Adaptive and Proactive Security Assessment for Energy Delivery Systems

Carlos Rubio-Medrano, Josephine Lamp, Vu Coughlin, Reinhard Gentz, Ziming Zhao, Anna Scaglione, and Gail-Joon Ahn (Arizona State University)

GOALS

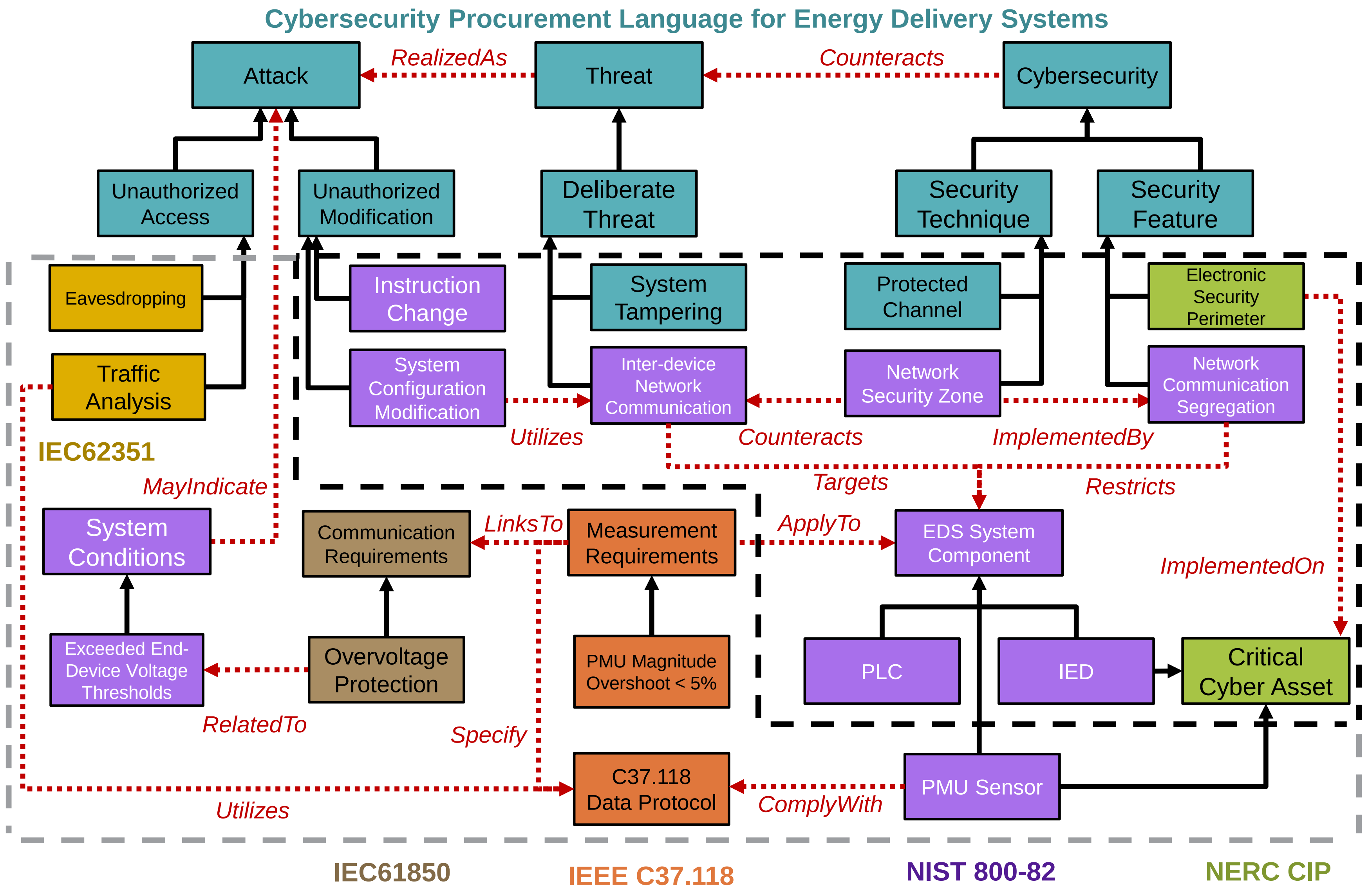
- Evaluate the state of EDS infrastructures through the use of a well-defined set of security requirements.
- Provide means for the efficient monitoring of security-related data, such that effective security assessment of EDS can be achieved.
- Utilize data-based evidence to guide the implementation of new protective measures to handle security incidents.

