Fall 2016

Robust and Scalable Security Monitoring and Compliance Management for Dynamic EDS

Carlos Rubio-Medrano, **Josephine Lamp**, Ziming Zhao and Gail-Joon Ahn

ARIZONA STATE UNIVERSITY

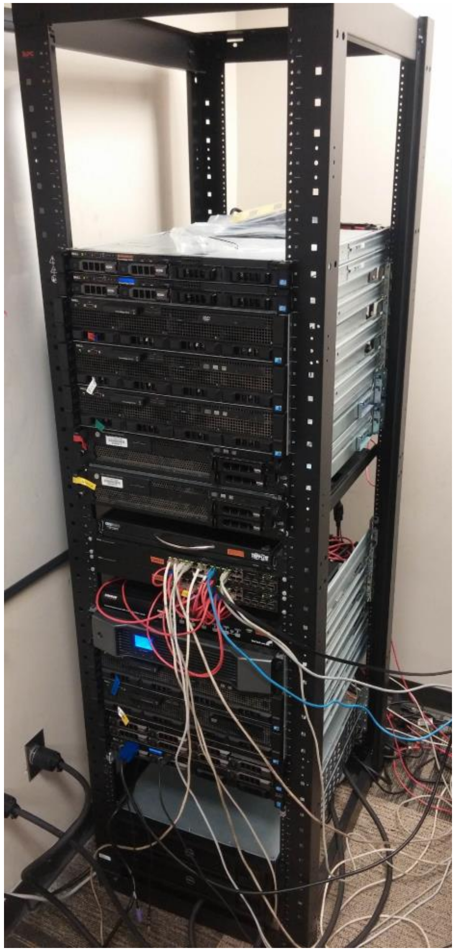
CENTER FOR CYBERSECURITY & DIGITAL FORENSICS

CREDC CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

Background

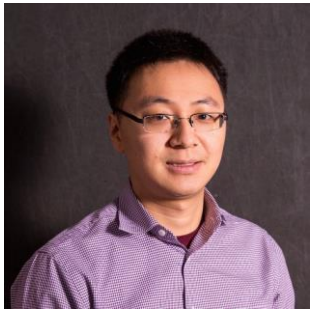
- The Center for Cybersecurity and Digital Forensics at ASU:
  - Identity management and access control,
  - Formal models for computer security,
  - Network and distributed systems security including web, mobile, SDN and cloud computing,
  - Vulnerability, risk assessment and cyber crime analysis
  - Digital Forensics

ASU-CDF Team



Carlos Rubio-Medrano

Josephine Lamp



Dr. Ziming Zhao

Prof. Gail-Joon Ahn

Research Challenges

- Security compliance in EDS gets complicated due to:
  - The distributed, high-interconnected and heterogeneous nature of EDS, e.g., monitoring software, meters, etc.
  - Continuous reconfigurations due to on-demand changes
  - The existence of multiple, large, dense (and sometimes conflicting) documents on security compliance
    - E.g., existence of subjective interpretations, non-standard implementations, and breakdowns among stakeholders

Challenges for Compliance Management

- Compliance as seen by CREDC participants*:
  - Requires considerable organizational effort
  - Does not necessarily advance security: seen mostly as a legal exercise
  - Varies significantly from state to state: adopting standards may not be straightforward
  - Must be addressed since design/installation time
  - Evidence must be collected for audits

CENTER FOR CYBERSECURITY & DIGITAL FORENSICS

* Highlights from Session on Compliance at CREDC Annual Industry Workshop, March 2016

CREDC

Proposed Solution

- We must assess if particular EDS implementations comply with well-defined security requirements
  - Filling in the gap between high-level requirements and *real-world* practical implementations
- We propose a framework for the *verification, validation and attestation* (VV&A) of EDS that is:
  - Automated, well-defined, and configurable (theoretically-justifiable)
  - Systematic (repeatable to validate)
  - Practical (deployable to organizations)
  - Non-intrusive (minor overhead/reconfiguration as possible)

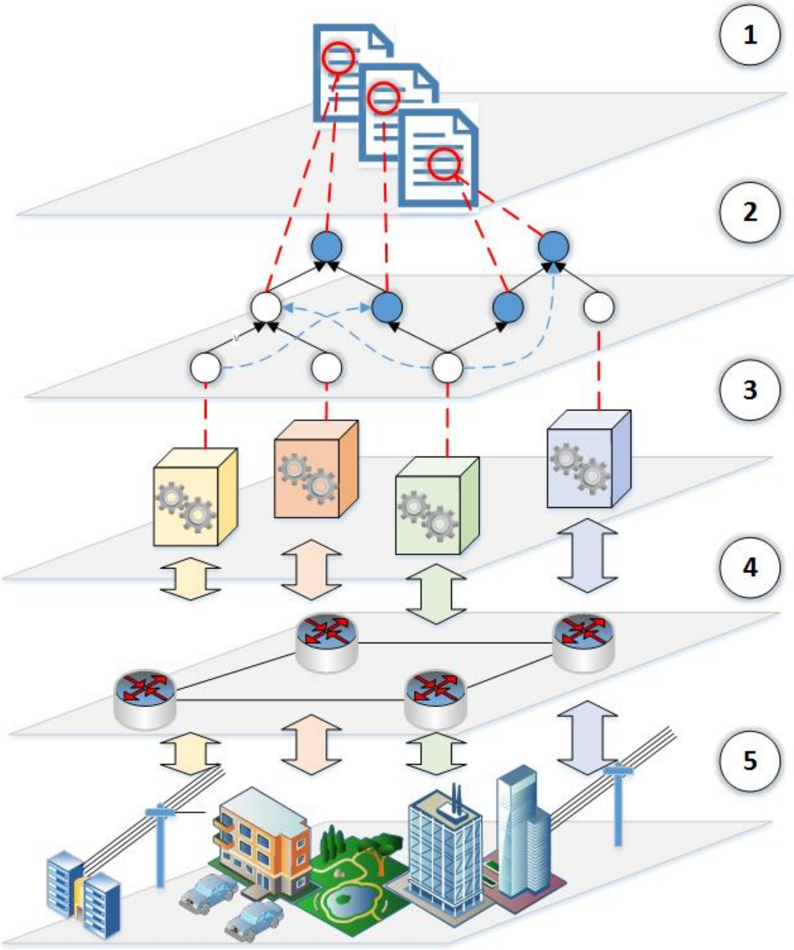
A Security M&C Framework for EDS

1. We gather the most relevant documents on best practices for EDS

2. Next, we obtain a description of such best practices by leveraging ontologies

3. We then introduce software-based modules for automated monitoring and compliance analysis

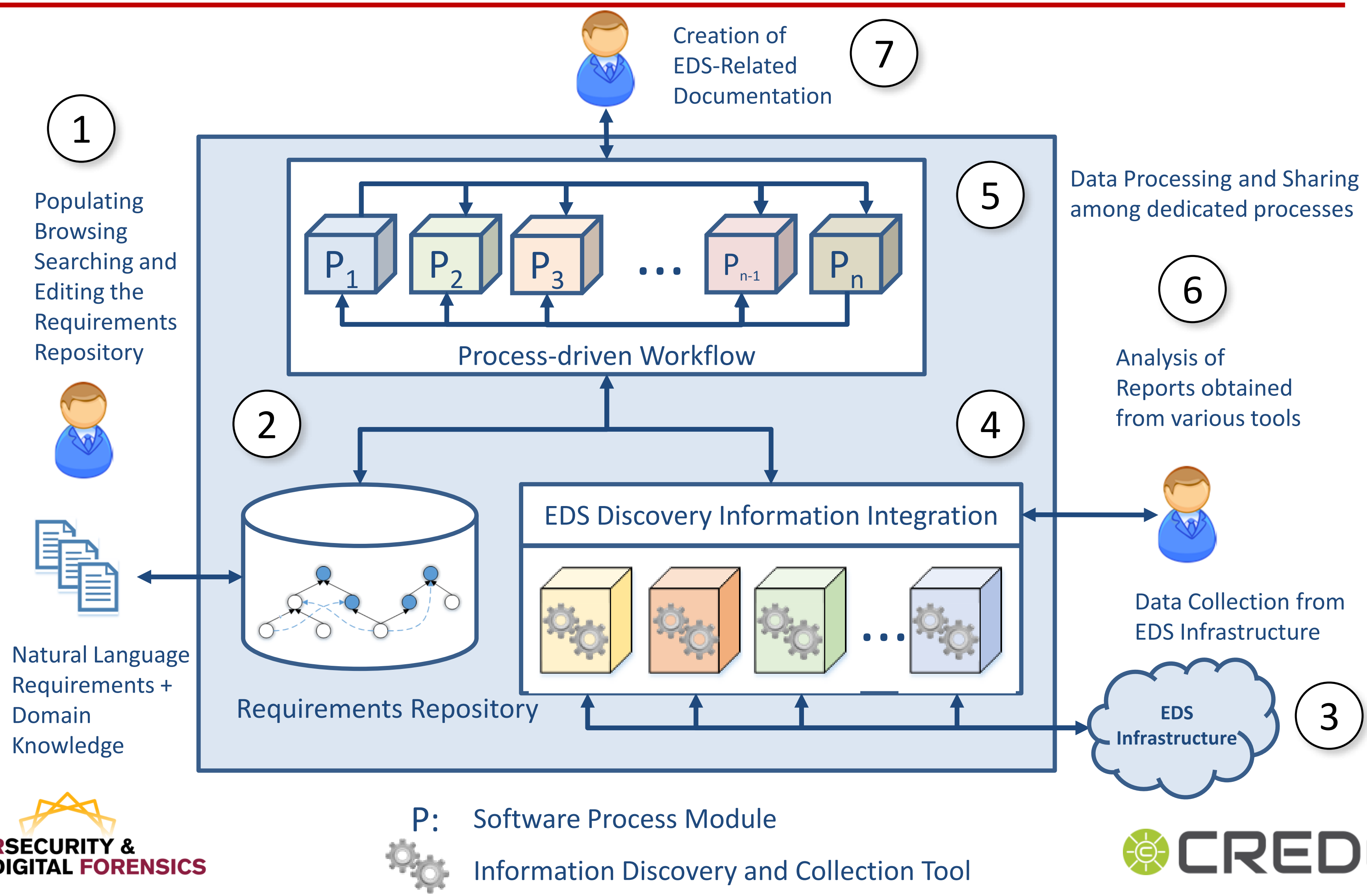
4. Data from EDS infrastructure (5) is collected and forwarded for further processing



