Network Function Insertion for Reliable and Secure Control Messaging Over Commodity Transport

Messaging Resiliency in Industrial Control Systems

Deniz Gurkan, Nicholas Bastin, Stuart Baxley, Art Conklin

FUNDAMENTAL QUESTIONS/CHALLENGES

- Sensor data and control directives from oil/gas production facilities are commonly transmitted unencrypted using unreliable transport protocols over lossy network infrastructures.
- Even in cases where encryption or reliable transmission is used, network threats evolve on a time scale significantly faster than the upgrade schedules of industrial equipment.
- This activity decouples the implementation of secure, reliable transport from the actual industrial hardware, providing agility in responding to new threats without downtime of production equipment or waiting for vendor upgrades.

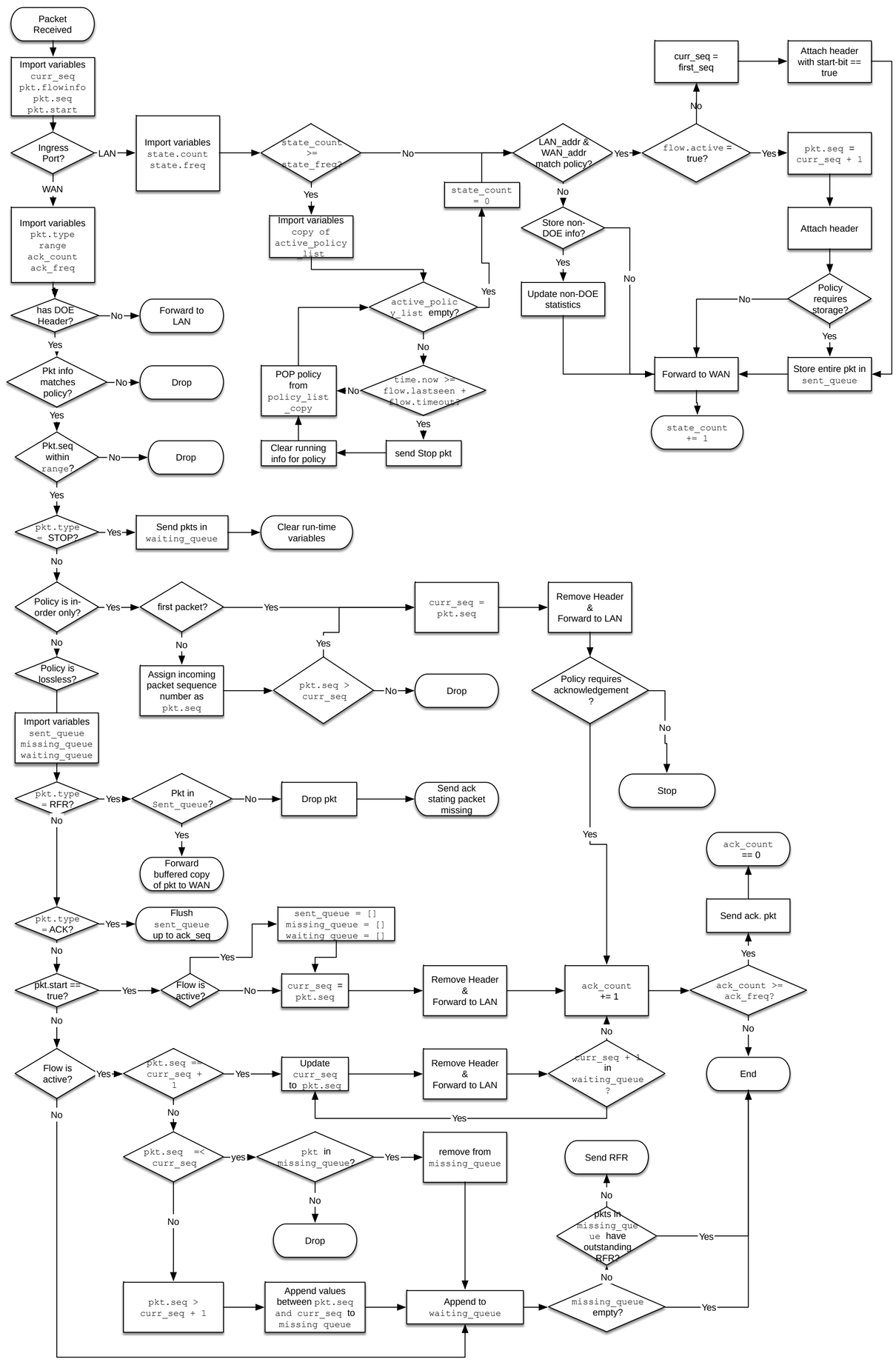
RESEARCH PLAN

- Create emulated topologies with end hosts to create the unreliable transfer scenarios in oil/gas industrial control systems (ICS)
- Observe and examine loss and other conditions that impact resilience of the network
- Develop and implement algorithms to increase connection resilience to be run on network function nodes
- Develop and create metrics to define and measure topology resilience and connection quality
- Test the connection quality achieved on infrastructure that is created on the GENI testbed

