11TH INTERNATIONAL CONFERENCE
ON CRITICAL INFORMATION
INFRASTRUCTURES
SECURITY

10-12 October 2016
UIC HQ Paris

CRITIS
2016

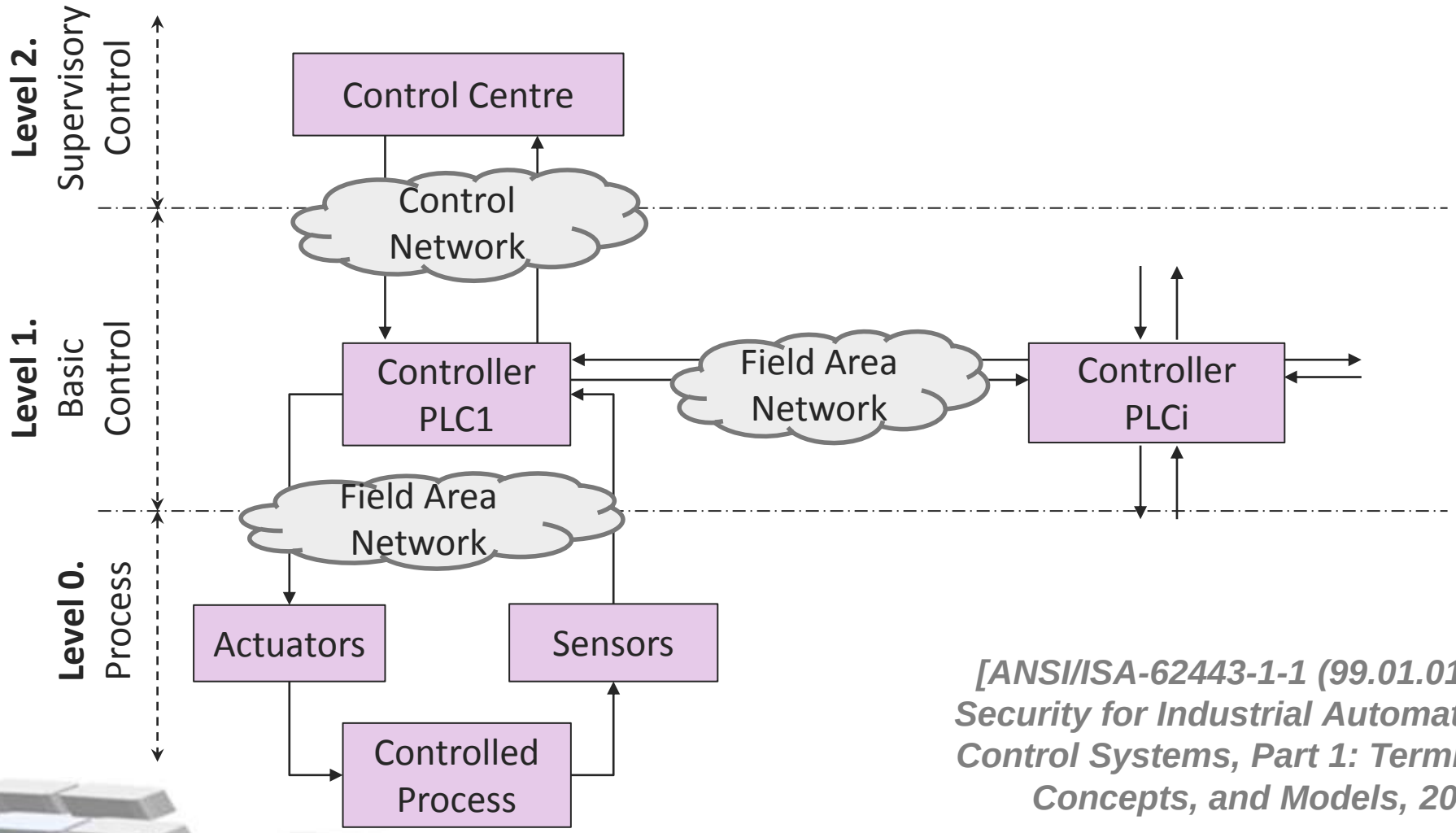
A Six-Step Model for Safety and Security Analysis of Cyber-Physical Systems

Giedre Sabaliauskaite, **Sridhar Adepu**, and Aditya Mathur

Singapore University of Technology and Design

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN
Established in collaboration with MIT

Cyber-Physical Systems (CPS)