CENTER FOR CYBERSECURITY & DIGITAL FORENSICS

CREDC

A Security M&C Framework for EDS (II)



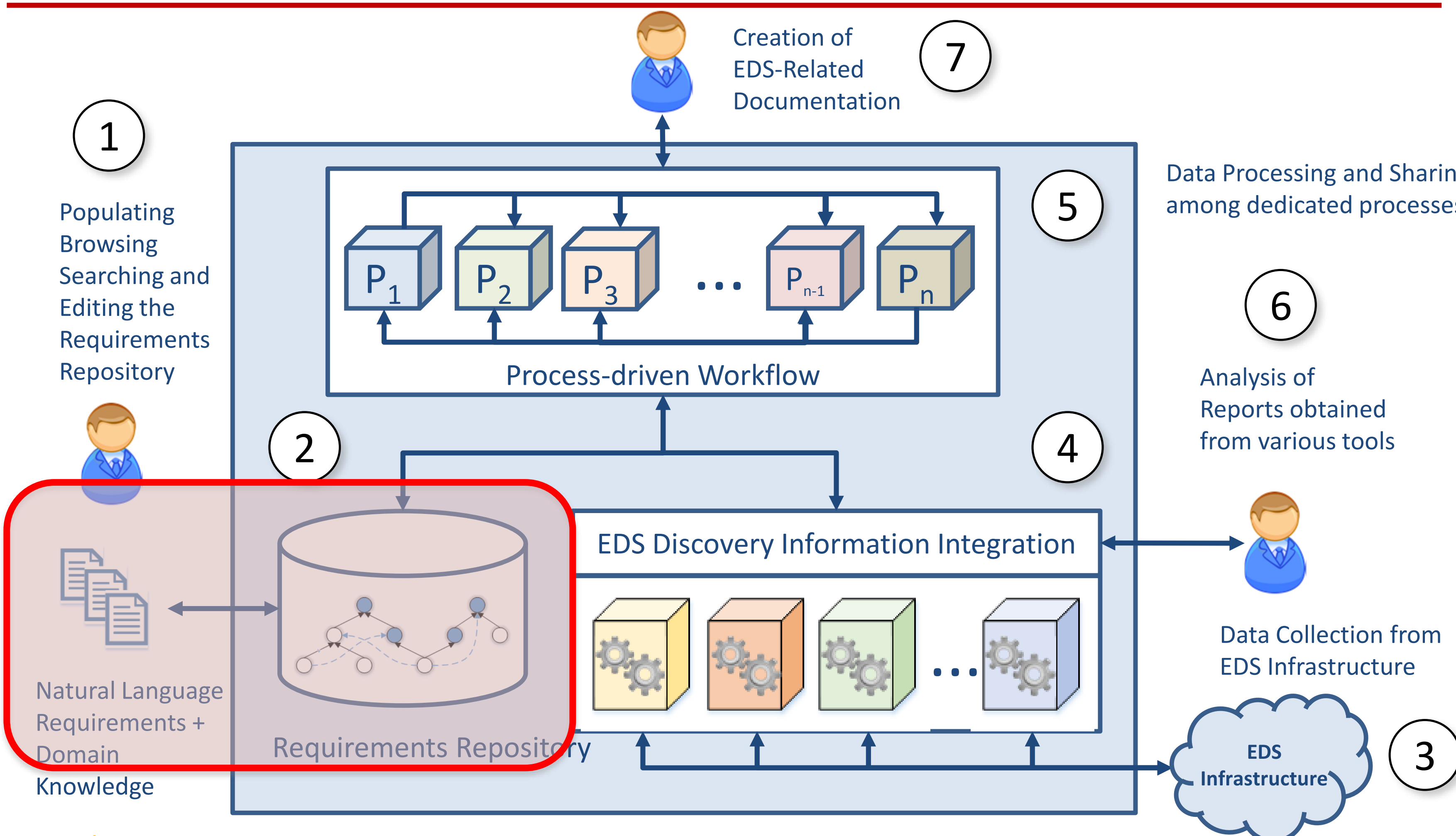
A Security M&C Framework for EDS (III)

- Leveraging our approach involves:
  - Creating dedicated compliance workflows based on analyzing ontology-based requirements
  - Collecting evidence on security-relevant data directly from EDS infrastructure
  - Creating customized processing modules implementing such workflows

A Security M&C Framework for EDS (IV)

- Our proposed framework is intended to:
  - Encourage the rigorous analysis of security requirements by leveraging ontologies
  - Continuously monitor the security of EDS infrastructure by leveraging emerging technologies, e.g., *software-defined networks* (SDN)
  - Automatically perform security compliance checks and management on EDS deployments
  - Promote the development of objective, traceable, justifiable and repeatable security metrics and measures for EDS

A Security Framework for EDS: Requirements



P: Software Process Module

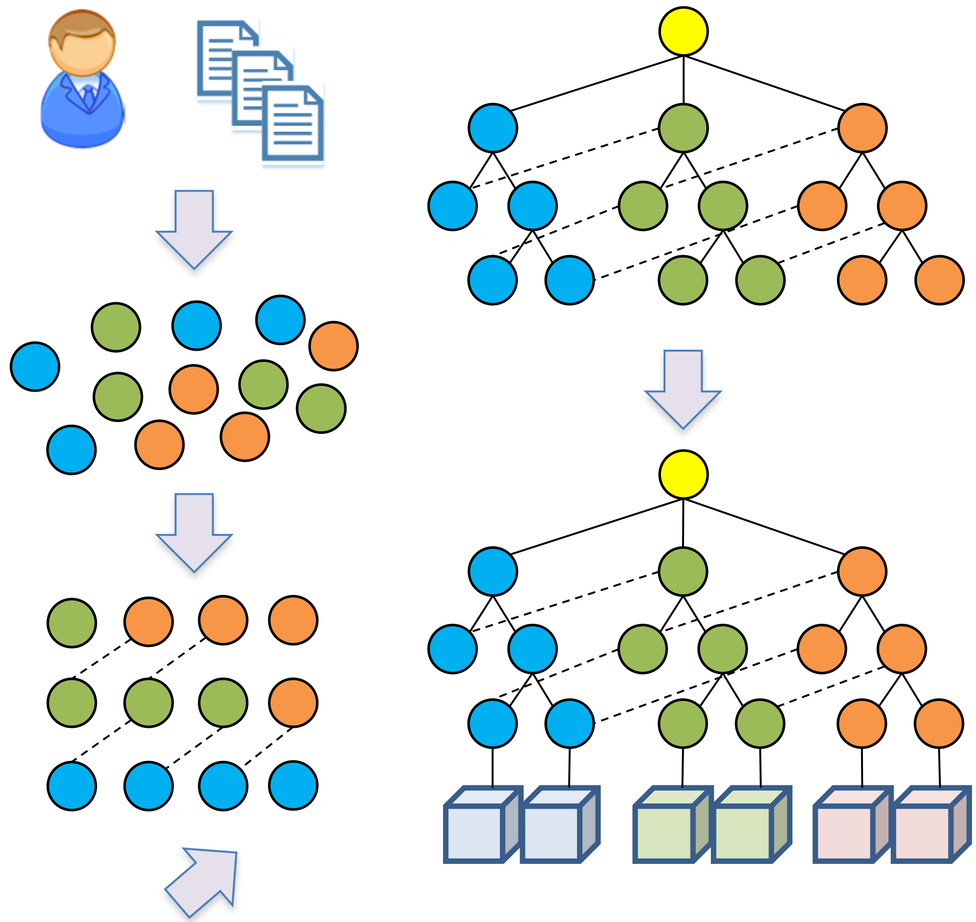
Information Discovery and Collection Tool

Ontology Representation: Onto-ArcRE*

1 Document Gathering: NIST, IEEE, etc.

2 Identification of Requirements, Stakeholders, Security controls, etc.

3 Classification and Categorization of Concepts and their relationships



4 Hierarchical grouping on common characteristics

5 Creation of monitoring / compliance tools

Center for Cybersecurity & Digital Forensics

*Lee SW and Gandhi RA. *Ontology-based active requirements engineering framework*. APSEC'05. 2005. IEEE.

CREDC

Ontology Representation: Example

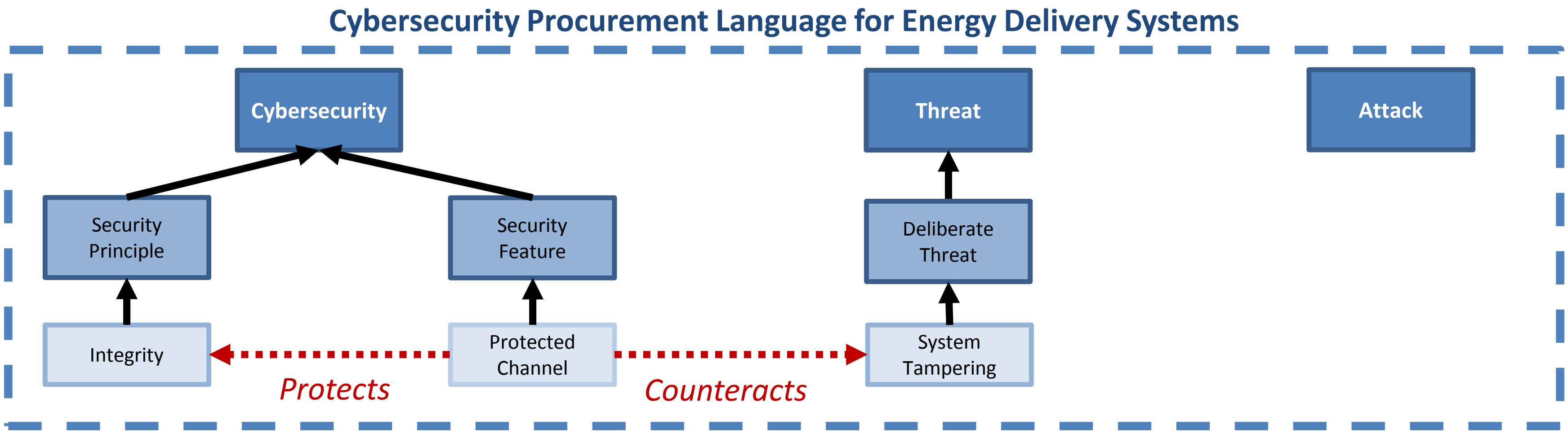
- *Communication channels must be secured:*
  - Security Principles: Integrity[1]
  - Security Threat: System Tampering[1]
  - Attack Vector: Network Communications[1,2]
  - Attacks: Intercept, Man in the Middle, Masquerade[3]
  - Security Features: Protected Channel[1]
  - Security Techniques: Secure Sockets Layer (SSL)[4]
  - EDS Infrastructure: MTU, IED, RTU[4]