FUNDAMENTAL QUESTIONS/CHALLENGES

- Introduction of dedicated cyber-infrastructures to EDS has significantly added new security threats, e.g., remote attacks.
- Security requirements are contained within multiple, large, dense, and sometimes conflicting documents, which results in the existence of subjective and non-standard implementations.
- A foundational approach is needed to identify conflicting requirements, identify system anomalies, and detect and respond to violations.

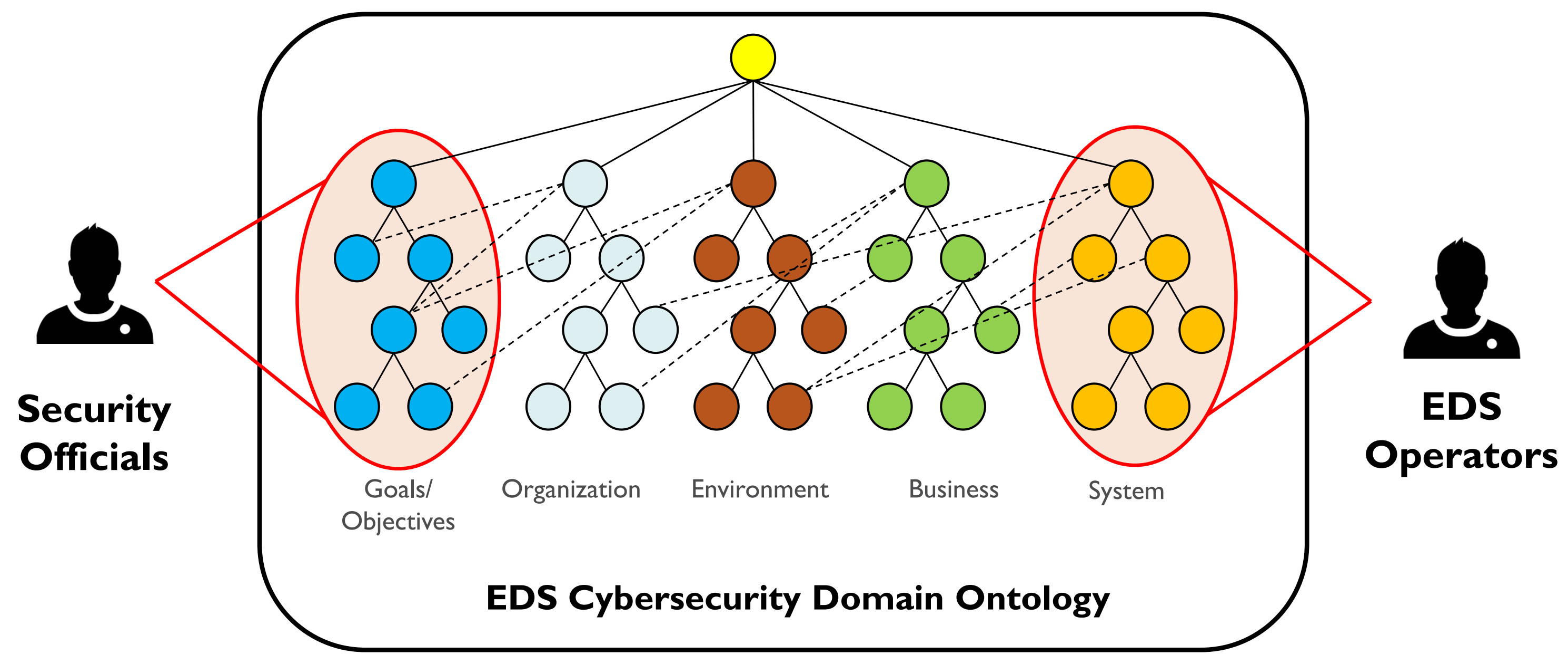
AN ONTOLOGY FOR SECURITY REQUIREMENTS

- Requirements from both cybersecurity and electrical engineering domains, containing different system scopes, focuses, and purposes, are being modeled through ontological representations.
- 7 documents modeled so far, including a total of over 1260 pages in length, ranging in size from 30 to 600 pages each.



