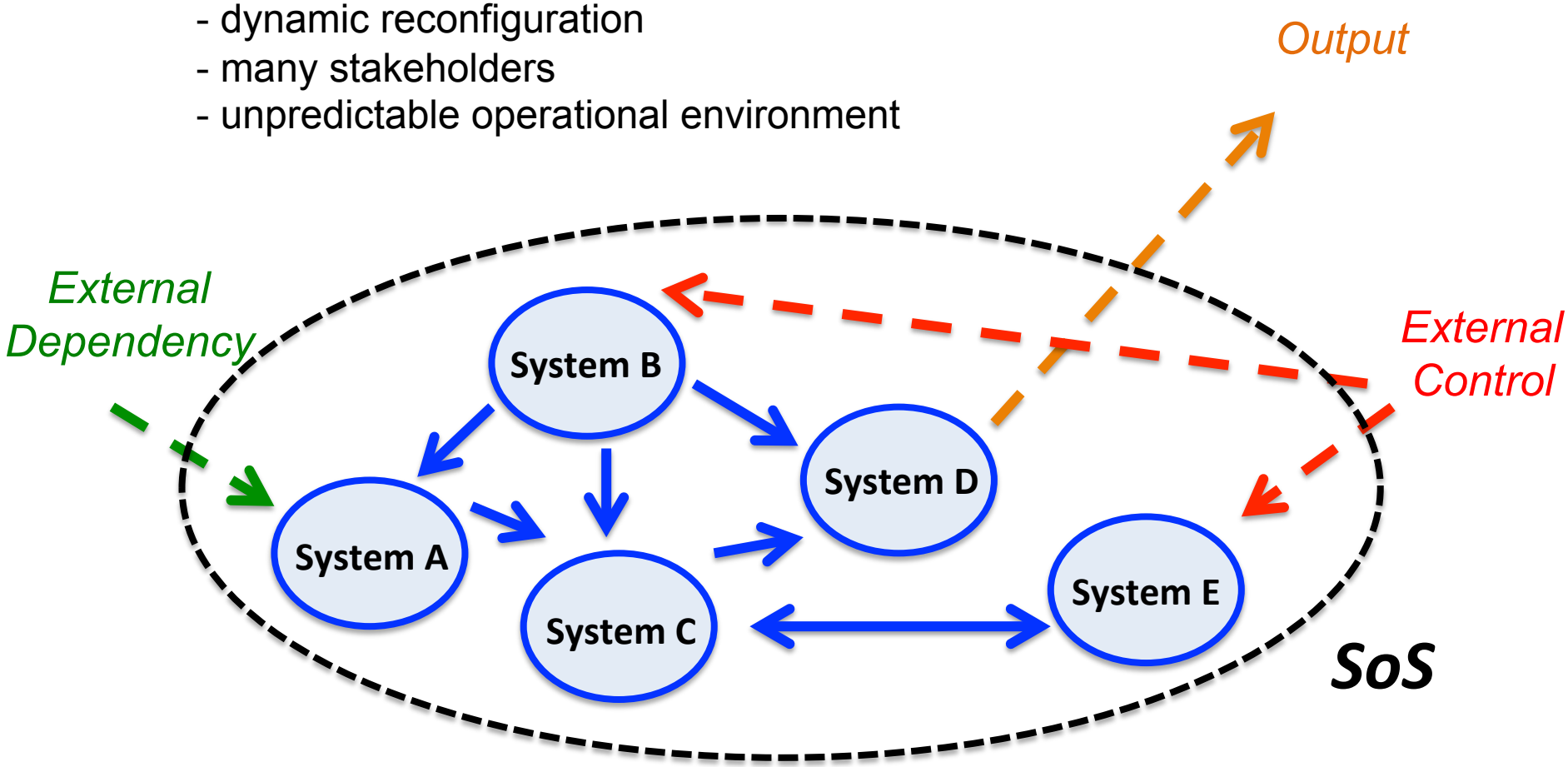
Content

MÄLARDALEN UNIVERSITY
SWEDEN

- Systems of Systems;
- Security Terminology;
- Attack Models;
- Autonomous Quarry;
- Incorporating Attack Models;
- Joint Safety and Security Argumentation;
- Conclusions and Future Work.