1) Cybersecurity Procurement Language for Energy Delivery Systems
2) NERC CIP-005
3) IEC62351
4) NIST SP 800-82

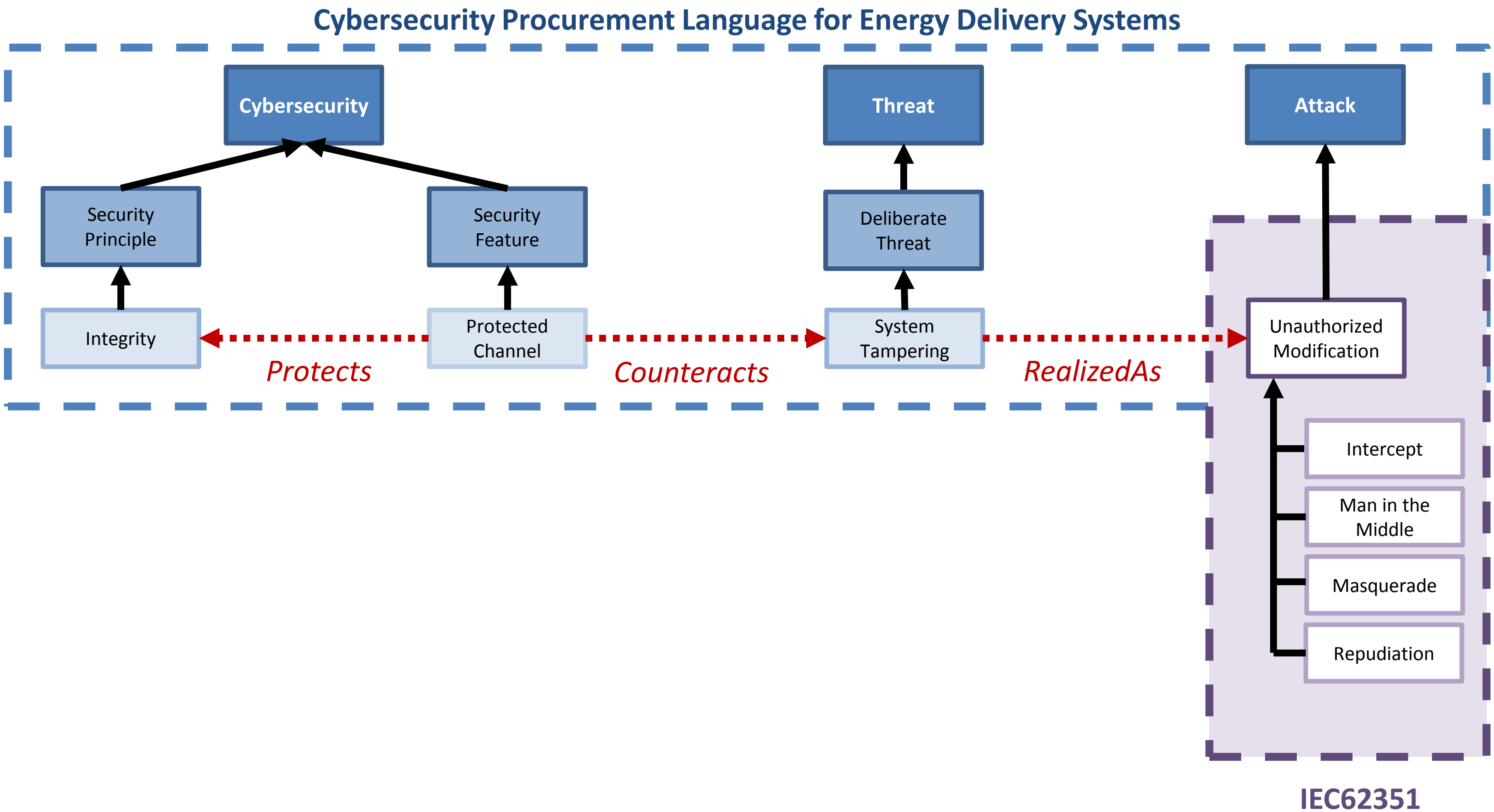
CENTER FOR CYBERSECURITY & DIGITAL FORENSICS

CREDC

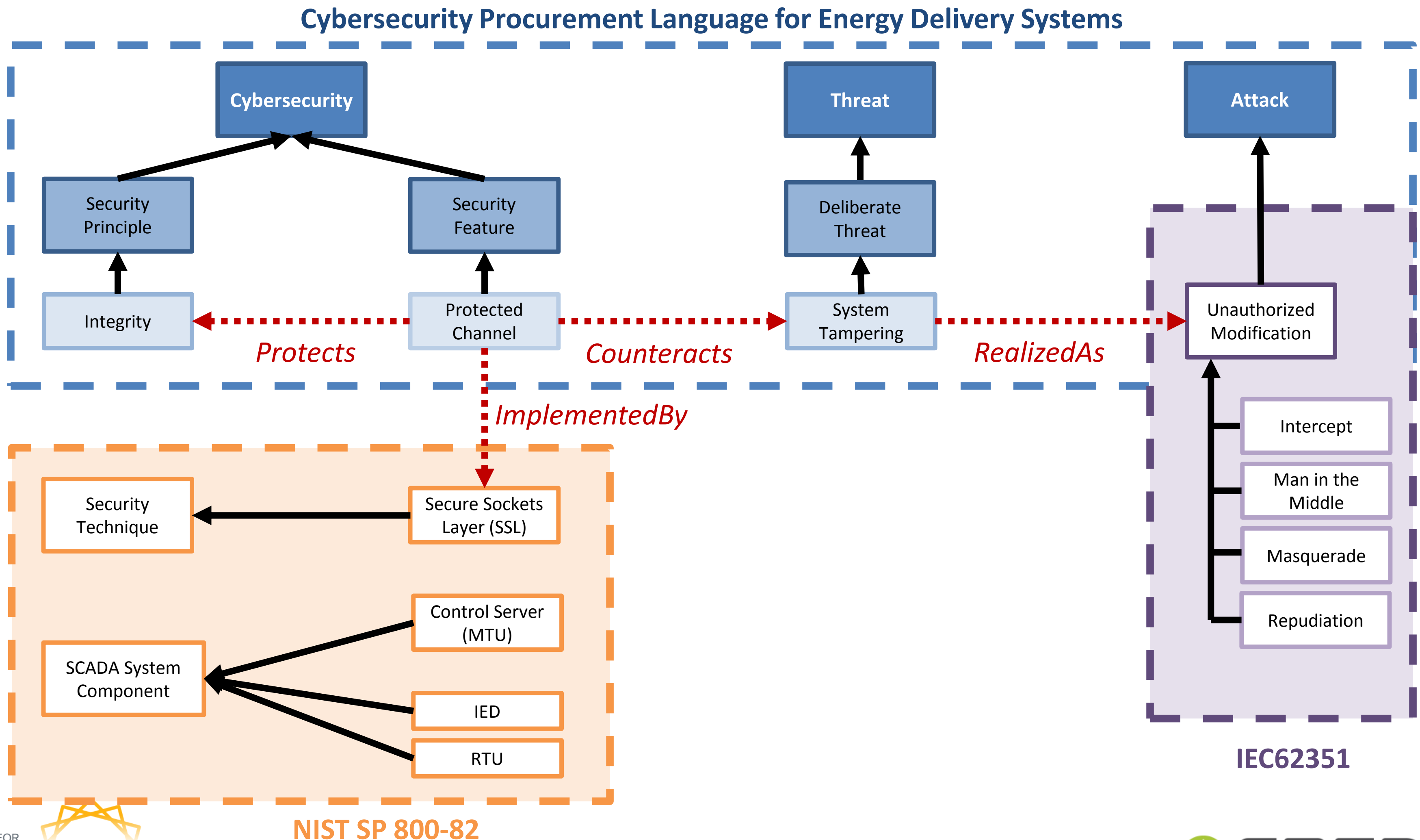
Ontology Representation: Example (IV)



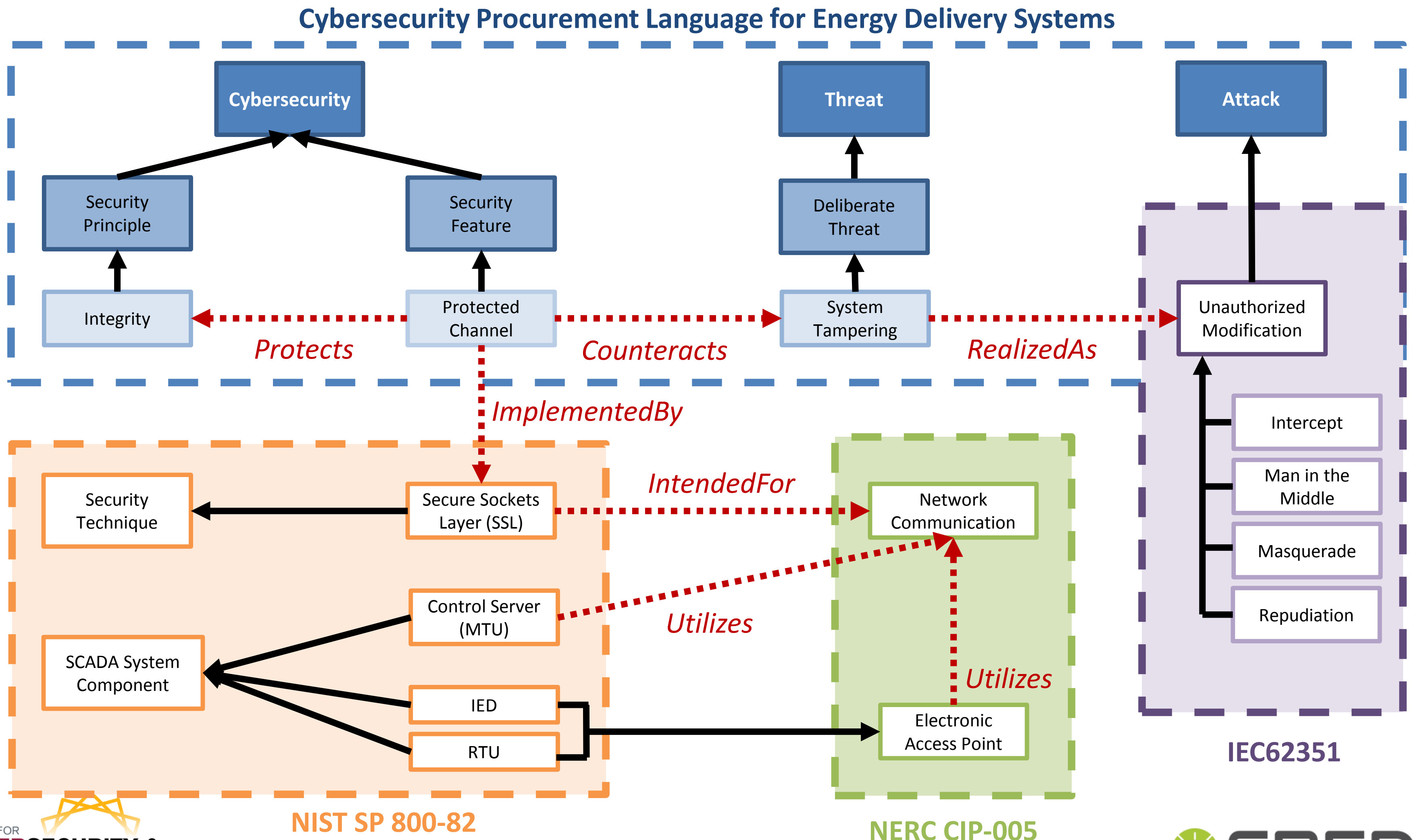
Ontology Representation: Example (IV)



