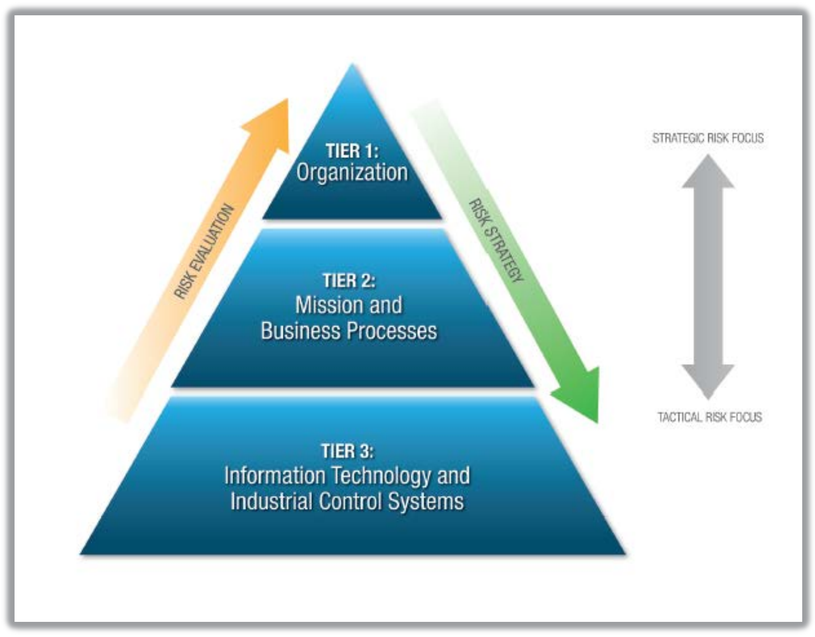
Towards Optimal Cyber Defense Remediation in Energy Delivery Systems