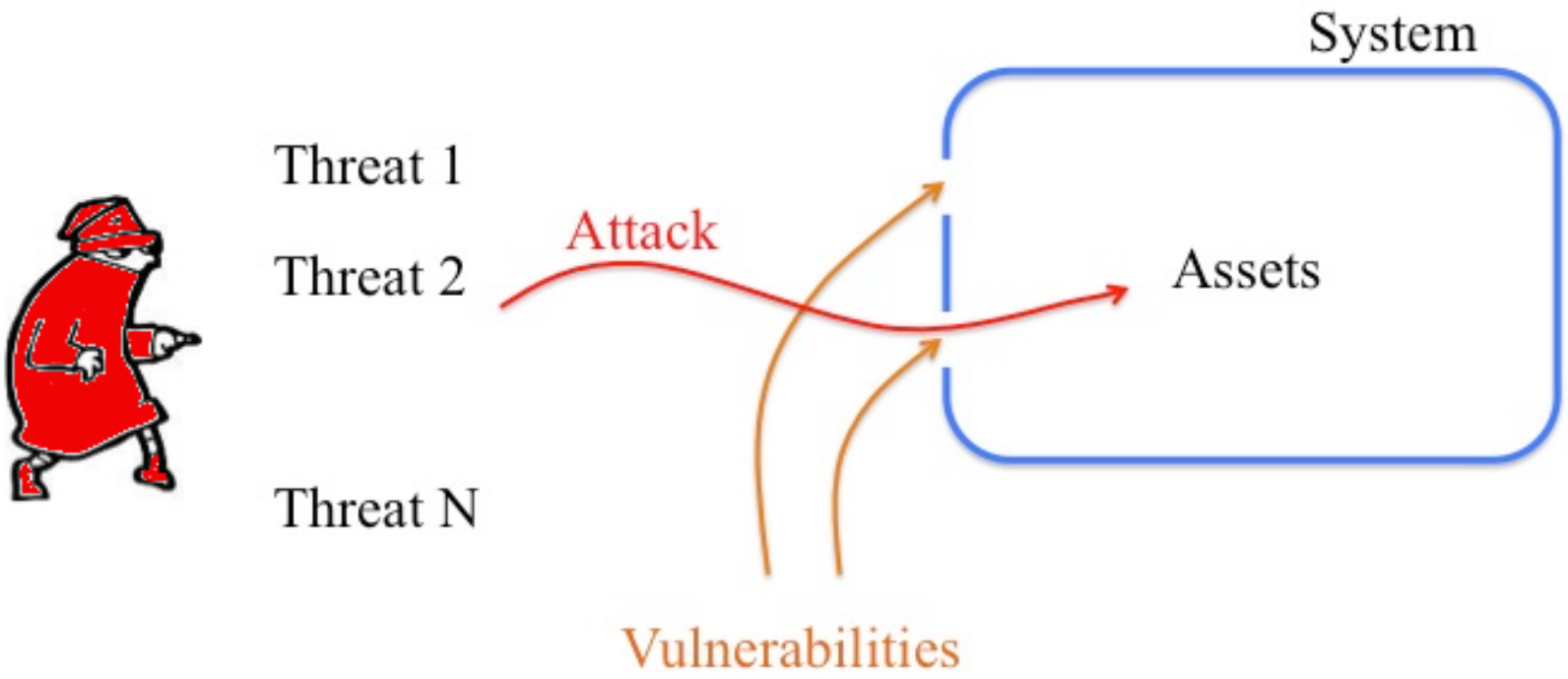
Systems of Systems

- complexity
- connectivity
- control by other systems
- dynamic reconfiguration
- many stakeholders
- unpredictable operational environment



Security

MÄLARDALEN UNIVERSITY
SWEDEN



Attack Models

MÄLARDALEN UNIVERSITY
SWEDEN

A literature survey, 2000-2018

Control Systems

- a general sensor attack model (DoS, integrity attacks);
- DoS and deception attacks;
- aspect-oriented models;
- smart grid attack model;
- power grid attack model;

Vehicular Domain

- attacks exploiting CAN vulnerabilities ;
- attacks exploiting OBU (on-board unit) vulnerabilities;
- attacks exploiting electrical vehicle infrastructure;
- vehicle position forging attacks;
- attacks towards resource-constrained UAV (unmanned aerial vehicle);

Recommender Systems

- shilling attacks;
- injection attacks;