[ANSI/ISA-62443-1-1 (99.01.01)-2007 Security for Industrial Automation and Control Systems, Part 1: Terminology, Concepts, and Models, 2007]

CPS Safety and Security

Safety and security are two key requirements of CPSs

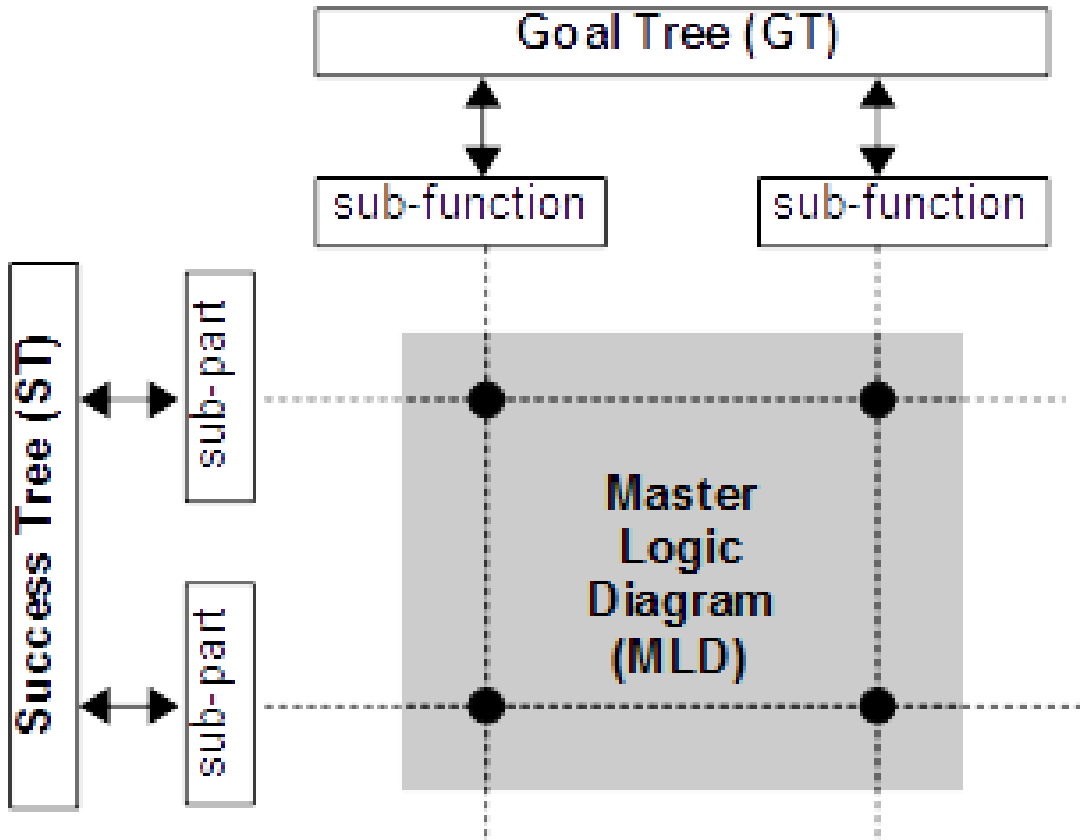
- Safety is concerned with protecting a CPS from accidental failures (safety failures)
  - Failure examples: faulty operation of the computing unit, software failures, compatibility issues, mechanical and electrical failures, etc.
- Security is aimed at protecting CPS from intentional attacks (security failures)
  - Physical attacks
  - Cyber attacks
- Safety and security share the same goal – protecting CPS from failing

Complex System Modelling (1/3)

Most complex systems are formed thr
functional, structural, behaviour, etc.