Kamrul Hasan, Sachin Shetty, Amin Hassanzadeh, Sharif Ullah

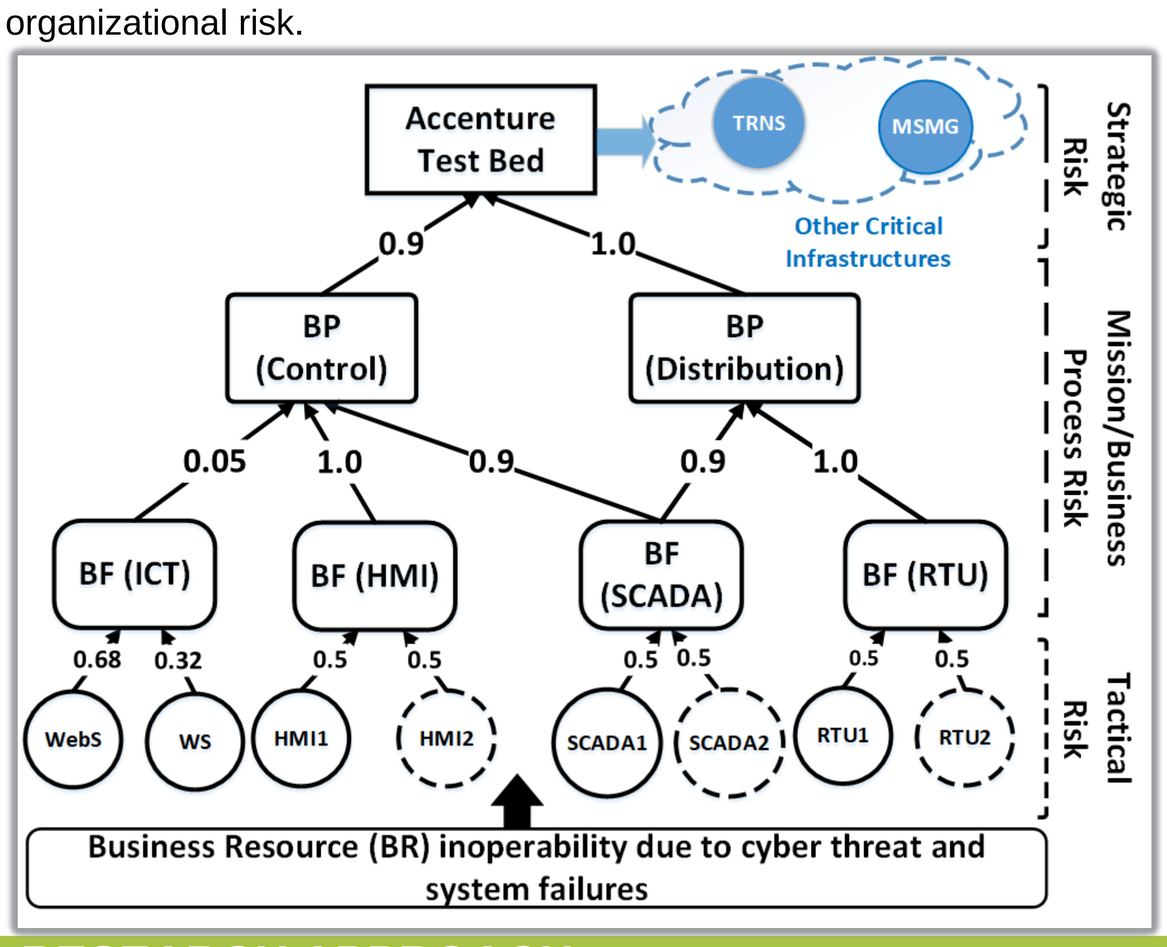
EDS OPERATIONAL RESILIENCE

- **NIST Special Publication 800-82/DoE electricity subsector cybersecurity RMP** suggests three-tiered structure to provide a comprehensive view of risk analysis of an electricity subsector organization.

