CREDC

Modeling Security Risk to and Resiliency of EDS using Software-Defined Networks and Robust Networked Control Systems

Sachin Shetty, L.H. Keel, Hellen Maziku, Sirisha Kallakuri, and Esther Amullen

RESEARCH GOALS

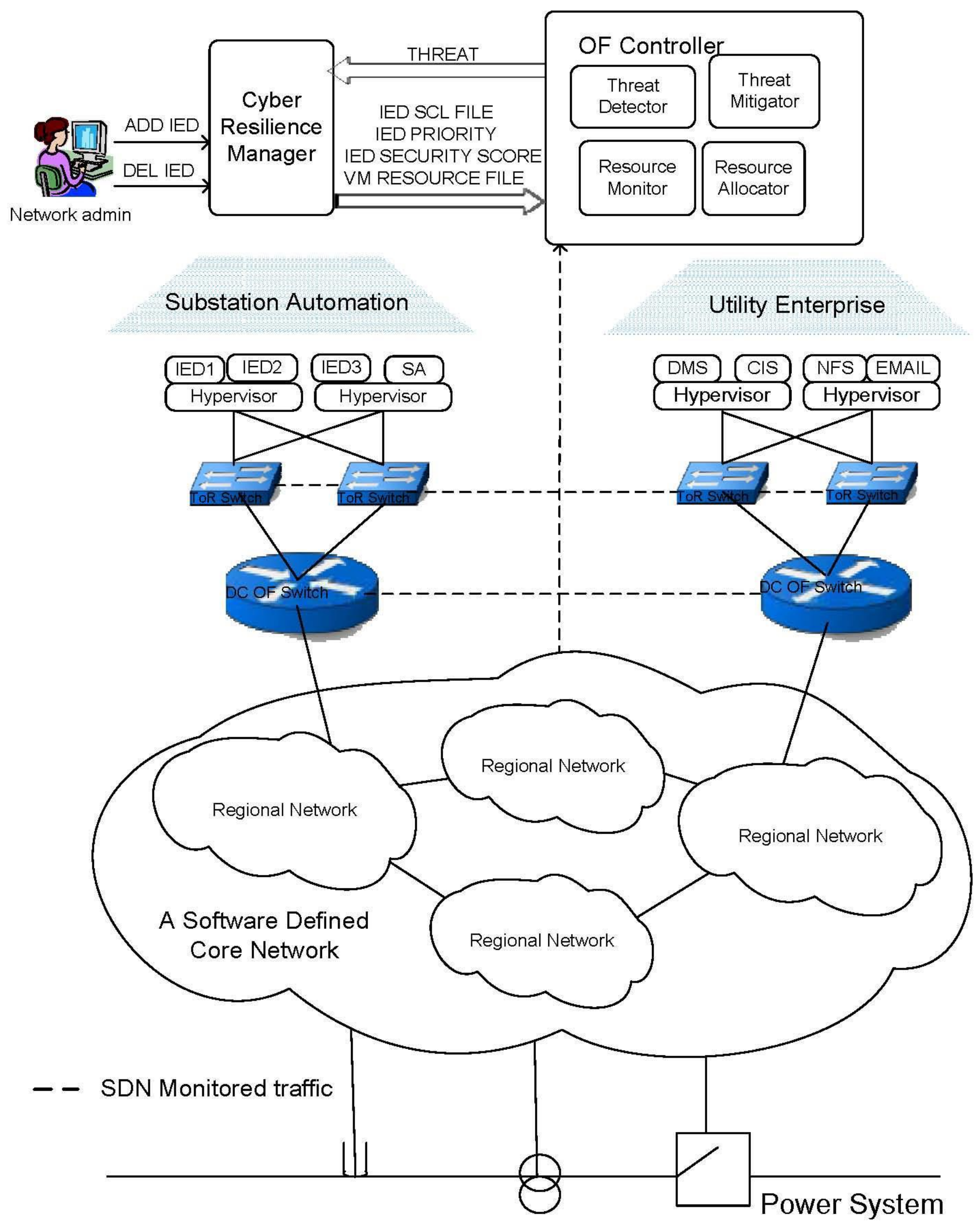
- Systematic characterization of attack paths exploited by zero-day vulnerabilities in EDS.
- Network diversity modeling to evaluate resiliency of EDS in presence of zero-day vulnerabilities.
- Attack detection, classification, and impact assessment on cyber-physical systems and mitigation of zero-day attacks.
- Designing controller algorithms to protect against specific attack categories.
- Develop a cloud-based risk assessment tool to monitor threats to EDS.