In 1999, Modarres and Cheon, propos
Success Tree – Master Logic Diagran

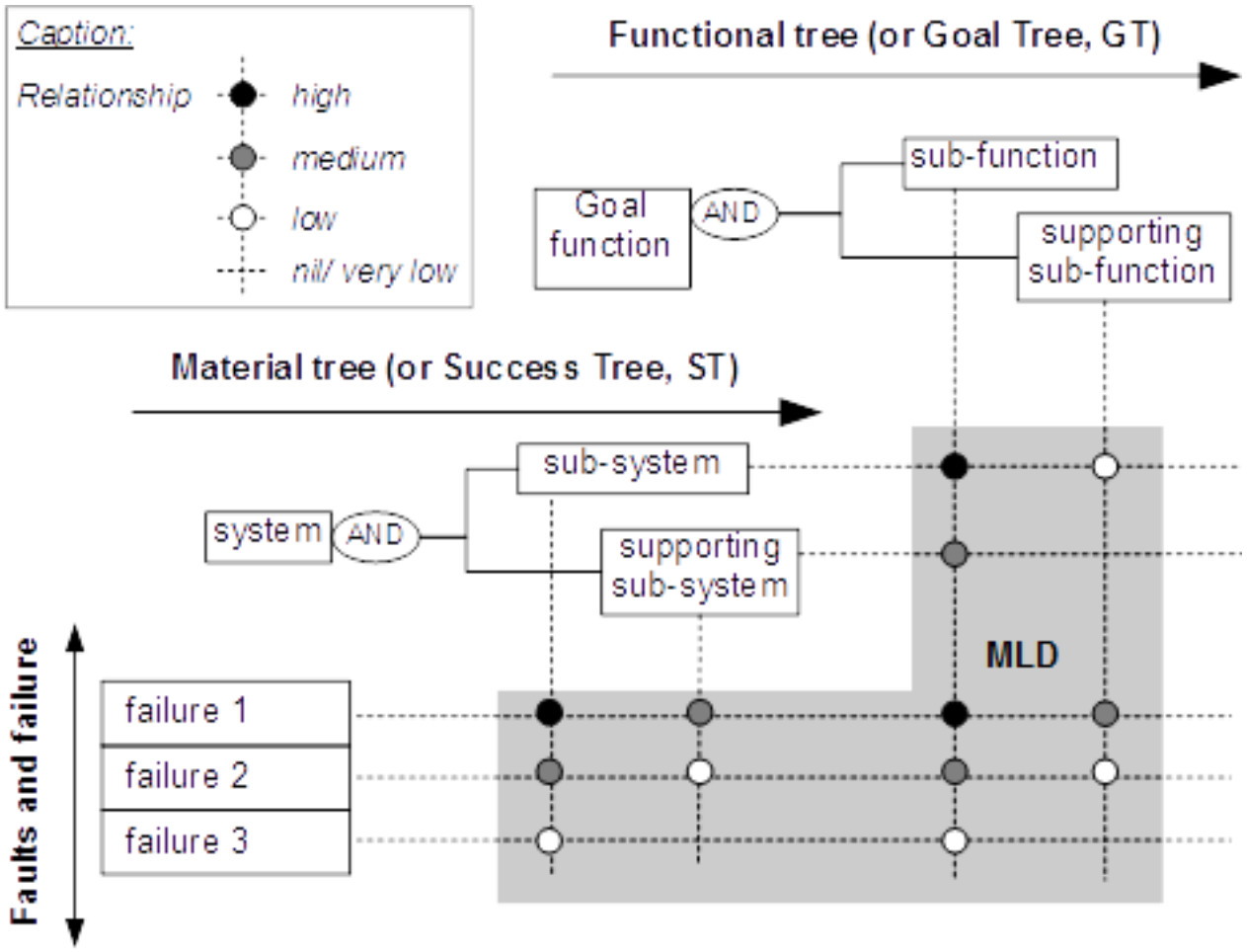
- Goal Tree GT describes system functions
- Success Tree ST – system structure
- Master Logic Diagram MLD – inter-relatic



GTST-MLD [Modarres and Cheon]

Complex System Modelling (2/3)