Ontology Representation: Example (IV)



Ontology Representation: Example (IV)



SPARQL Query – Security Principle

```
SELECT ?secTech ?prnpl
WHERE
{
   eds:protectsIntegrity
rdfs:domain ?secTech ;

   rdfs:range ?prnpl.
}
```

SecurityTechnique	Principle
Access Control	Integrity
Credentials	Integrity
DMZ	Integrity
Encryption	Integrity
Firewall	Integrity
NetworkMonitoring	Integrity
PKI	Integrity
SSL	Integrity

SPARQL Query – Documentation

```
SELECT ?secTech ?doc
WHERE
{
   eds:specifiedBy
rdfs:domain ?secTech ;

   rdfs:range ?doc.
}
```

SecurityTechnique	Principle
Access Control	CyberProc Lang
Credentials	NIST800-82
DMZ	CyberProc Lang
Encryption	NERC_CIP
Firewall	IEC62351
NetworkMonitoring	IEC62351
PKI	NIST800-82
SSL	NIST800-82

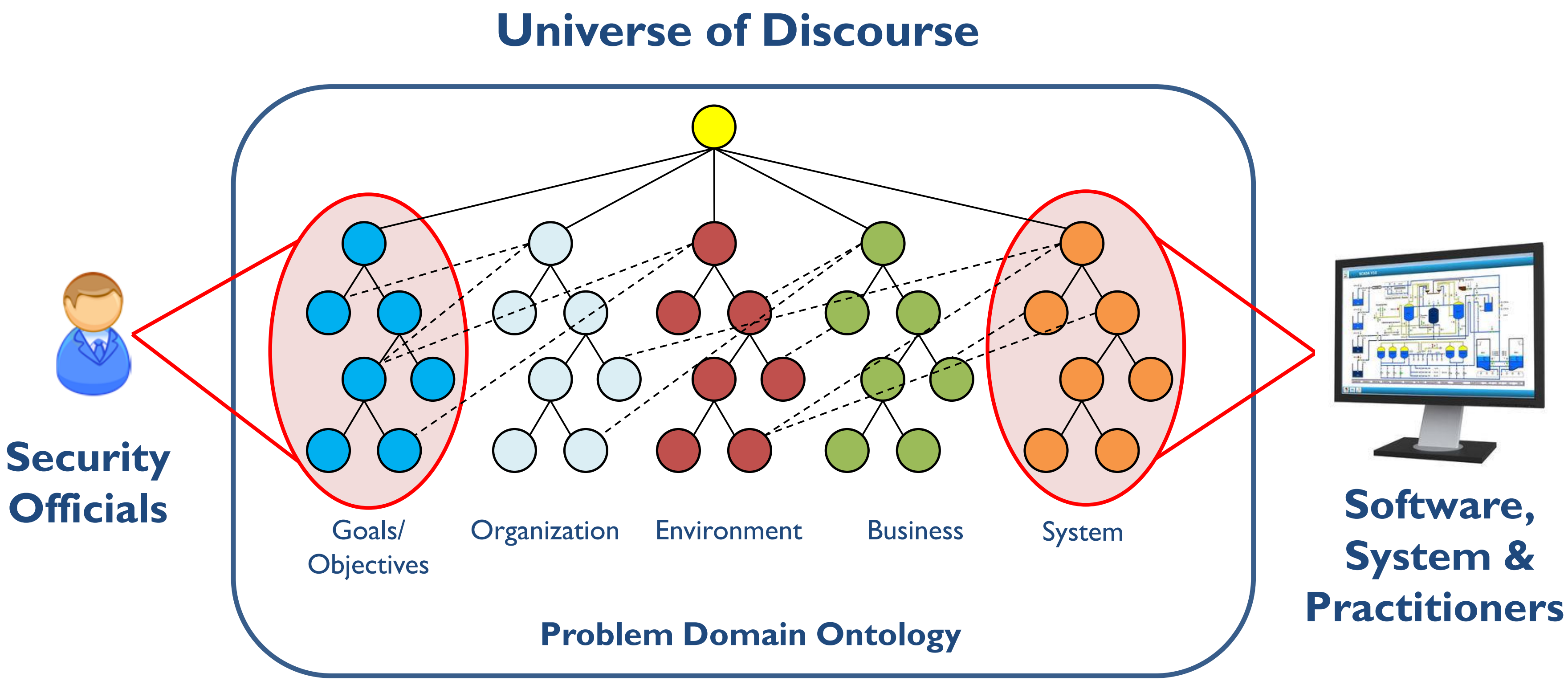
SPARQL Query – Properties

```
SELECT ?attack ?property ?sysComp
WHERE
{
  ?property rdfs:domain+ ?attack ;
            rdfs:range+ ?sysComp .
  eds:Attack (^rdfs:domain/rdfs:range)* ?attack .
  ?attack (^rdfs:domain/rdfs:range)* ?sysComp .
}
```

SPARQL Query - Properties

Domain	Property	Range
ControlBypass	targets	MTU
PrivilegeEscalation	targets	AccessControlMech
ManInTheMiddle	targets	RTU
Intercept	targets	NetworkComm
Masquerade	targets	IED
TrafficAnalysis	targets	NetworkTraffic
Repudiation	targets	Software
Virus	targets	Application

Ontology Representation: Onto-ArcRE*



*Lee SW and Gandhi RA. *Ontology-based active requirements engineering framework*. APSEC'05. 2005. IEEE.

Ontology Representation: Benefits

- Well-defined: provide an unambiguous representation of requirements knowledge depicting *common vulnerabilities and exposures* (CVEs) * synthesized cohesively

- Multi-dimensional: represents multiple dimensions and viewpoints, i.e., relevant information for engineers vs vendors

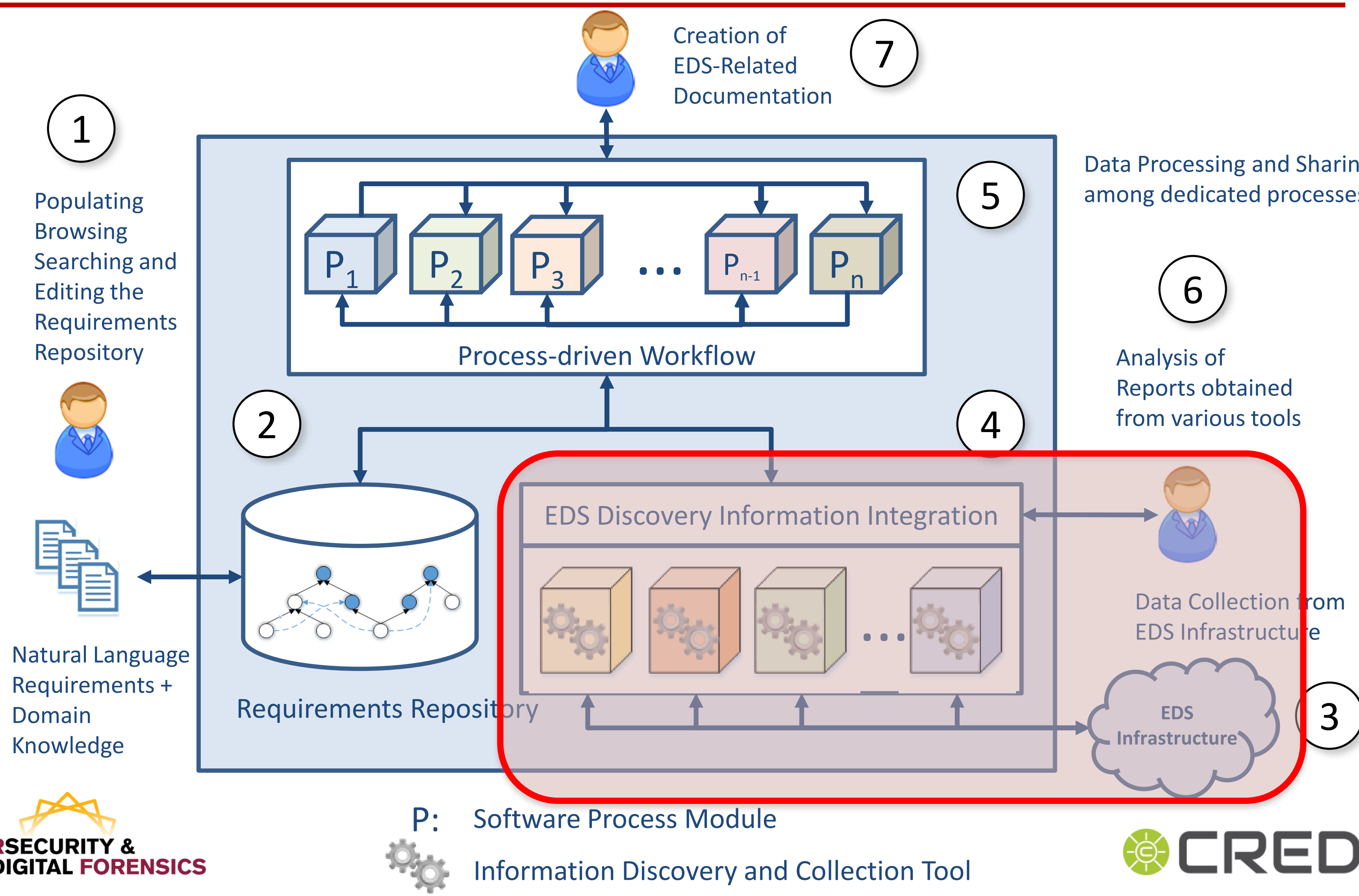
- Link analysis: identifies interdependencies, missing and conflicting information among diverse knowledge sources

