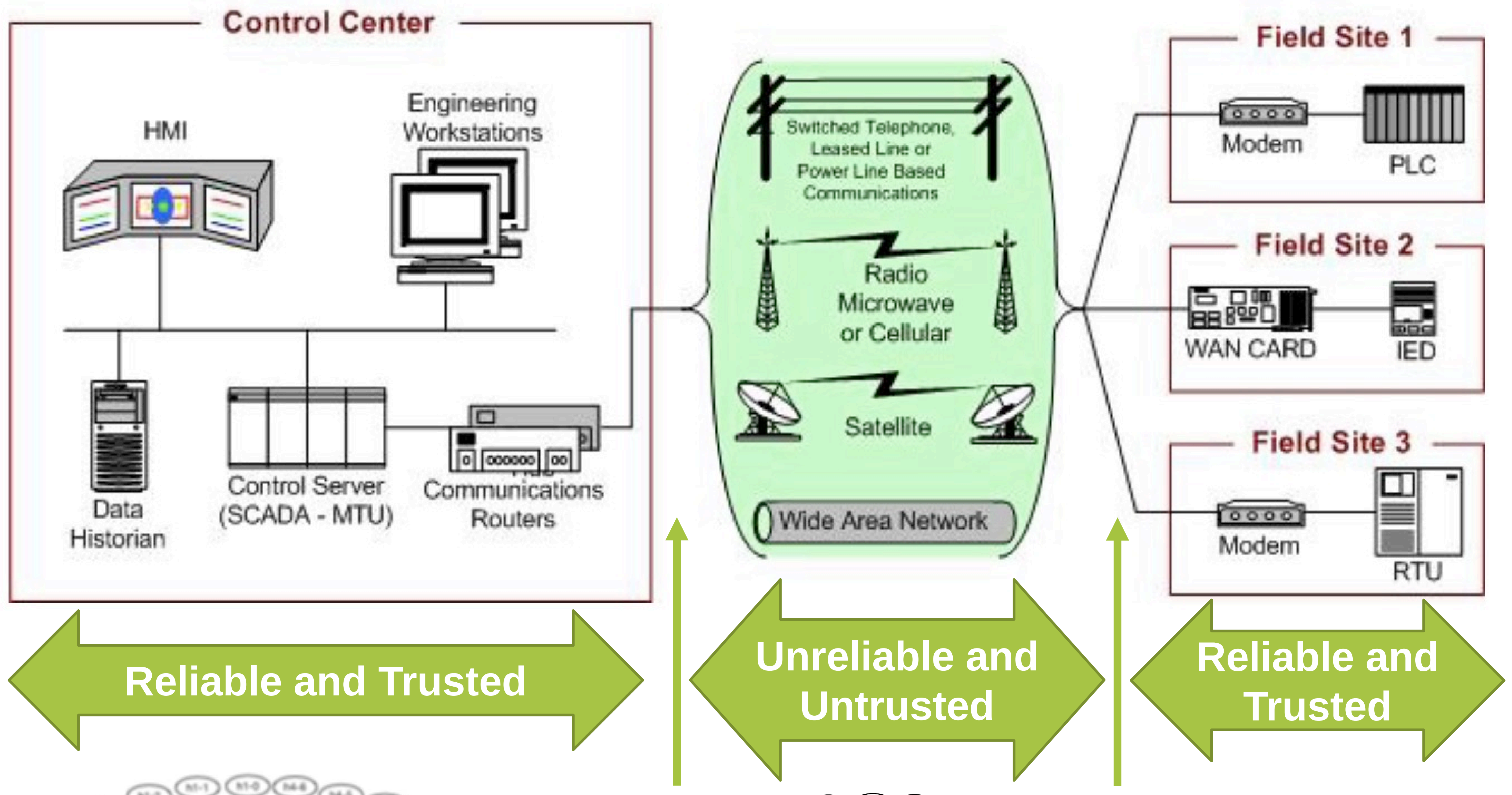
CREDC

Policy Enforcement Network Functions: Resiliency in Industrial Control Systems

Stuart Baxley, Nicholas Bastin, and Deniz Gurkan   University of Houston Networking Lab