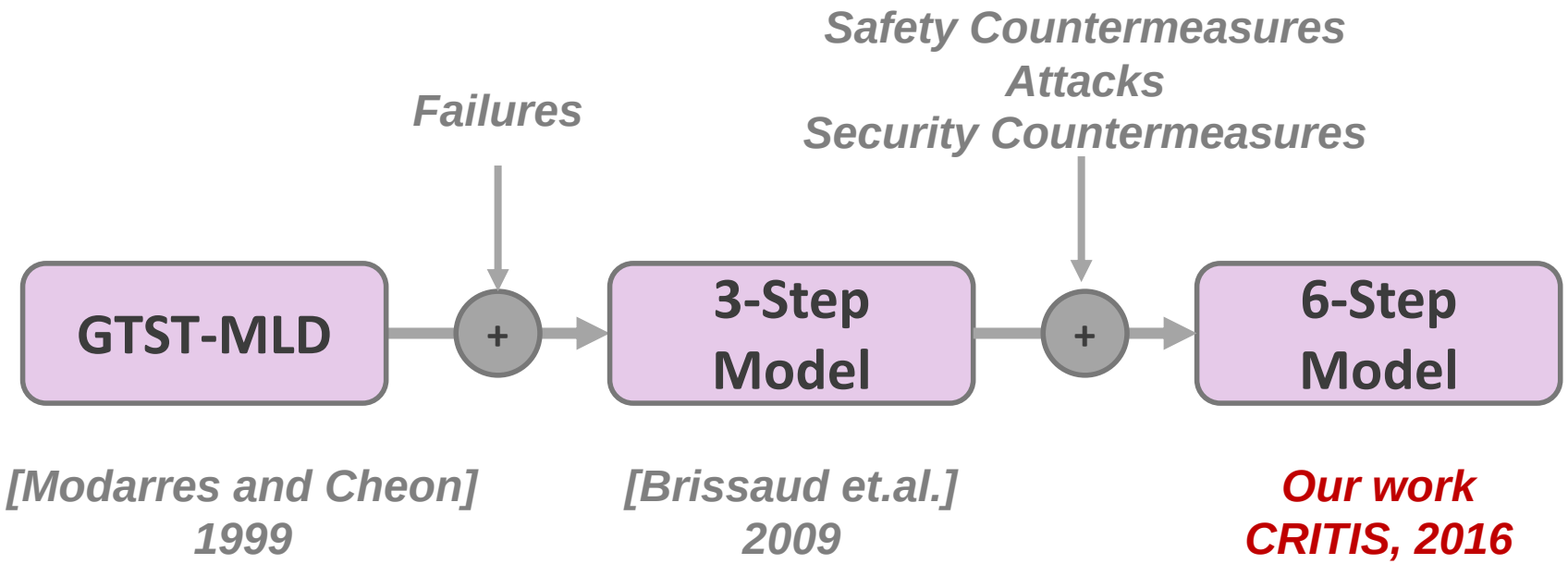
In 2009, Brissaud et al. extend
developed the 3-Step Model



The 3-Step [Brissaud et.al.]

Complex System Modelling (3/3)

In this work, we further extended the 3-Step Model and added safety countermeasures, attacks, and security countermeasures to fit the Cyber-Physical System needs



The Six-Step Model (SSM)

SSM consists of the following six steps:

Step 1. Define Functions

Step 2. Define Structure

Step 3. Identify Failures

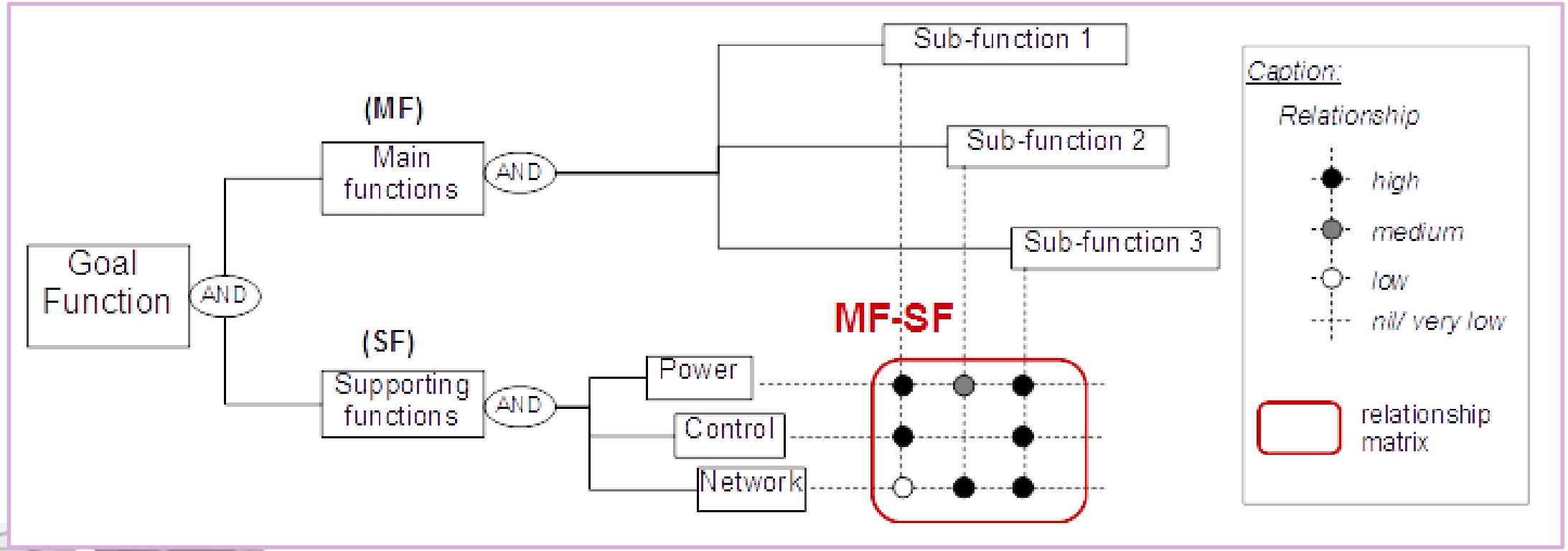
Step 4. Add Safety Countermeasures

Step 5. Identify Attacks

Step 6. Add Security Countermeasures

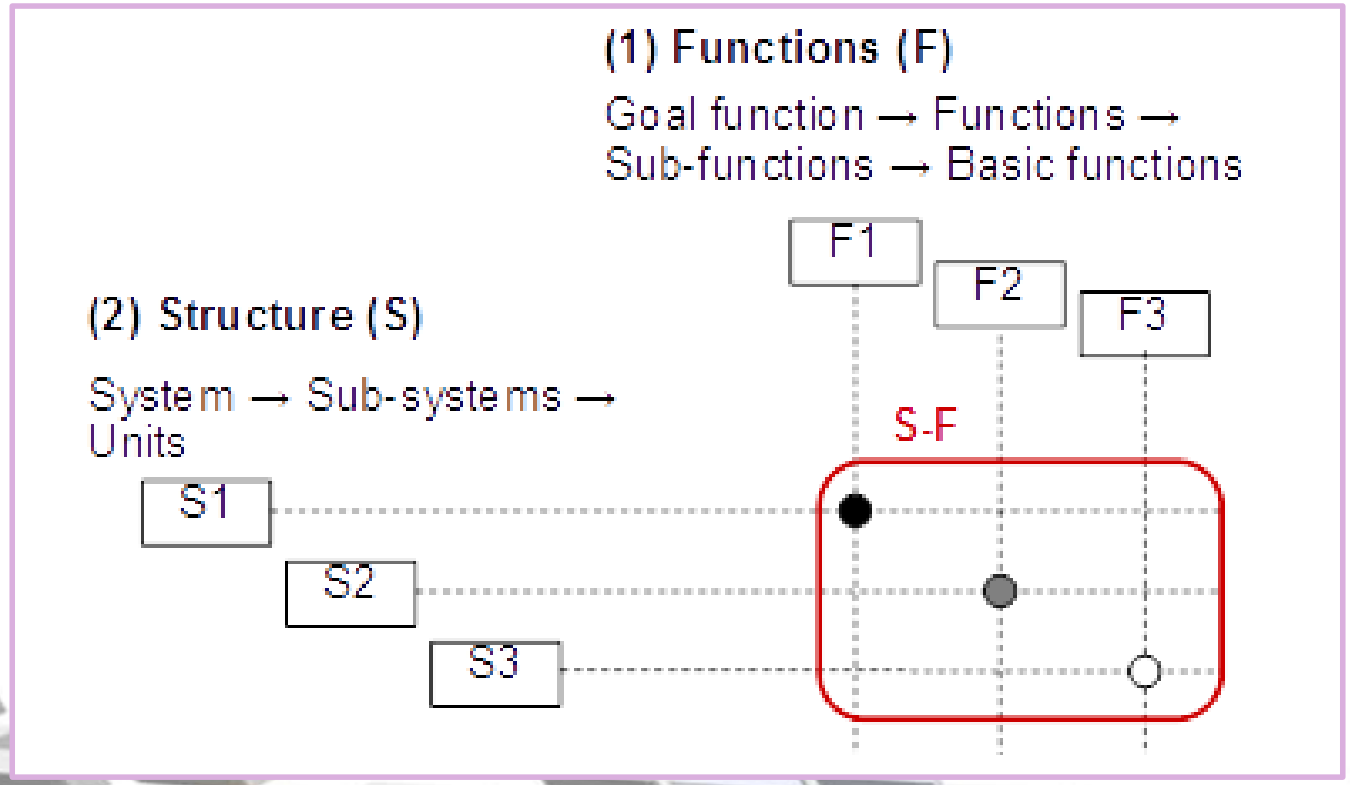
SSM Step 1: Define Functions

- System's goal tree, which includes main and supporting functions, is constructed
- Relationships between the functions are identified (relationship matrix MF-SF)