CENTER FOR CYBERSECURITY & DIGITAL FORENSICS

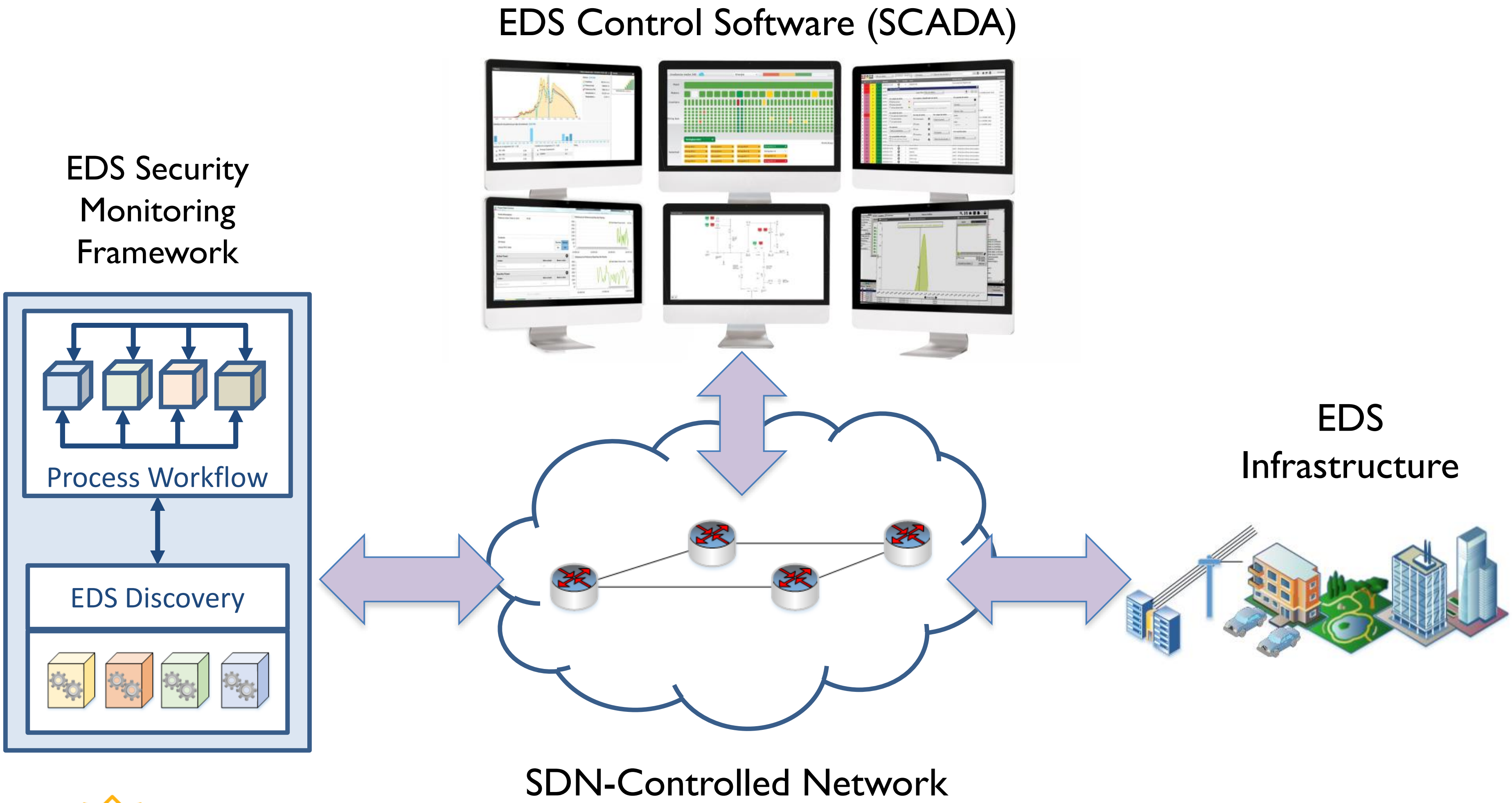
* https://cve.mitre.org/

CREDC

A Security Framework for EDS: SDN



Leveraging SDN for Security Monitoring



SDN Example

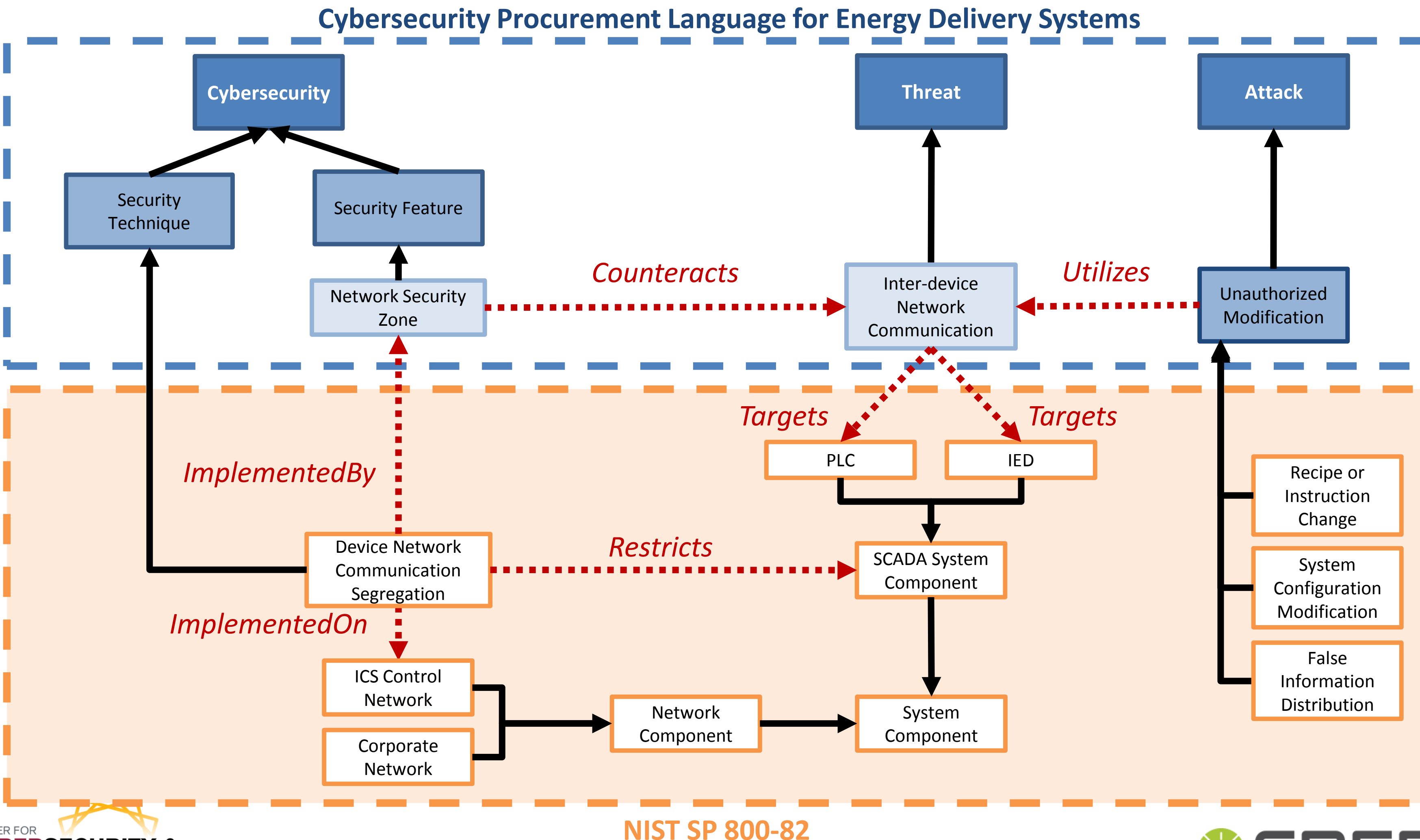
- *PLCs and IEDs must not talk to each other directly:*

  - Security Threat: Inter-device Network Communication[2]
  - Attacks: Recipe or Instruction Change, System Configuration Modification, False Information Distribution[1,2]

