THE SECURITY FOR SAFETY PROBLEM IN CYBERPHYSICAL SYSTEMS

Semen Kort, Ekaterina Rudina

Critical Infrastructure Defense, Future Technologies

MOTIVATION

Why this research has to be done

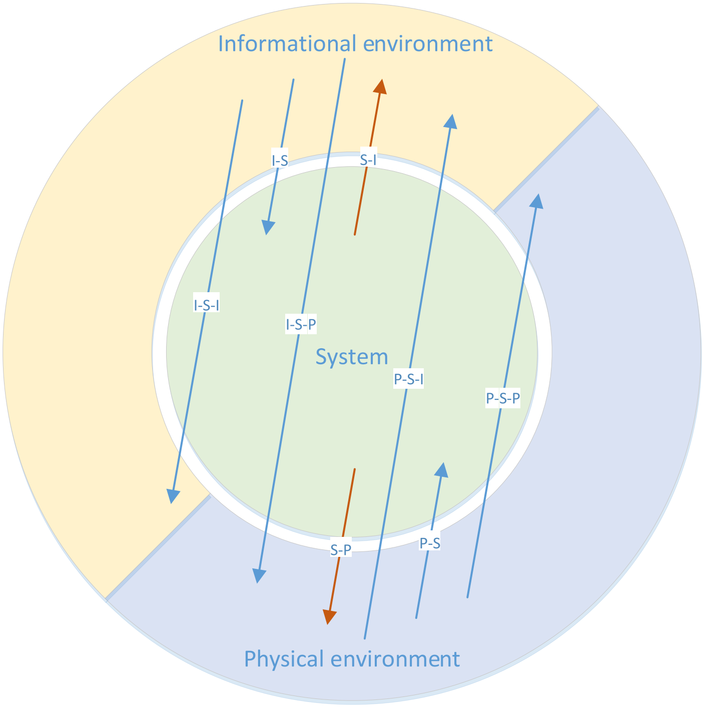
- The continued disputes about the validity of using cybersecurity methods to enhance the safety of cyberphysical systems
- The lack of threat modeling based approaches to Security for Safety assessment
- The need of some formal reasoning on use of MILS findings and recommendations in our current projects related to the cyberphysical systems security

THE GOAL

This research aims to

- Analyze the relations between security and safety in cyberphysical systems
- Perform threat modeling and identify the possible weaknesses in enforcement of security and safety considered together
- Propose an enhanced approach to the security and safety enforcement based on MILS architecture

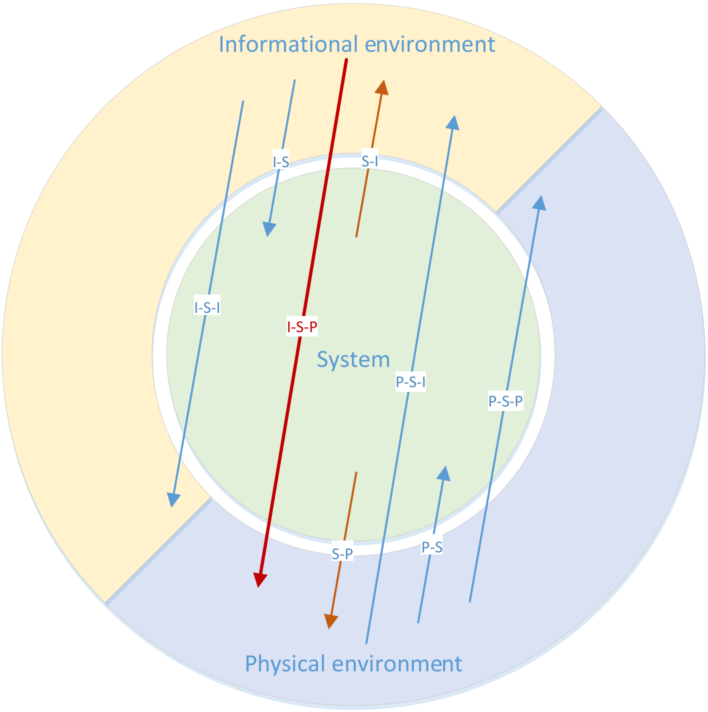
SAFETY AND SECURITY ISSUES IN CYBERPHYSICAL SYSTEMS



- Cyberphysical systems exist in at least two types of environment: the **informational** environment and the **physical** environment.