PROBLEM: PERFORMANCE DEGRADATION AND SECURITY VULNERABILITIES IN ICS NETWORKS

NIST Guide to ICS Security 800-82 Figure 2-2

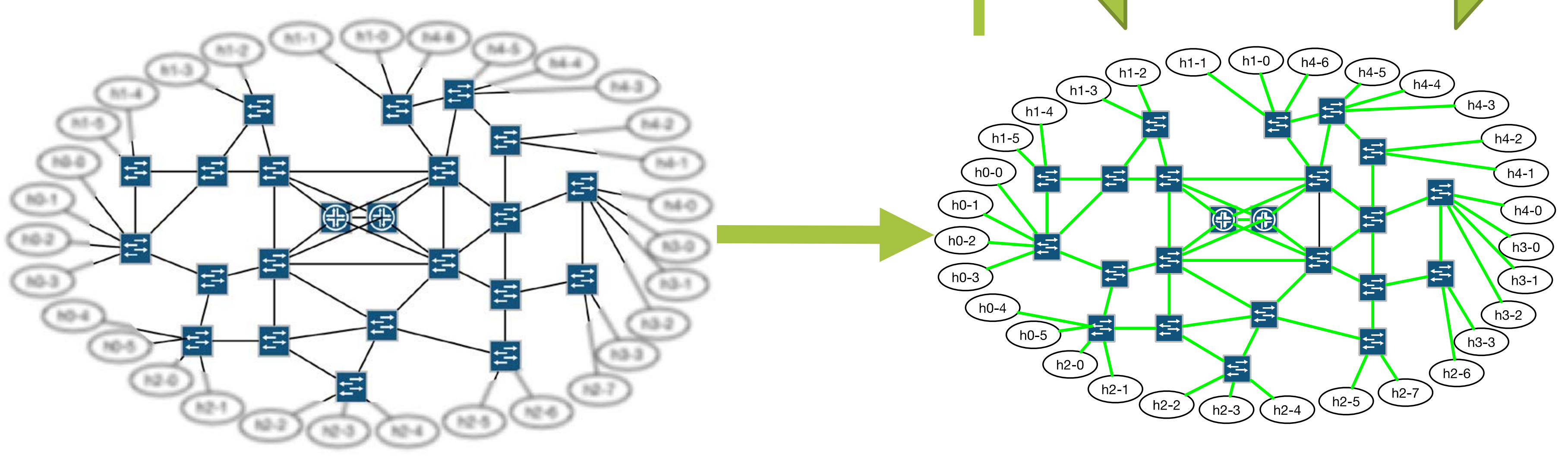


Reliable and Trusted

Unreliable and Untrusted

Reliable and Trusted

SOLUTION: ENFORCE BUSINESS POLICY AND MITIGATE INDUSTRIAL CONTROL SYSTEM (ICS) RISK WITHIN THE NETWORK



A set of given NFs with policy enforcement goals of $\{p_i, p_j, \ldots\}$ and on network flows $\{f_a, f_b, \ldots\}$
Resources mapped onto existing infrastructure
Redundancy assurance for resiliency