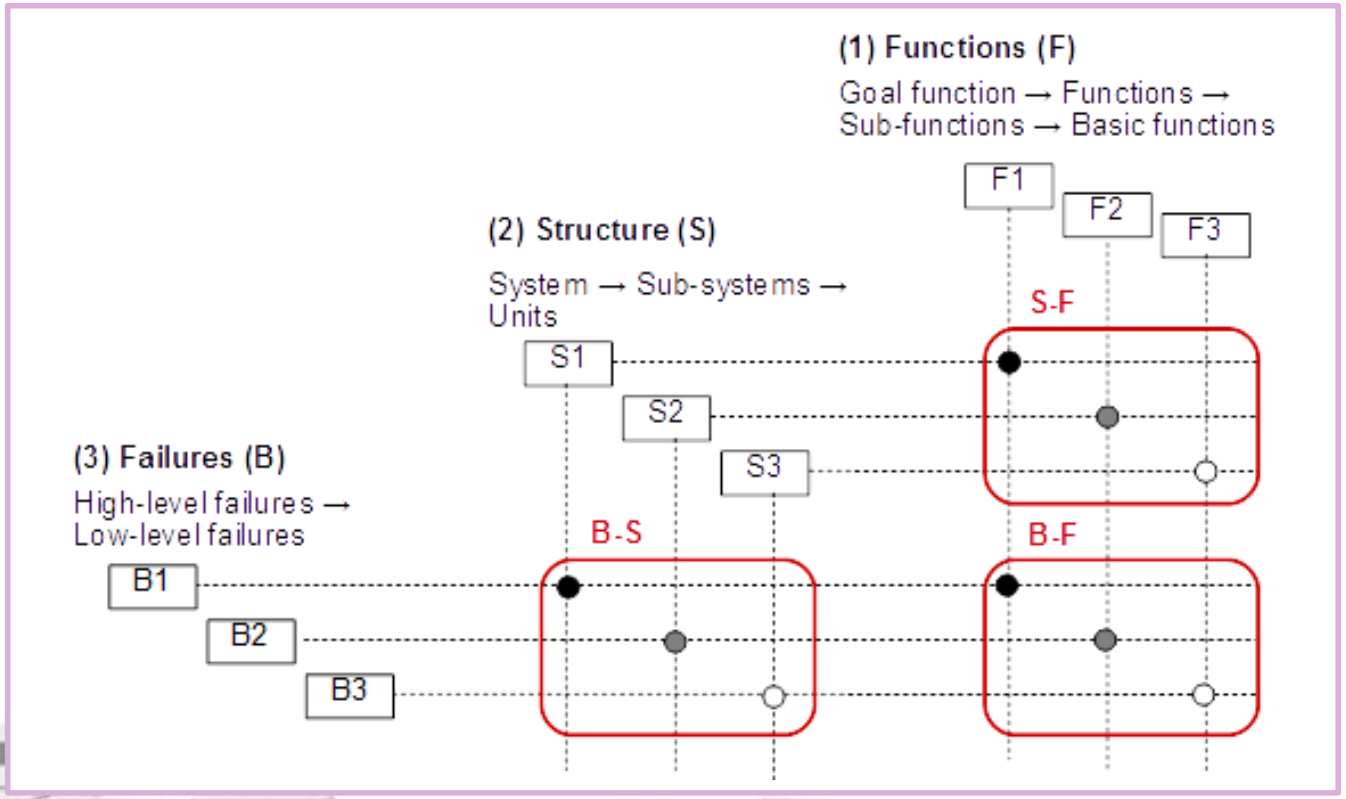
SSM Step 2: Define Structure

- System's success tree, which includes function, sub-functions and units, is constructed
- Relationships between structure and functions are identified (relationship matrix S-F)