- Issues may arise from both types of environment and affect physical aspects, informational aspects and the system itself

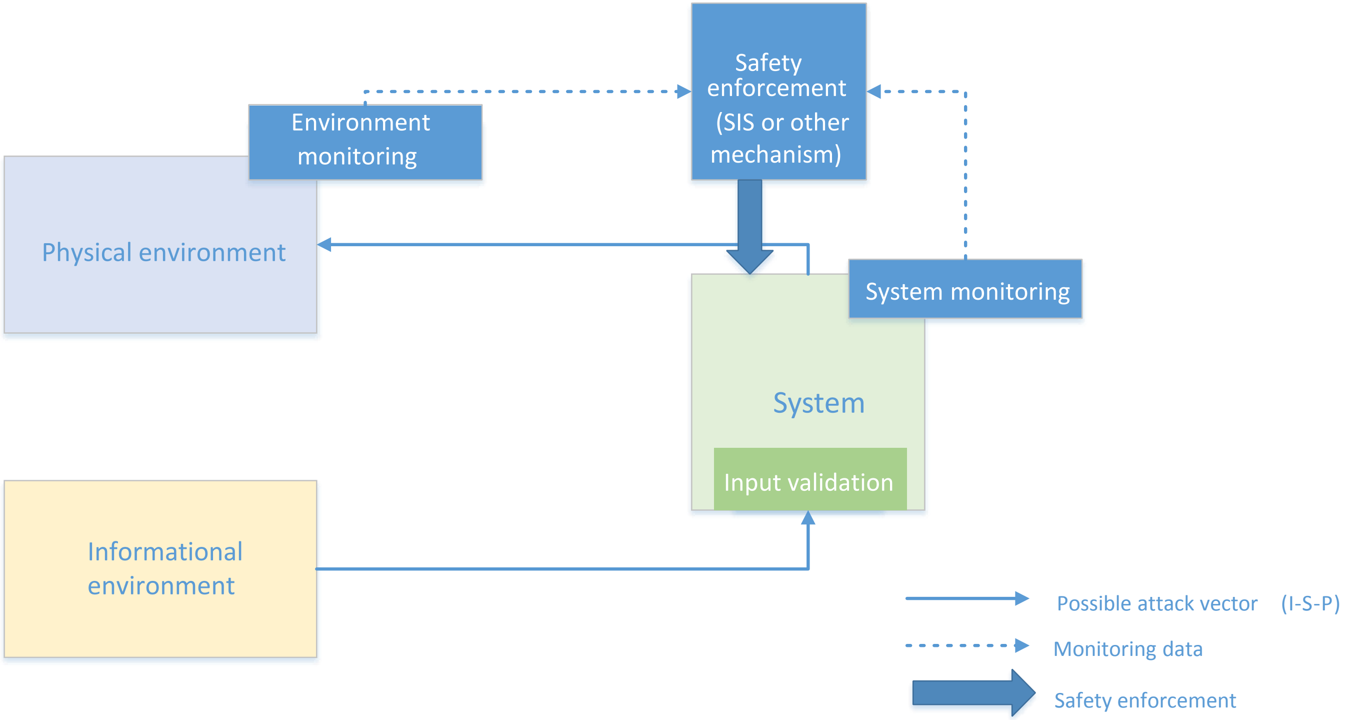
THE PROBLEM IN FOCUS



- The vector **I-S-P** relates to attacks targeting the physical environment of the system

- The problem of protecting against dangerous impacts on system safety caused by cyberattacks – **Security for Safety** (SfS) problem.

SECURITY FOR SAFETY PROTECTION



THREAT MODELING

We apply STRIDE model to identify weaknesses in the Security for Safety protection scheme

Object under attack

- input control, monitoring sensors channels, safety enforcement mechanism and channels

For each object

- Security/Safety assumptions that might not remain true (for each object)
- Defect or vulnerability exploited by attacker
- Possible threats according STRIDE (for each object)
- Prior countermeasures and recommendations

PROPOSED MILS-BASED APPROACH

to provide the solution for the SfS problem

- Proposal #1:

  Implement validation of untrusted external input in a separated MILS domain

- Proposal #2:

  Run monitoring sensors in the dedicated domains

- Proposal #3:

  Do not expose monitoring data to application domains

- Proposal #4:

  Do not expose the safety enforcement mechanism, implement special security measures

- Proposal #5:

  Use dedicated channel(s) to put the system or its components in a safe state

CONCLUSION

The conducted research helps us

- Make determining of significant threats in cyberphysical systems more clear (*by instantiating the I-S-P vector, not by using CIA triad or some other irrelevant concept*)

- Identify the possible weaknesses in our ‘Security for Safety’ solutions

- Reasonably enhance the approach to the security and safety enforcement using MILS architecture principles

LET'S TALK?

Kaspersky Lab HQ
39A/3 Leningradskoe Shosse
Moscow, 125212, Russian Federation
Tel: +7 (495) 797-8700
www.kaspersky.com