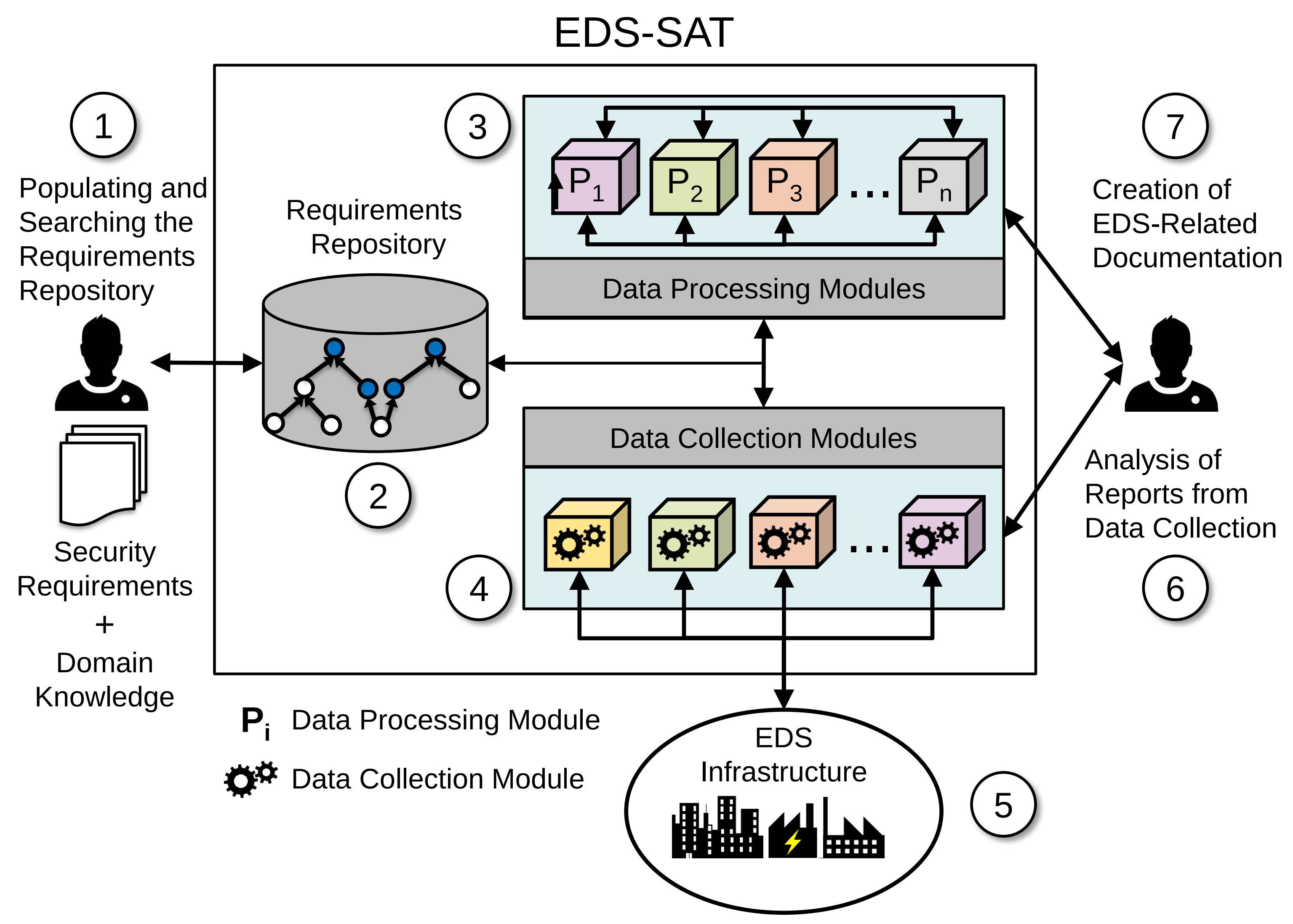
ONTOLOGY EXPLORATION AND ANALYSIS

- We are developing an ontology exploration engine to effectively retrieve security requirements from our proposed ontologies.
- We leverage multi-view analysis to allow for different stakeholders to assess the security of EDS based on their unique viewpoints.
- We also leverage multi-link analysis to retrieve requirements that share common elements by proactively following *links* between ontology entities.