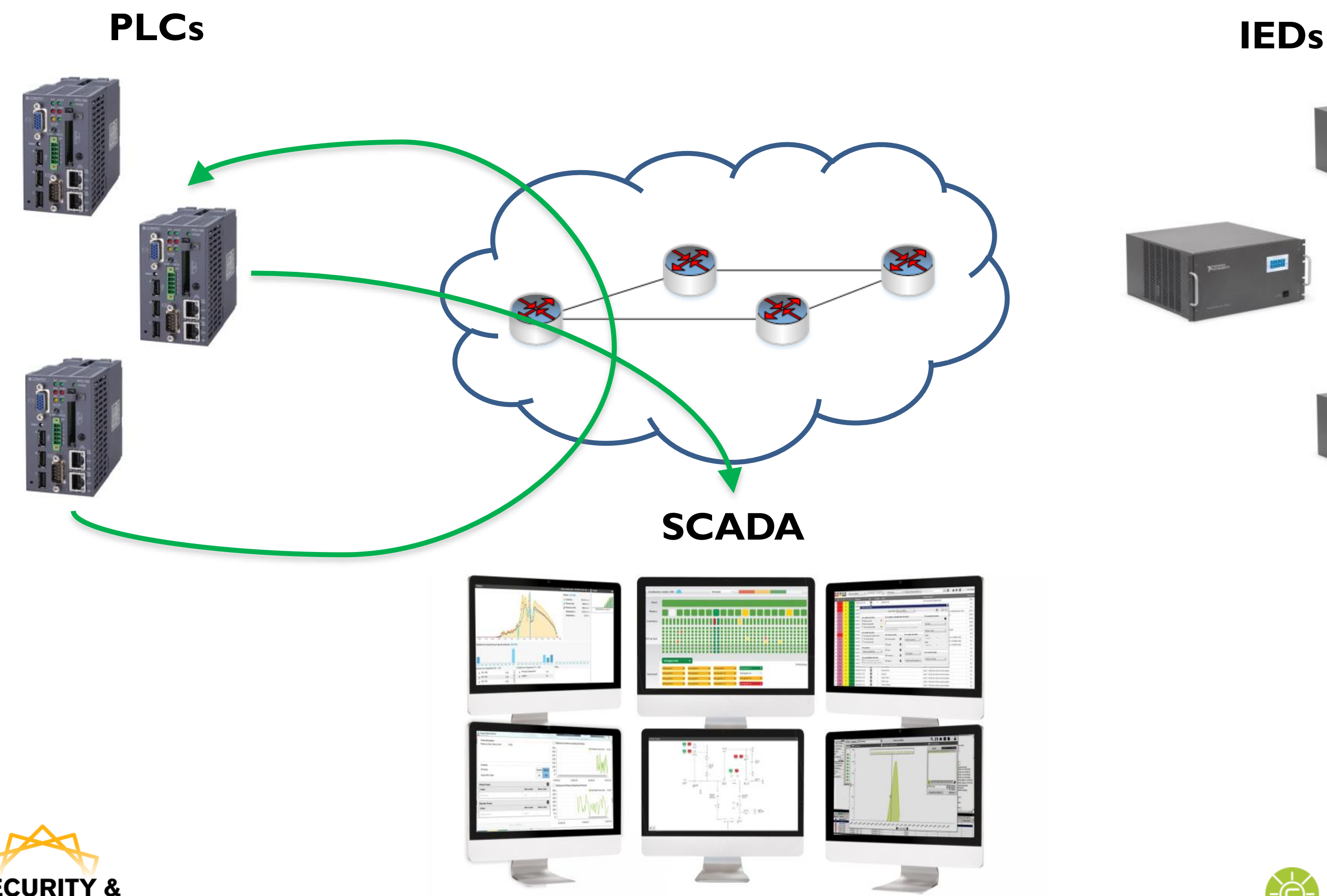
  - Security Features: Network Security Zone[1]
  - Security Techniques: Device Network Communication Segregation[2]
  - EDS Infrastructure: ICS Control Network, IED, PLC[2]

1) Cybersecurity Procurement Language for Energy Delivery Systems
2) NIST SP 800-82

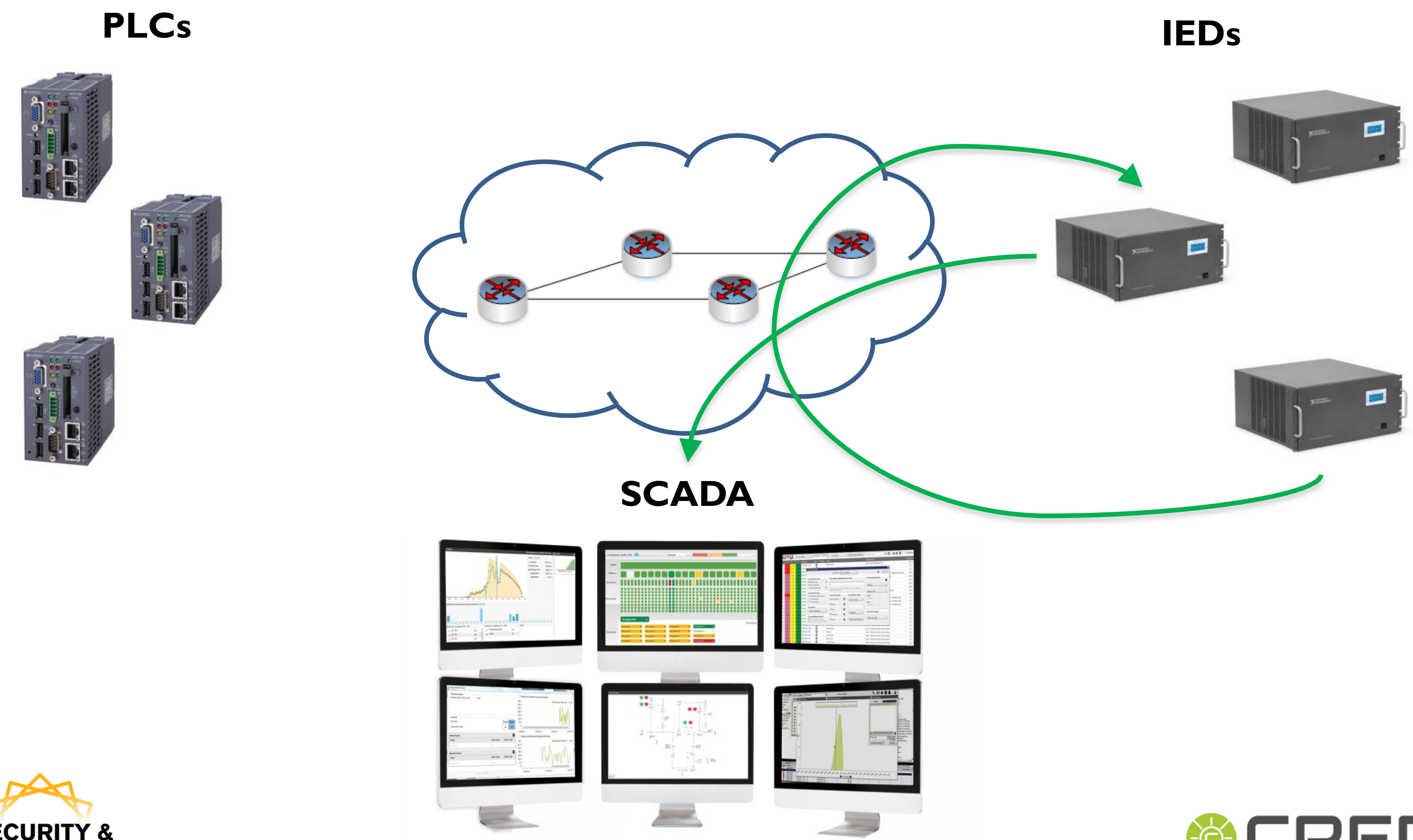
Ontology Representation: SDN Example



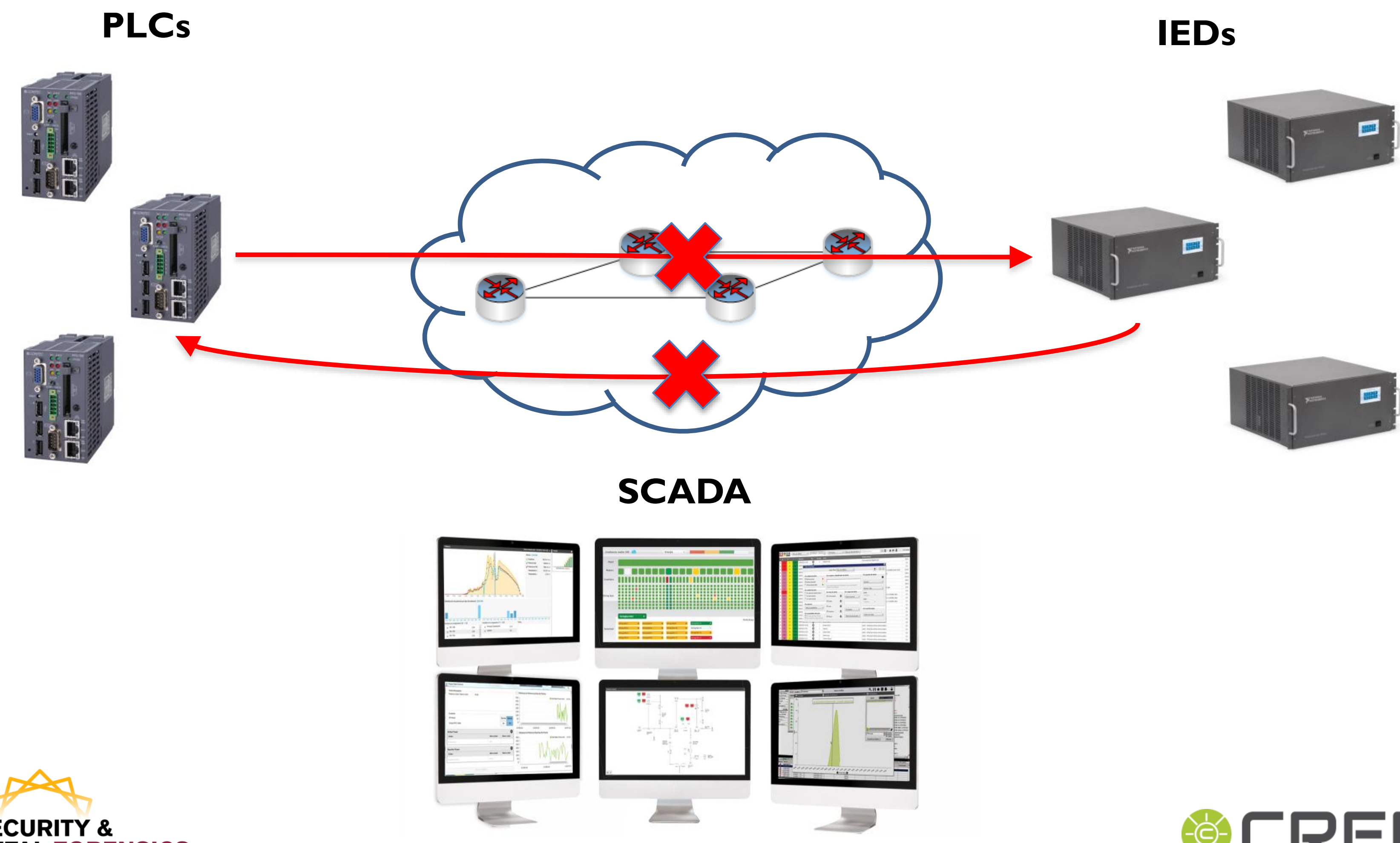
Leveraging SDN for Monitoring Traffic



Leveraging SDN for Monitoring Traffic (II)