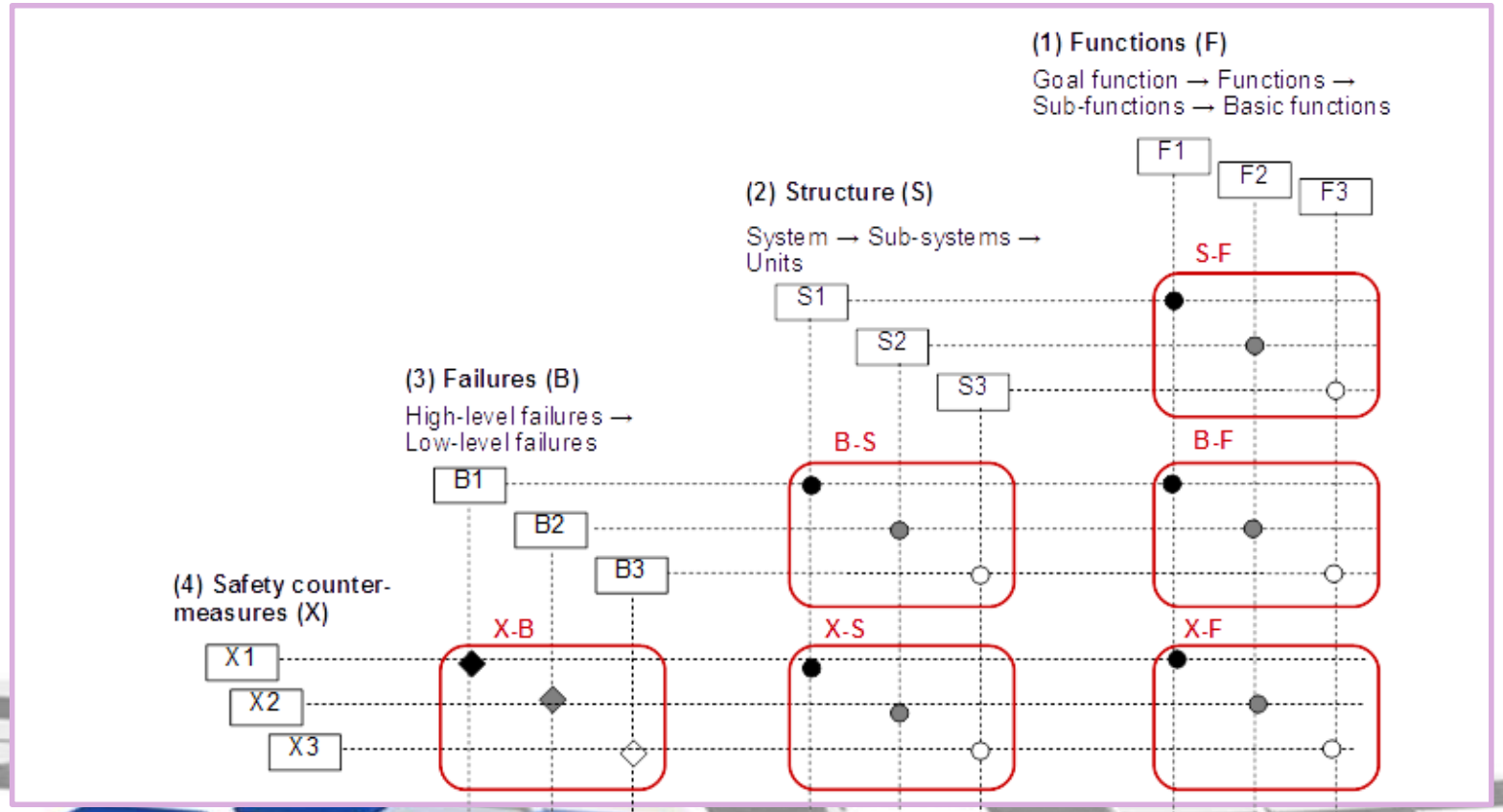
SSM Step 3: Identify Failures

- System's failures are identified and added to the model
- Relationships between failures and system's structure and functions are identified (relationship matrices B-S and B-F)



SSM Step 4: Add Safety Countermeasures

- Safety countermeasures are added to the model
- Relationships between them and the failures, as well as system structure and functions, are defined (relationship matrices X-B, X-S, and X-F)



SSM Step 5: Identify Attacks

- Attacks are added to the model, and their relationships with another elements of the model are identified