RESEARCH CHALLENGES

- For risk assessment modeling and security quantification, the biggest challenge lies in determining criticality of individual components in physical and cyber systems, and the impact on the overall cyber-physical system if these individual components were to be compromised.
- For network diversity modeling, the challenge is the systematic identification of attack paths and diversity solutions that are easily deployed. Also, the verification and validation of security metrics is a challenging task.
- The resilient SDN design will have performance consequences for the cyber-physical network. The challenge lies in incorporating such performance tradeoffs like accuracy while meeting the resilient requirements.
- For attack classification, the biggest challenge is to identify parameters (measurement variables) for the classification. Determining anomalies of the physical system operation from output measurements is also a big challenge.
- Assuring model accuracy is key challenge in designing a resilient controller technique.

RESEARCH PLAN

- Network diversity modeling to assess the resiliency of EDS against zero-day attacks.
- Quantify the impact of the various attacks paths on EDS.
- Network-diversity-based metric computed for different network configurations and policies for evaluating the impact of different classes of malicious software.
- Realize security risk assessment using OpenFlow controller.
- Mitigation techniques will include reroute, rate limit, drop flows, migrate virtualized IED, prioritize flows, etc.
- Timing for triggering resilient control when intrusion is detected in network level.
- Model-based estimation of resilient control action.
- Continued model adaptation to maintain the accuracy of the model based on input/output data.