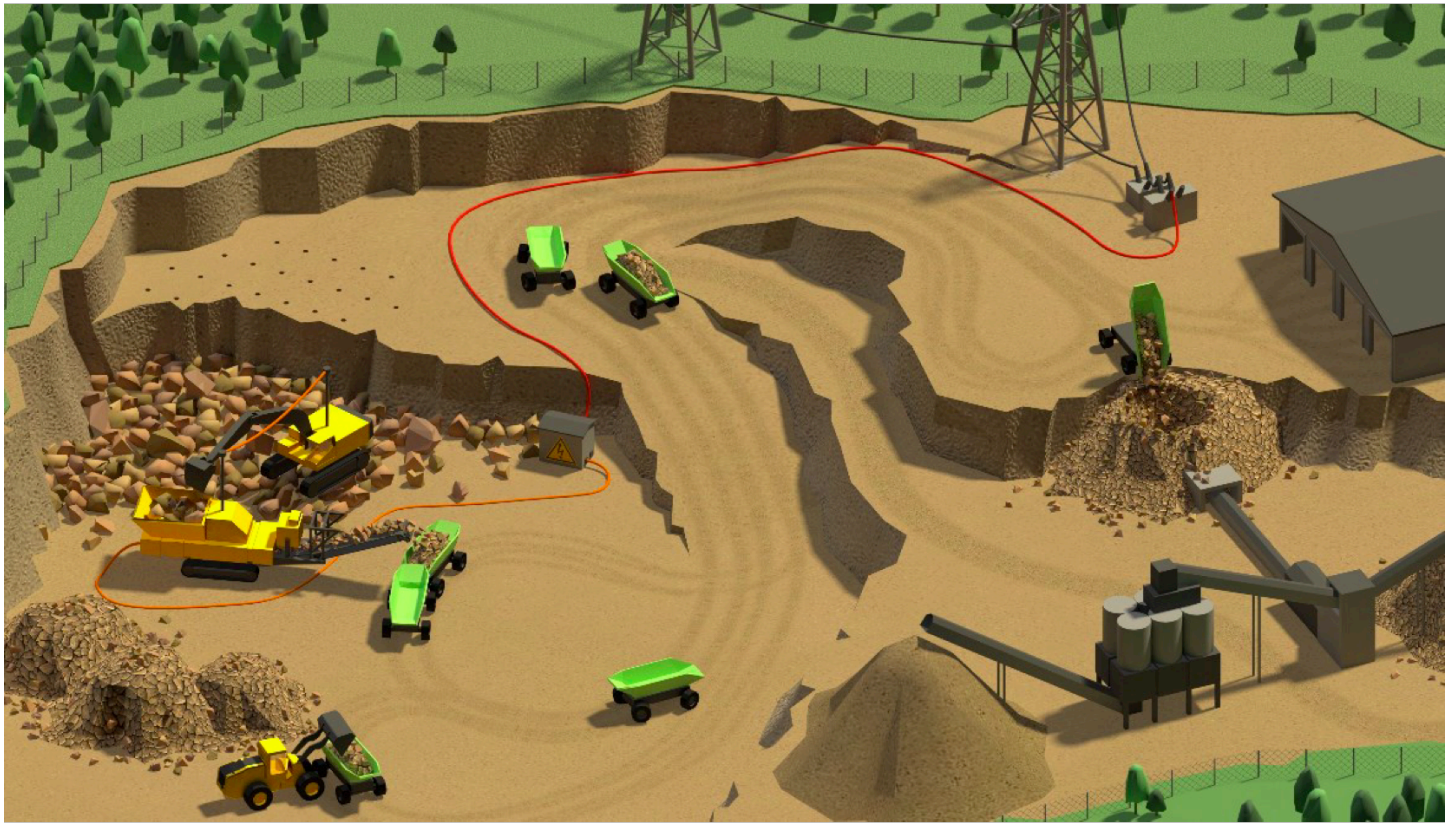
Attack Models

MÄLARDALEN UNIVERSITY
SWEDEN

IoT	❑ related to IoT middleware; ❑ a command disaggregation attack;
Cloud	❑ attacks towards sensitive information; ❑ attacks aligned with stages of using cloud services;
Communications	❑ attacks for different network layers; ❑ DoS attacks; ❑ deception attacks; ❑ attacks targeting HTTP/2 Internet service; ❑ jamming attacks for wireless networks;
RFID	❑ forgery attacks; ❑ replay attacks; ❑ main-in-the-middle attacks; ❑ tracking attacks; ❑ DoS attacks; ❑ eavesdropping and scanning attacks; ❑ attacks focusing of air interface;