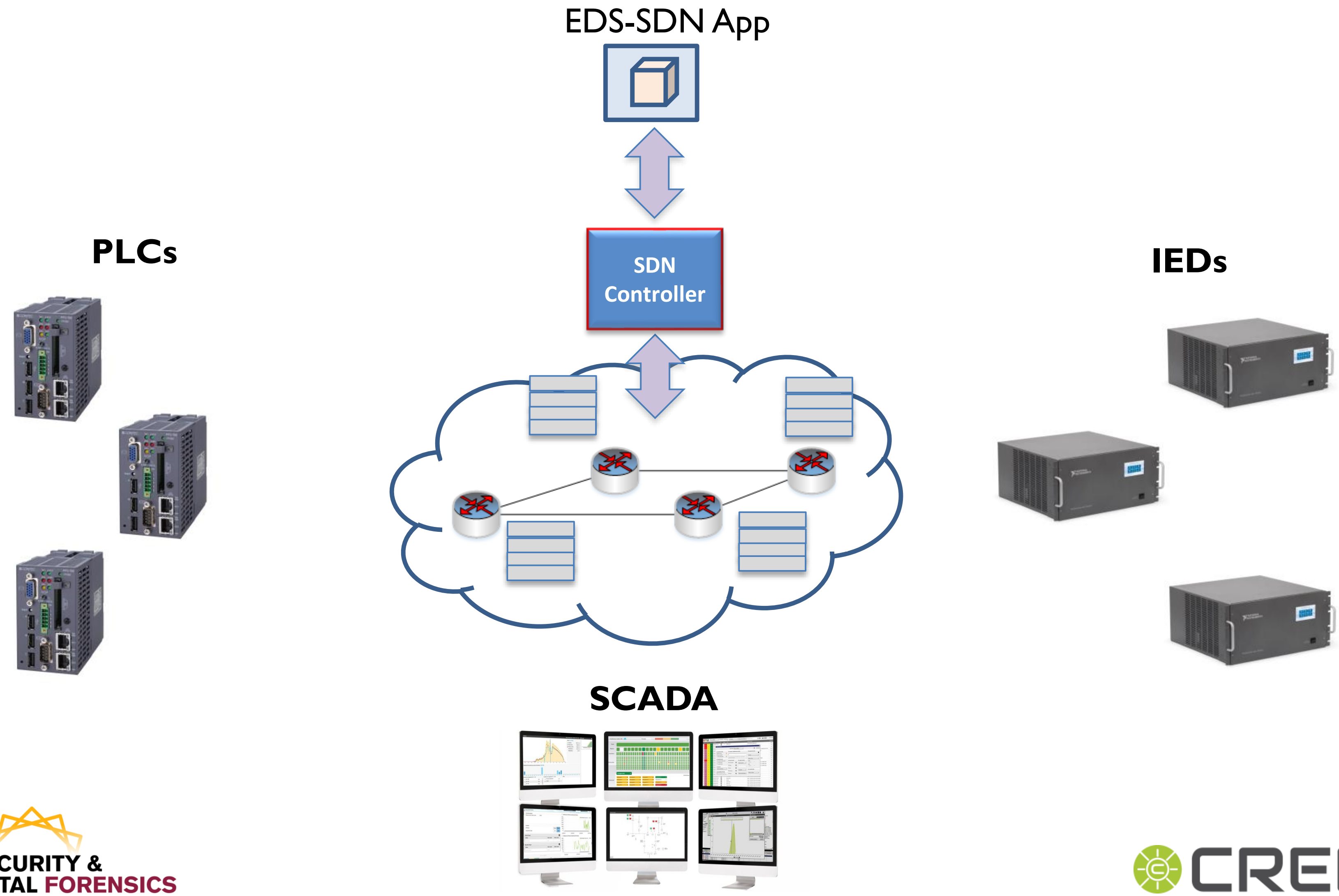
Leveraging SDN for Monitoring Traffic (III)



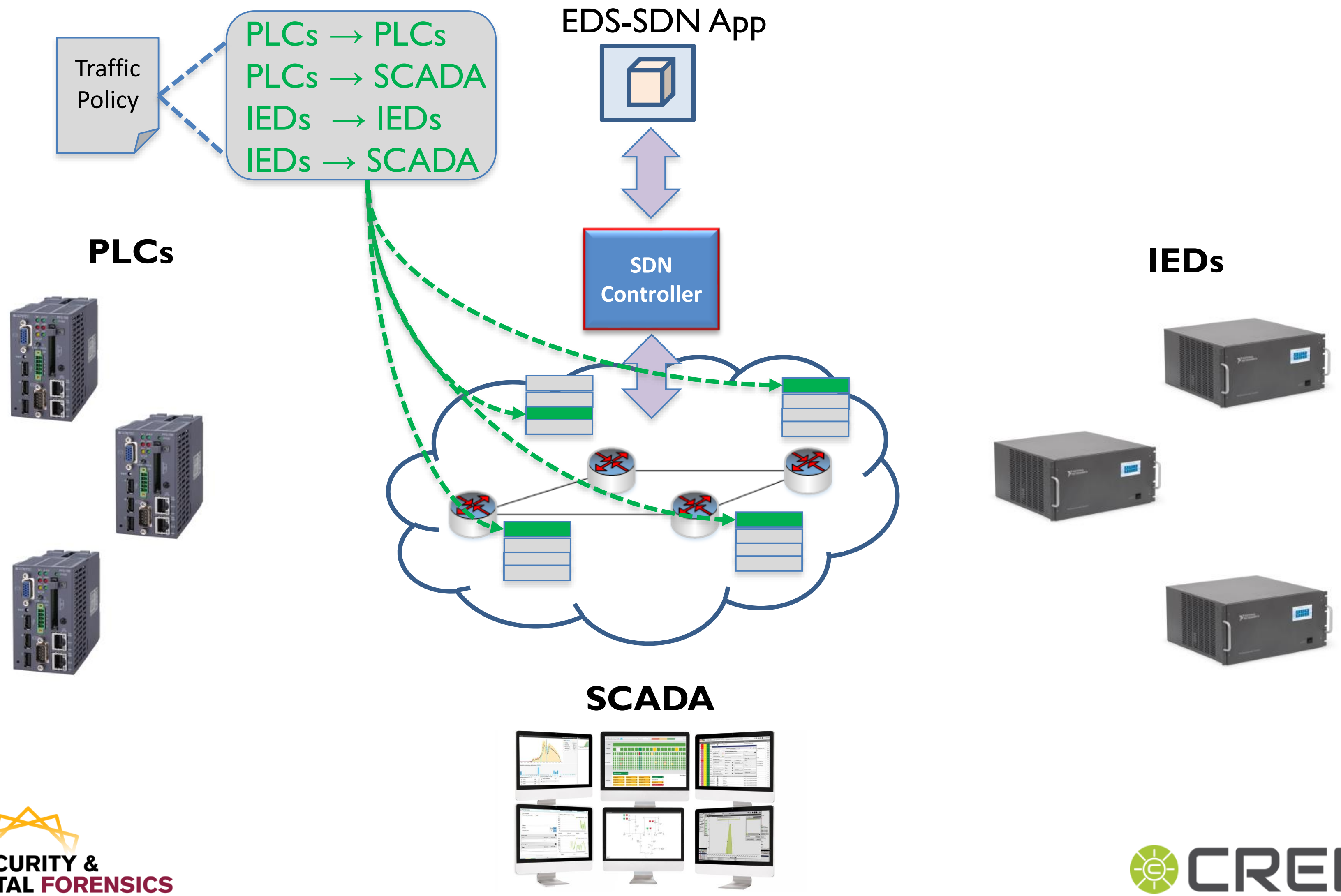
CENTER FOR CYBERSECURITY & DIGITAL FORENSICS

CREDC

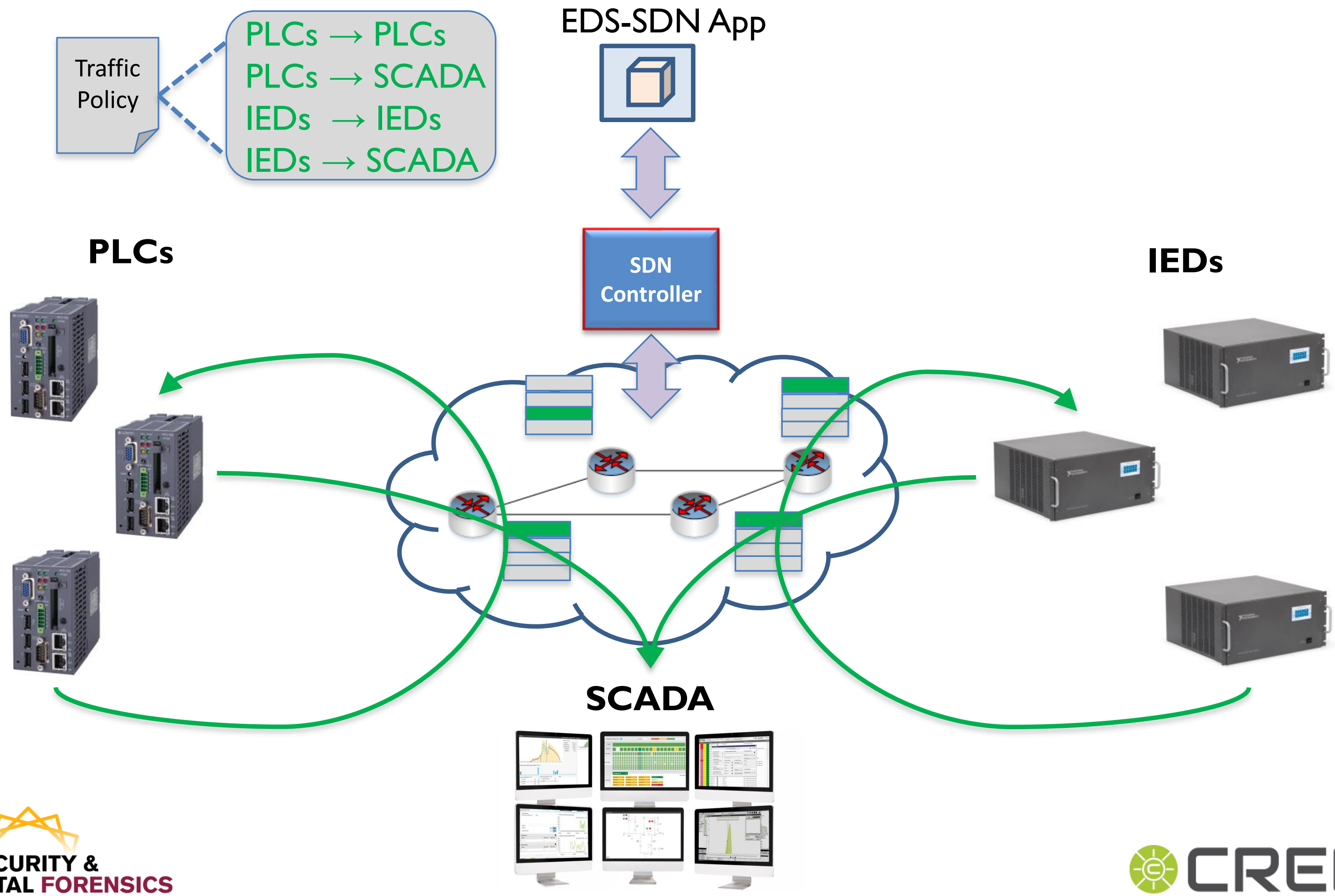
Leveraging SDN for Monitoring Traffic (IV)