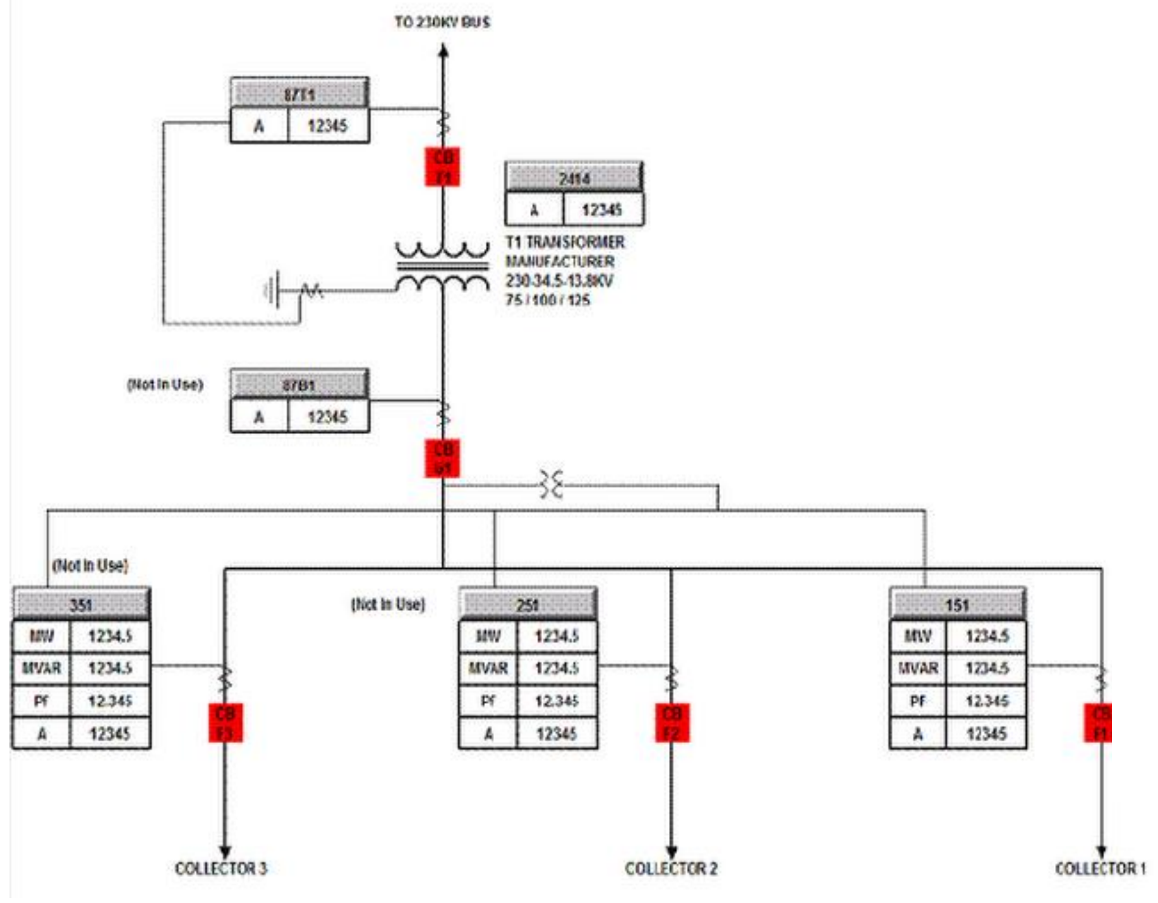


Architecture to model security and resiliency in EDS

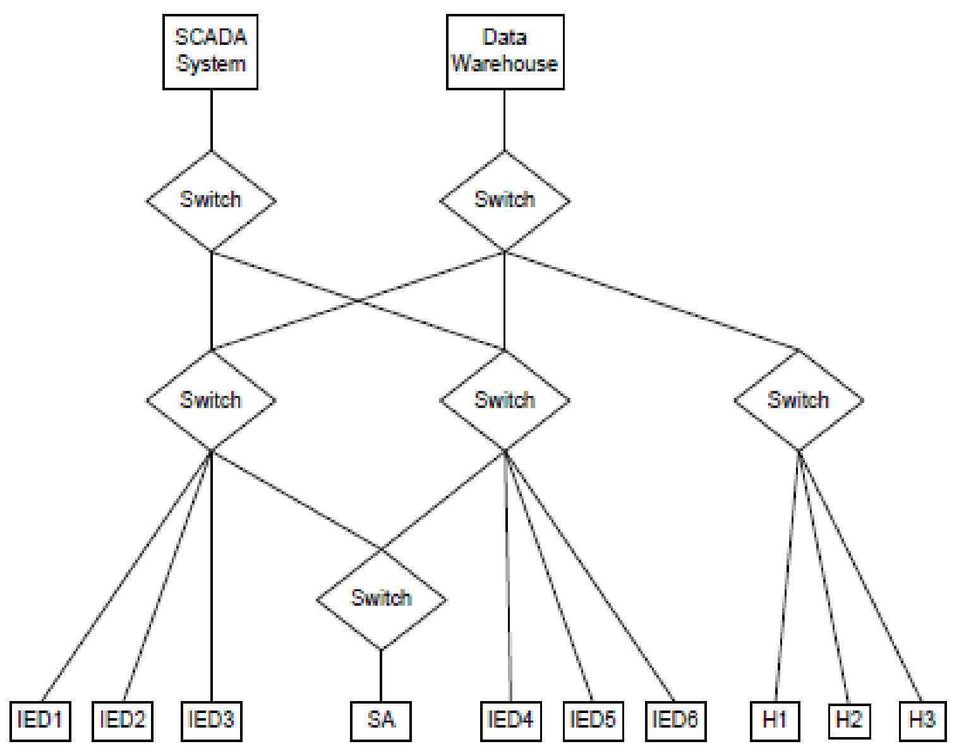
PRELIMINARY SECURITY RISK MODEL

- Model security score of IEDs in EDS.
- The score for a particular threat based upon its susceptibility s_i and countermeasure factor c_i is given by $t_i = s_i(1 - c_i)$.
- The score for the jth IED with m_j threats is $E_j = \sum_{i=1}^{m_j} t_i * S_R$
  - Where S_R is security requirement of an IED.
  - If this IED were to be compromised, how much impact would it have on the Smart Grid?
- Overall security score of the network with n IEDs: $R = 10 - \min\left(10, \sum_{j=1}^{n} E_j\right)$