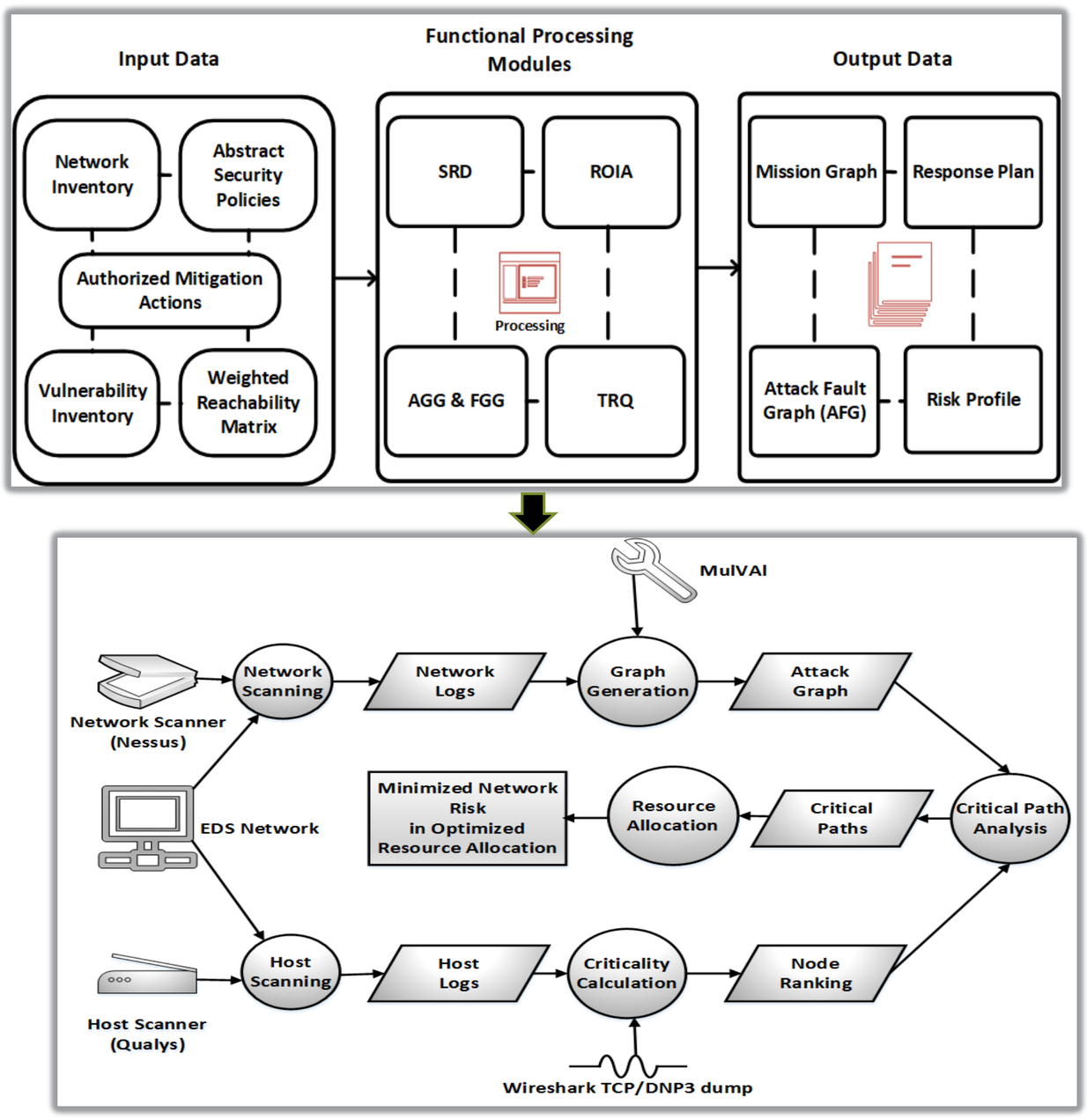


RESEARCH VISION

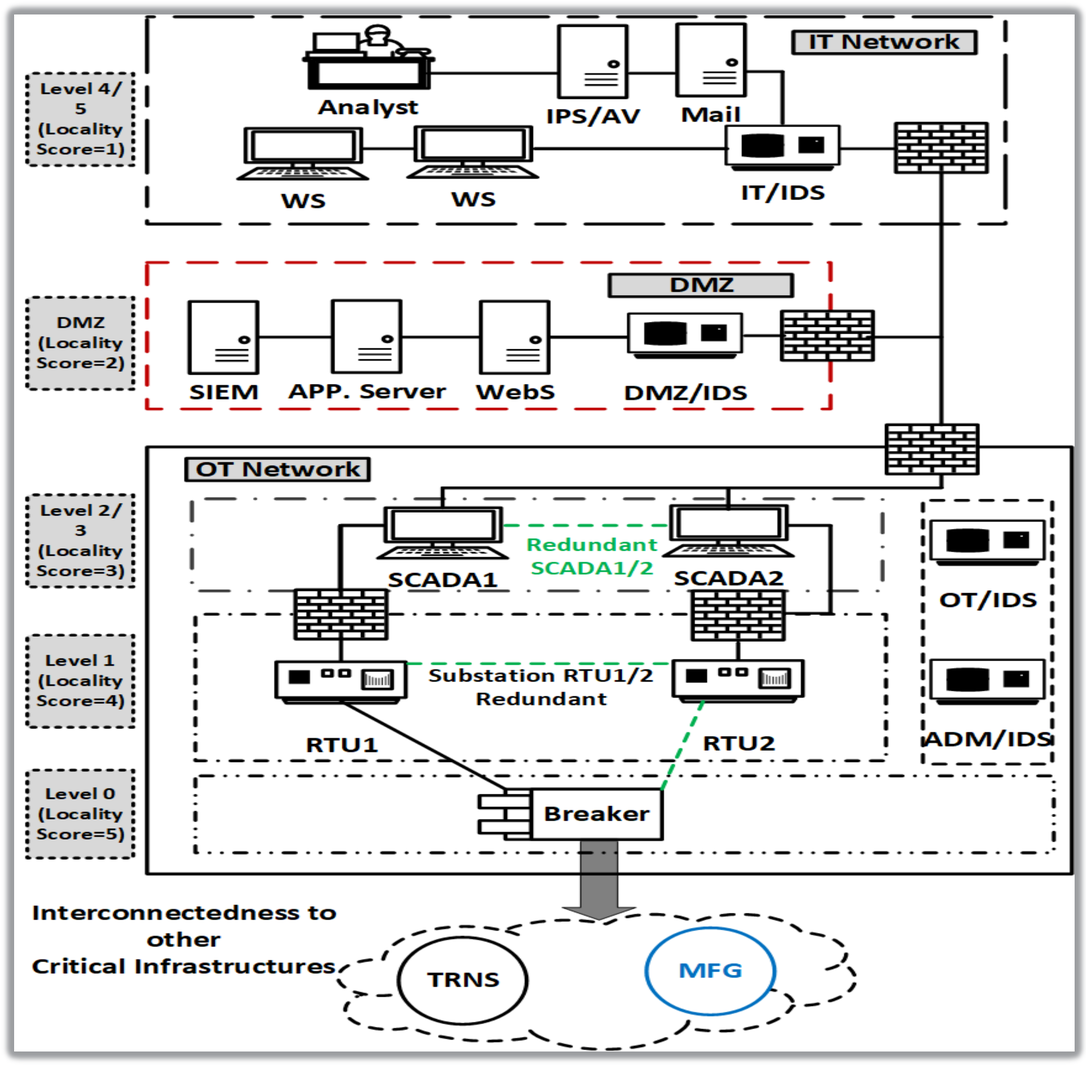
- Optimal selection of security controls at operational level which balances the tradeoff among tactical risk, mission/business process risk, and organizational risk.



RESEARCH APPROACH



TESTBED



- The system model is implemented in Accenture's ICS test-bed for analyzing cyber risk at different cyber threat scenarios.

PRELIMINARY RESULTS

Mitigation Actions	Threat Likelihood at assets					Business Inoperability (I)
	WS	WebS	SCADA	HMI	RTU	
No Action	0.72	0.144	0.1152	0.1152	0.1152	1.26×10^{-6}
Software Patching (SP)	0.638	0.0924	0.0570	0.0570	0.05975	1.01×10^{-7}
SP + System Redundancy	0.638	0.0924	0.0569	0.0569	0.05970	9.28×10^{-8}

Table 1: Threat likelihood and Business inoperability

Mitigation Actions	Business Inoperability (I)(10^{-5}) & Economic Loss (EL) (Units)					
	Electric Distribution (ED) (I)	ED (EL)	TRNS (I)	TRNS (EL)	MFG (I)	MFG (EL)
Policy0 (No mitigation)	0.1522	152.2	0.0005	0.5	0.0027	2.7
Policy1 (SP)	0.01222	12.22	0.00004	0.04	0.00022	0.22
Policy2 (SP + Redundancy)	0.01124	11.24	0.00004	0.04	0.0002	0.20

Table 2: IIM Output and Economic Loss

- **Provide decision-makers ability to estimate ROI associated with security control selection.**

COLLABORATION OPPORTUNITIES

Seeking collaborative opportunities from industry partners:

- Need relevant system and network traces to ascertain asset's criticality index.
- Identifying negative impacts of applying a security control considering operational quality of service.
- Identifying parameters for determining operational resilience

✓ Contact: sshetty@odu.edu

✓ Activity webpage: https://cred-c.org/researchactivity/modeling-security-risk-and-resiliency-eds-using-software-defined-networks-and

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