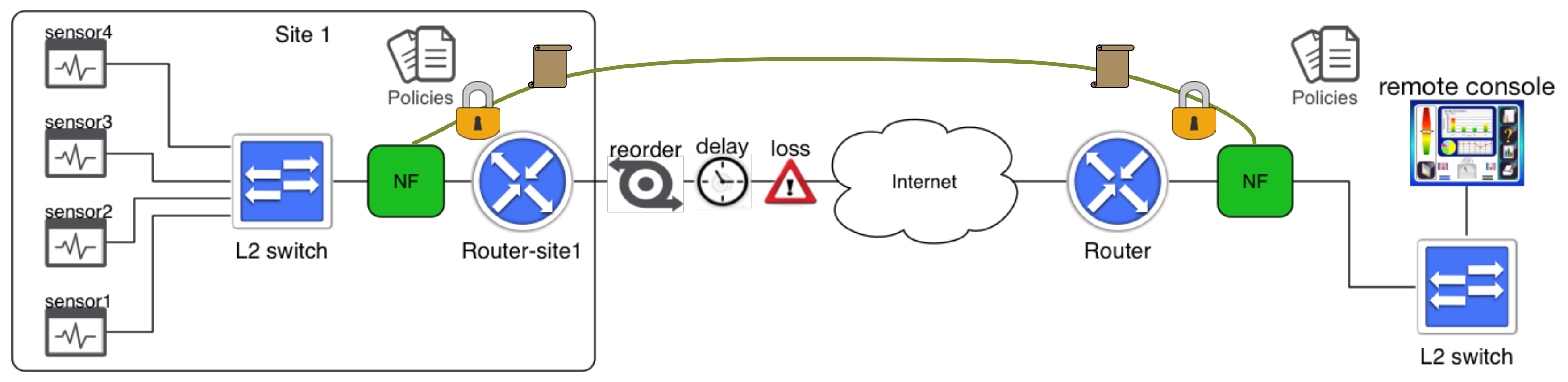
BUSINESS POLICY ON ICS NETWORKS

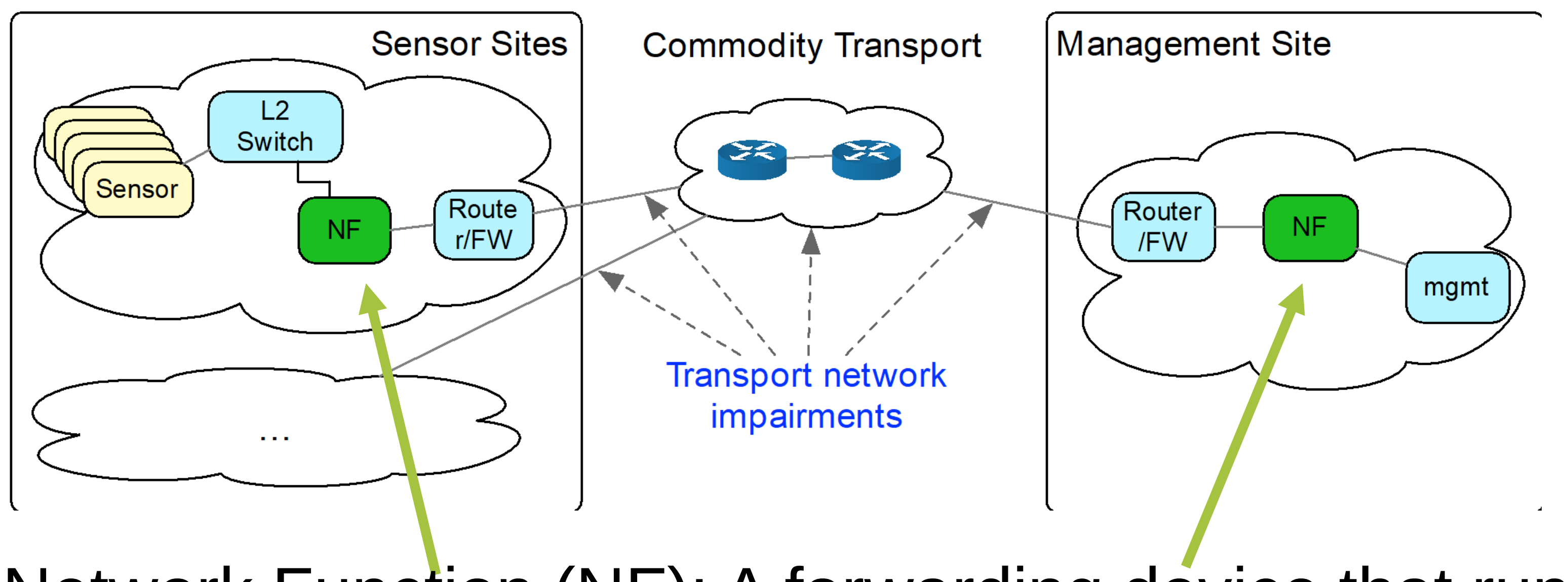
Security risk identification and control with fine granularity on data flows

Customized mitigation of security risks in the network *without modifying the existing ICS systems*

Targeted protection of data integrity & confidentiality proportional to estimated risk and value of assets

ICS RISK MITIGATION





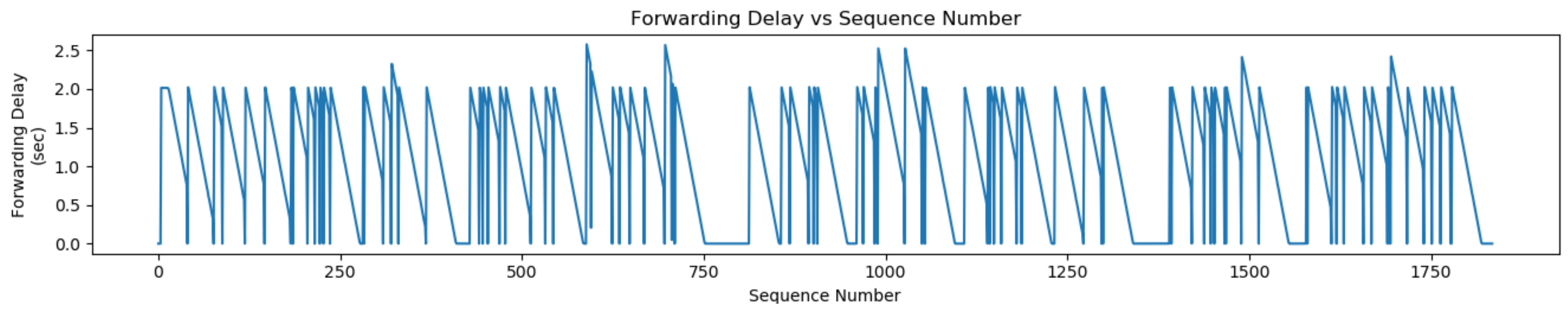
Network Function (NF): A forwarding device that runs the business policy enforcement software

Reduce attack surface
Preserve data integrity and confidentiality

TARGETED POLICY ENFORCEMENT

Asset addresses:
IP + MAC addresses and port numbers to identify the traffic to apply policy on

CUSTOMIZED MITIGATION



If there is 10% loss in the WAN, ensure delivery with a maximum delay of 3 sec

TARGETED PROTECTION

Policy Statements:
Drop all out of order packets
Recover lost packets
Encrypt all communications
Sign all packets

SEEKING INDUSTRY PARTNERSHIPS FOR …

Articulation of Policy Statements
Determination of Policy for Targeted Protection
Reference Implementation and Test Suite

MORE INFORMATION

All reference implementation is documented as flow charts
Open Source Code and Documents:
https://bitbucket.org/UH-netlab/doe-nf

Contact: Deniz Gurkan (dgurkan@Central.UH.EDU)
Activity web site: https://cred-c.org/researchactivity/nfimessaging

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