PRELIMINARY IMPLEMENTATION

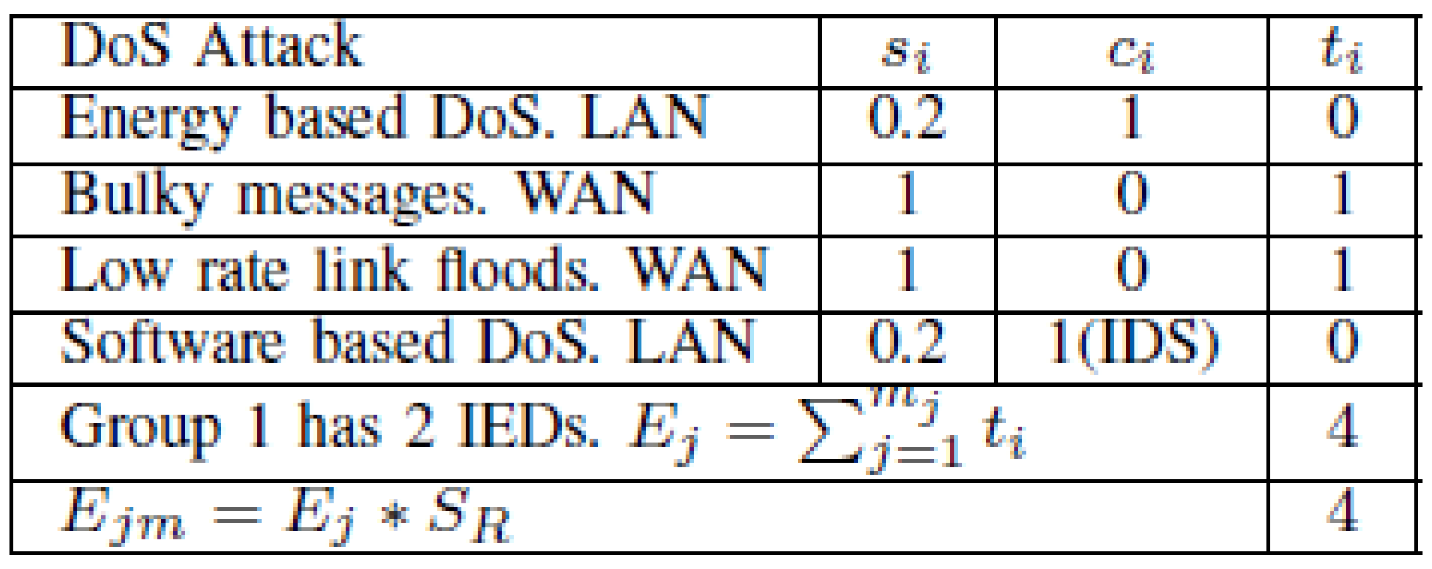


Windmill Collector Substation



Network Topology for Windmill Collector Substation

- Consider a windmill collector substation
  - 2 current differential and overcurrent IEDs.
    - Transmission domain (medium critical).
  - 1 distribution substation transformer monitoring IED.
    - Substation domain (most critical).
  - 3 distribution feeder protection and control IEDs.
    - Distribution domain (least critical).
  - 6 OpenFlow switches, 3 end hosts, and 3 servers.
- Mininet used to simulate the OpenFlow switches.
- Triangle Microworks IEC61850 suite to simulate IEDs.
- Ryu for implementing the OpenFlow controller.



DoS Attack	s_i	c_i	t_i
Energy based DoS. LAN	0.2	1	0
Bulky messages. WAN	1	0	1
Low rate link floods. WAN	1	0	1
Software based DoS. LAN	0.2	1(IDS)	0
Group 1 has 2 IEDs. $E_j = \sum_{j=1}^{m_j} t_i$			4
$E_{jm} = E_j * S_R$			4

SECURITY SCORE FOR GROUP 1 IEDS. S_R = MEDIUM = 1.0

BROADER IMPACT

- EDS security administrators will confidently assess the security posture of their cyber-physical infrastructure.
- EDS security administrators will be able to gauge the criticality of individual components in the cyber-physical infrastructure based on how they are impacted by the cyber-attacks, and then prioritize protection mechanisms.
- EDS security administrators will be able to decide the level of cyber resilience to be achieved by looking at the risk models without compromising other performance requirements, like accuracy.

INTERACTION WITH OTHER PROJECTS

- Assessment and evaluation of security risk assessment, network diversity, and resilient control algorithms on SDN testbeds available at partnering CREDC institutions.
- Use EDS testbeds with hardware-in-the-loop for testing and evaluation.
- Integration of EDS security-related concepts, techniques, and tools derived from CREDC research projects in graduate and undergraduate courses in computer network, network security, and control systems.

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM | CRED-C.ORG

FUNDING SUPPORT PROVIDED BY THE DEPARTMENT OF ENERGY, OFFICE OF ELECTRICITY DELIVERY & ENERGY RELIABILITY