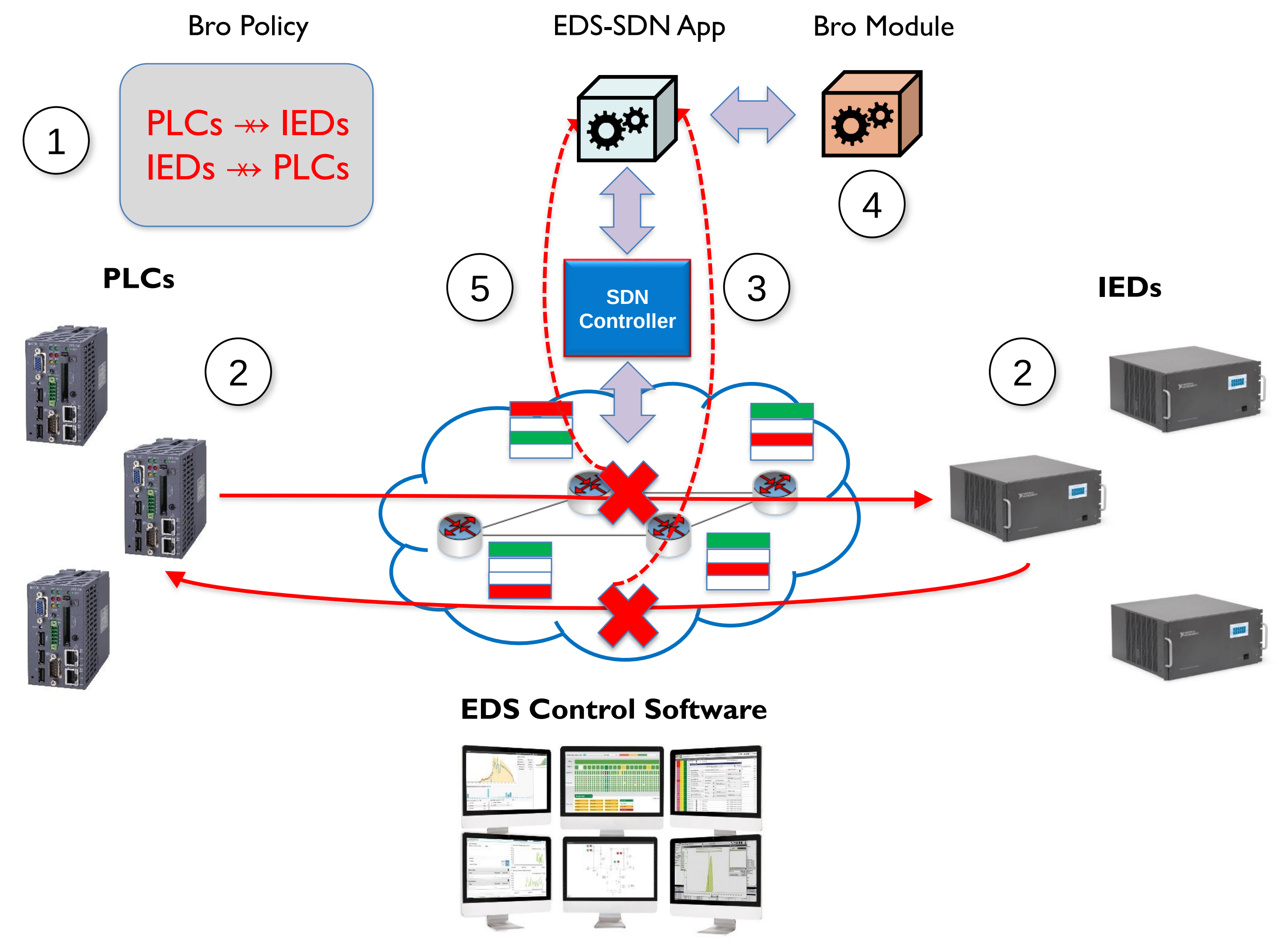
A FRAMEWORK FOR SECURITY ASSESSMENT

- We are currently developing an adaptive and extensible framework for automated monitoring and security assessment, which leverages our ontology engine and consumes data from EDS infrastructures.


EDS-SAT
1
Populating and Searching the Requirements Repository
Security Requirements + Domain Knowledge
3
Requirements Repository
2
P1
P2
P3
…
Pn
Data Processing Modules
Data Collection Modules
4
7
Creation of EDS-Related Documentation
Analysis of Reports from Data Collection
6
Pi Data Processing Module
Data Collection Module
EDS Infrastructure
5

ENFORCING REQUIREMENTS WITH SDN AND BRO

- *Software-defined networks* (SDN) may be leveraged to respond to violations of security requirements expressed as Bro policies.
- This way, not only *offending* packets may be detected, but *on-the-fly* modifications to network flows may deter ongoing attacks.



BROADER IMPACT

- Support for advanced decision making and correcting actions for secure management of EDS.
- Support for the rigorous study of security risks and assessments by means of the simulation, prevention and analysis of attacks.
- Improvement of the public's confidence on mission-critical EDS cyber-infrastructures.

CURRENT AND FUTURE EFFORTS

- We are expanding and enhancing our ontology repository incorporating feedback from both academia and industry.
- We are constructing a chain of toolkits to allow for EDS engineers to develop their own processing modules for better security analysis and decision making.
- We are developing a monitoring and collection infrastructure for both *cyber-based* and *physical* EDS data.

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM | CRED-C.ORG

FUNDING SUPPORT PROVIDED BY THE U.S. DEPARTMENT OF ENERGY AND THE U.S. DEPARTMENT OF HOMELAND SECURITY