Leveraging SDN for Monitoring Traffic (V)



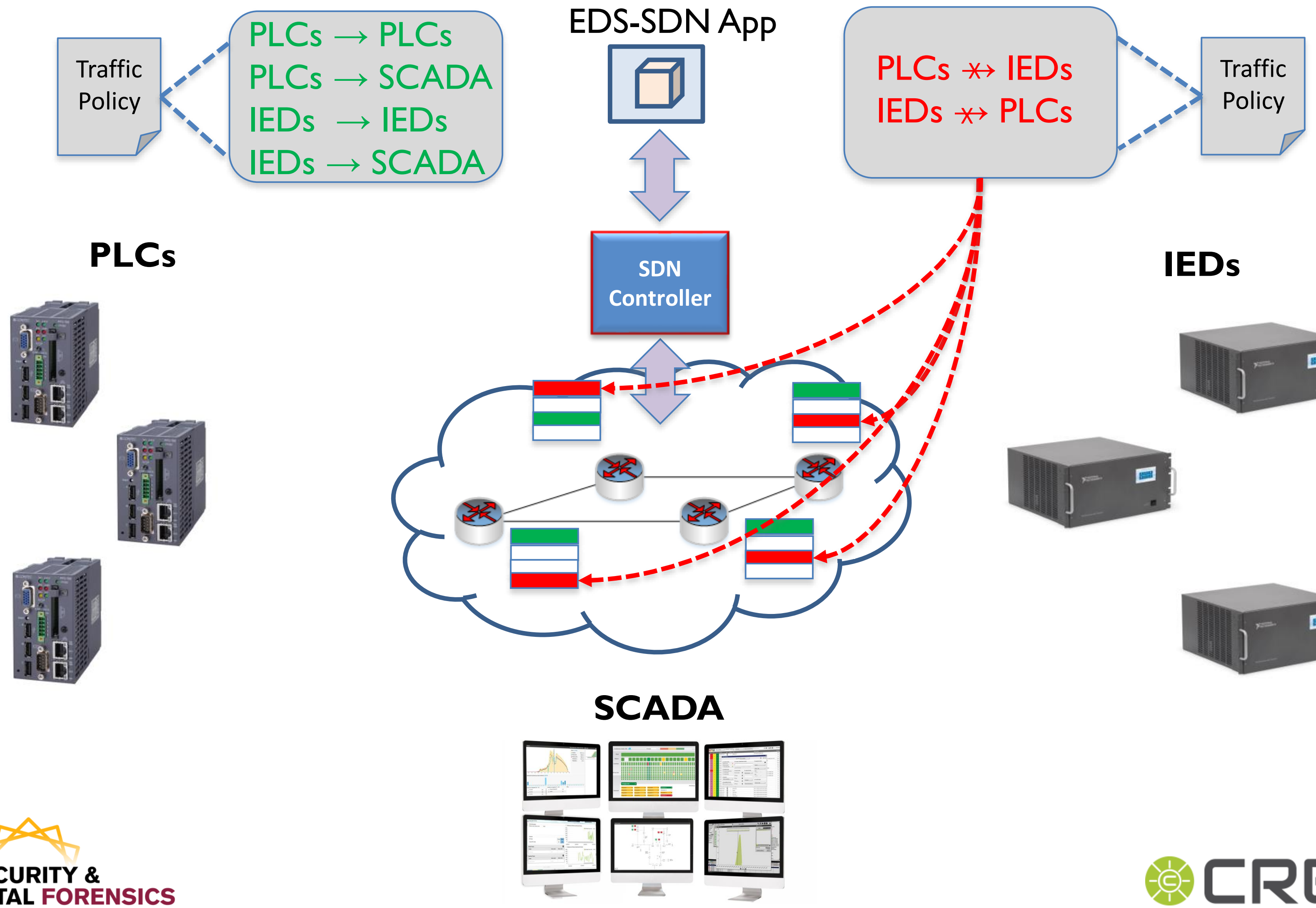
Leveraging SDN for Monitoring Traffic (VI)



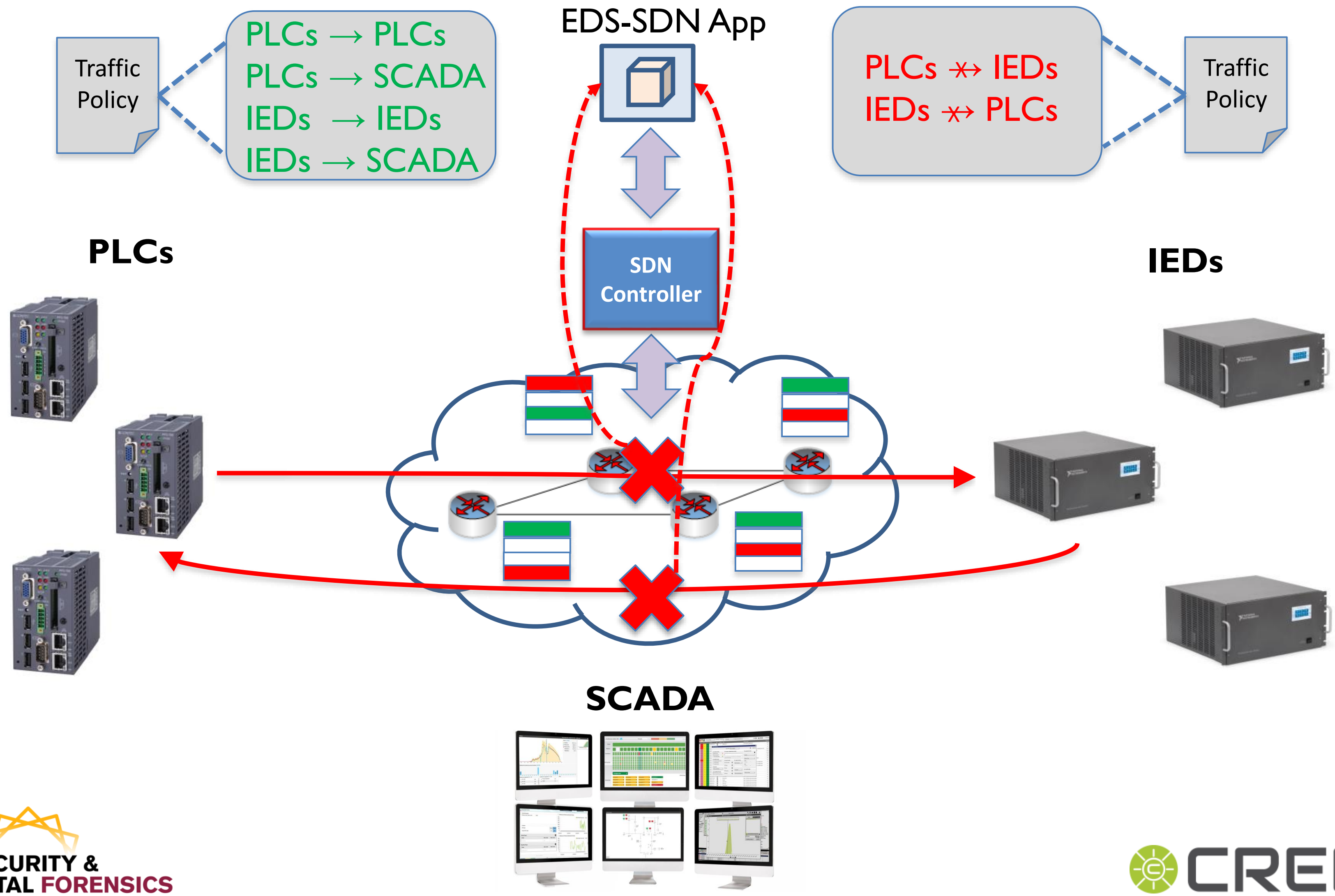
CENTER FOR CYBERSECURITY & DIGITAL FORENSICS

CREDC

Leveraging SDN for Monitoring Traffic (VII)



Leveraging SDN for Monitoring Traffic (VIII)



Security Monitoring Using SDN

- Benefits of using an SDN-based solution:
  - Customizable: new SDN applications may be added
  - Non-Intrusive: no need to modify existing EDS infrastructure, e.g., SCADA, physical meters, etc.
  - Scalable: new network nodes should be accommodated
  - Platform Independent: may support different components and configurations

Ongoing Work

- We are currently working on the following:
  - Ontology-based engine: several documents parsed, 1324 logical axioms, 425 classes, 214 properties, 441 subclass relationships
  - SDN infrastructure developed, working on testing and refinement
  - Supporting backbone framework in progress, as well as in a *proof-of-concept* module depicting automated monitoring for compliance

Industry Involvement

- We are actively looking for industry partners for:
  - Getting input/feedback on current security compliance requirements and best practices
    - Relevant documents, conflicts, use cases, experience, etc.
  - Implementing a *proof-of-concept* software module leveraging a realistic EDS scenario:
    - Defining a customized workflow based on requirements
    - Defining data that can be collected using our SDN approach

Conclusions

- Future Work:
  - Support for friendly visualization techniques, e.g., *graphical user interfaces* (GUIs) for ontology queries in SPARQL
  - Support for the rigorous study of security risks and assessments by means of the simulation of attacks
- Broader Impact:
  - Improvement of the public's confidence on mission-critical EDS infrastructure

Contact

- Thank you all for listening!

- CDF Website: https://globalsecurity.asu.edu/cdf
- Carlos Rubio-Medrano: crubiome@asu.edu