INTERACTION WITH OTHER PROJECTS

- Operational knowledge has been gained through our meetings with our collaborator, Dr. Art Conklin.
- We collaborate and participate in the NSF GENI project, a nationwide testbed for network science and engineering research.
- Our research utilizes University of Houston's NSA-funded testbed:
  - Over 1000 1Gb and 10Gb switch ports from Brocade, Cisco, Dell/Force10, HP, Intel and Pica8
  - Over a dozen SDN switches
  - A variety of specialized forwarding devices (NPUs, hybrid server-switches, etc.) from Caros, Cavium, Freescale, Intel, and Znyx
  - Over 250 general purpose CPU cores and 1.5TB of ram across two dozen servers
  - Over 100TB of raw storage capacity and 24 line-rate taps

RESEARCH RESULTS

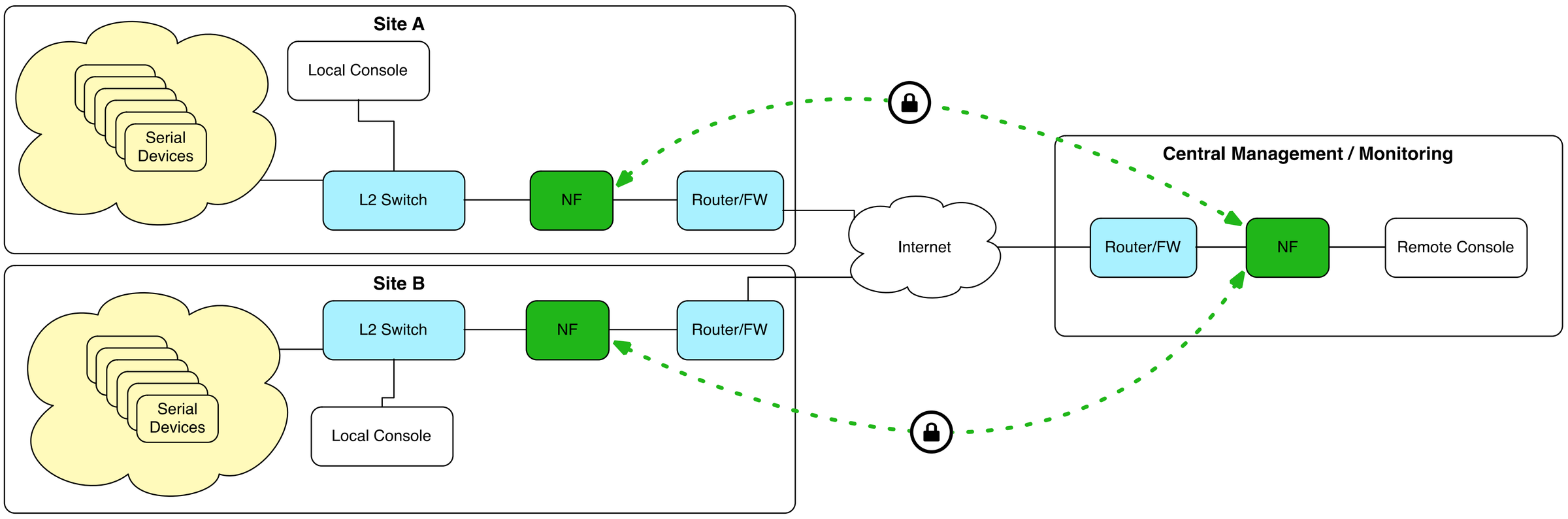


BROADER IMPACT

Network function insertion for reliable and secure control messaging over commodity transport

- No need to replace existing equipment to gain functionality
- Single point of testing and certification
- Single point of configuration for an entire site
- No need for power-hungry CPU or added cost to individual devices

- Guarantee in-order delivery of individual messages
- Per-device/flow or per-site ordering
- Wide options for site-to-site encryption
- Possible transparent (port-mirroring) operation



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