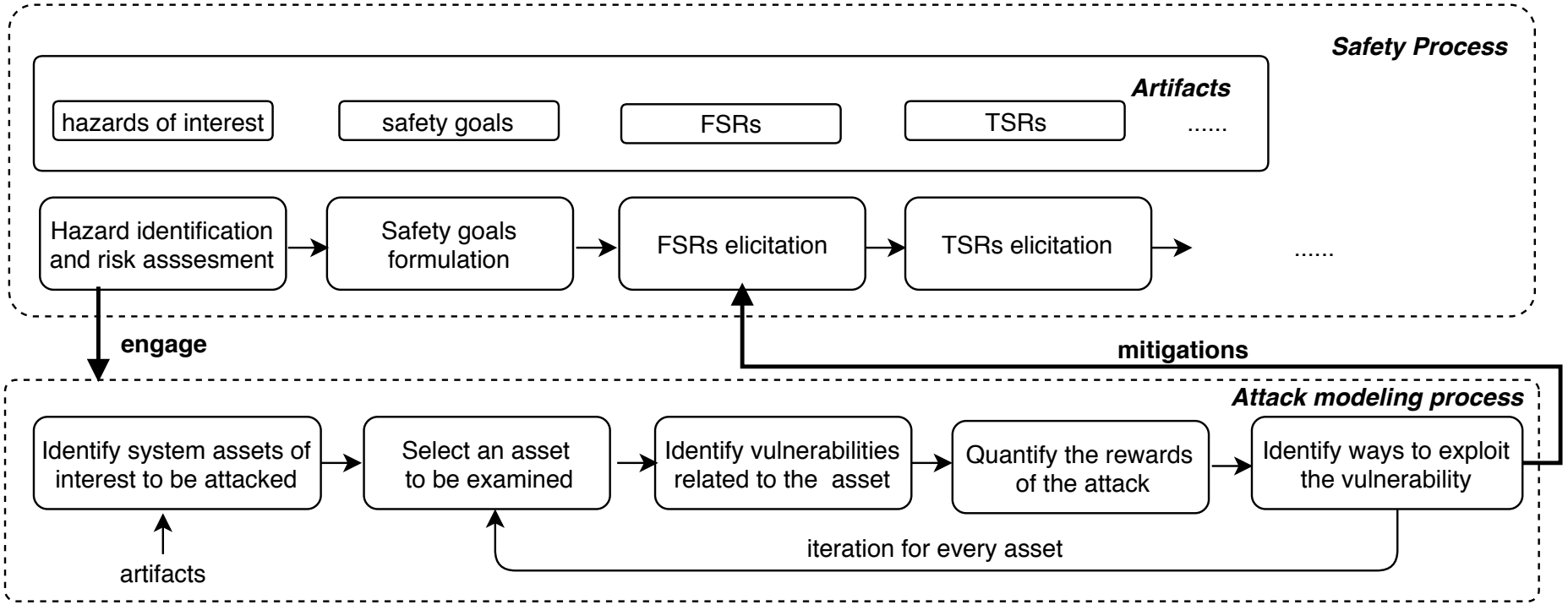
Autonomous Quarry

MÄLARDALEN UNIVERSITY
SWEDEN



Incorporating Attack Models

MÄLARDALEN UNIVERSITY
SWEDEN



Incorporating Attack Models

MÄLARDALEN UNIVERSITY
SWEDEN

Hazards derived following ISO 17757.

Attack model from Wang et al. [2018] focusing on in-vehicle networks.

CAN vulnerabilities that can be exploited:

- weak access control mechanism;
- CAN data frames do not have encryption;
- no authentication in data exchange.

Two scenarios:

- a short-range attack; ← An attacker camouflages as a legitimate user and sends illegitimate control commands in in-vehicle CAN
- a long-range attack. ← An attacker deploys its own malware.

Incorporating Attack Models

MÄLARDALEN UNIVERSITY
SWEDEN

- A1: **a forgery attack** when an attacker communicates with braking system using commands as a legitimate user device or an OBU;
- A2: **a DoS attack** resulting in information blocking by injecting irrelevant data in-vehicle CAN and OBU ;
- A3: **a replay attack** affecting operation of braking equipment by repeating transmitting data to CAN;
- A4: **an eavesdropping attack** resulting in stealing users data and compromising privacy.

- M1: identity authentication and access control;
- M2: data authentication and filtering false information;
- M3: blocking a large number of packets;
- M4: hardware isolation.