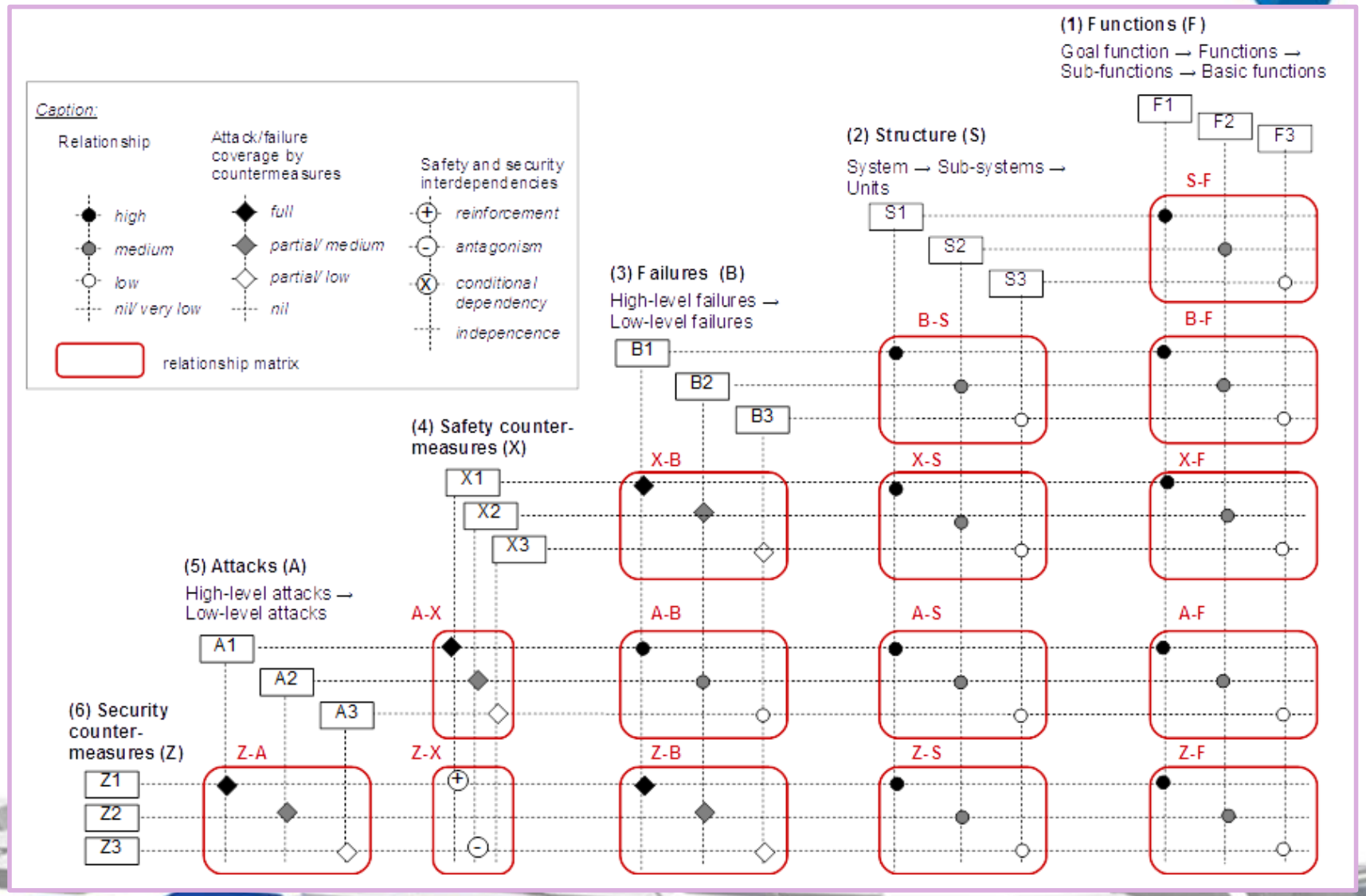
- After completion of step 5, it is necessary to go back to steps 3 and 4 to verify if there are no changes in failures and safety countermeasures due to attacks identified in this step

SSM Step 6: Add Security Countermeasures

- Security countermeasures are added to the model, and the relationships between them and the other elements of the model are identified

- Same as in step 5, after completion of step 6 it is necessary to go back to steps 3 and 4 to verify if there are no changes due to selected security countermeasures

Complete Six-Step Model



SSM case study

- Applied to a realistic testbed.
- Details are in the paper.
- The resulting model was used for cost analysis of alternate measures for safety and security.

Conclusions

The Six-Step Model [SSM] for safety and security modelling of CPS is proposed that:

- incorporates six hierarchies of a CPS: functions, structure, failures, safety countermeasures, cyber-attacks, and security countermeasures,
- facilitates the analysis of their inter-relationships, and
- enables comprehensive analysis of the safety and security of CPSs.

Future Work

Integration of the Six-Step Model with other models, such as Information Flow Diagrams to facilitate identification of failures and attacks, and selection of safety and security countermeasures

Thank You!

CRITIS 2016

Author contact information:

- giedre@sutd.edu.sg
- adepu_sridhar@mymail.sutd.edu.sg
- aditya_mathur@sutd.edu.sg

iTrust
Centre for Research in Cyber Security

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN
Established in collaboration with MIT