Incorporating Attack Models

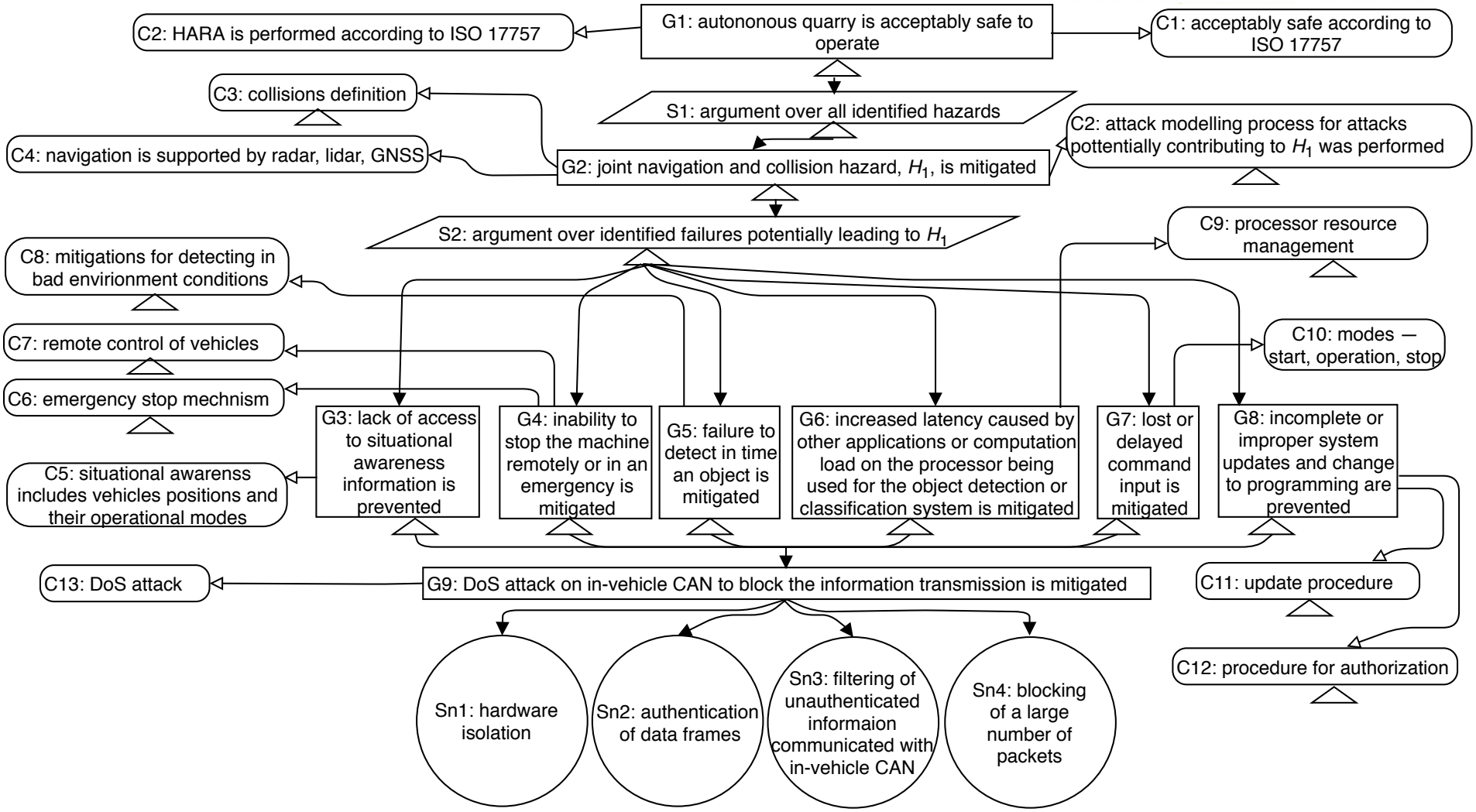
MÄLARDALEN UNIVERSITY
SWEDEN

The navigation and collision hazard due to:

- A2 failures to detect in time an object;
- A1, 2 increased latency caused by other applications or computation load to the processor being used for the object detection or classification system;
- A1 material on the transmitter or receiver erroneously detected as objects;
- A1 erroneous location of a detected object;
- A2 inability to stop the machine remotely or in an emergency state;
- A2 lack of access to situational awareness information;
- A1 inaccurate terrain data;
- A1, 2 lost or delayed command input;
- A1 inaccurate planning information;
- A1 inaccurate position;
- A1, 2 incomplete or improper system updates and changes to software.

Joint S&S Argumentation

MÄLARDALEN UNIVERSITY



Conclusions and Future Work

MÄLARDALEN UNIVERSITY
SWEDEN

- joint assurance and joint consideration of safety and security is getting more and more attention;
- a need to observe a system from an adversary point of view;
- incorporation attacks in argumentation for system safety;
- demonstrated on the example of an autonomous quarry;

- incorporating joint argumentation and attacks models in conjunction for security assurance case

MÄLARDALEN UNIVERSITY
SWEDEN

Thank you!

Questions and Comments?