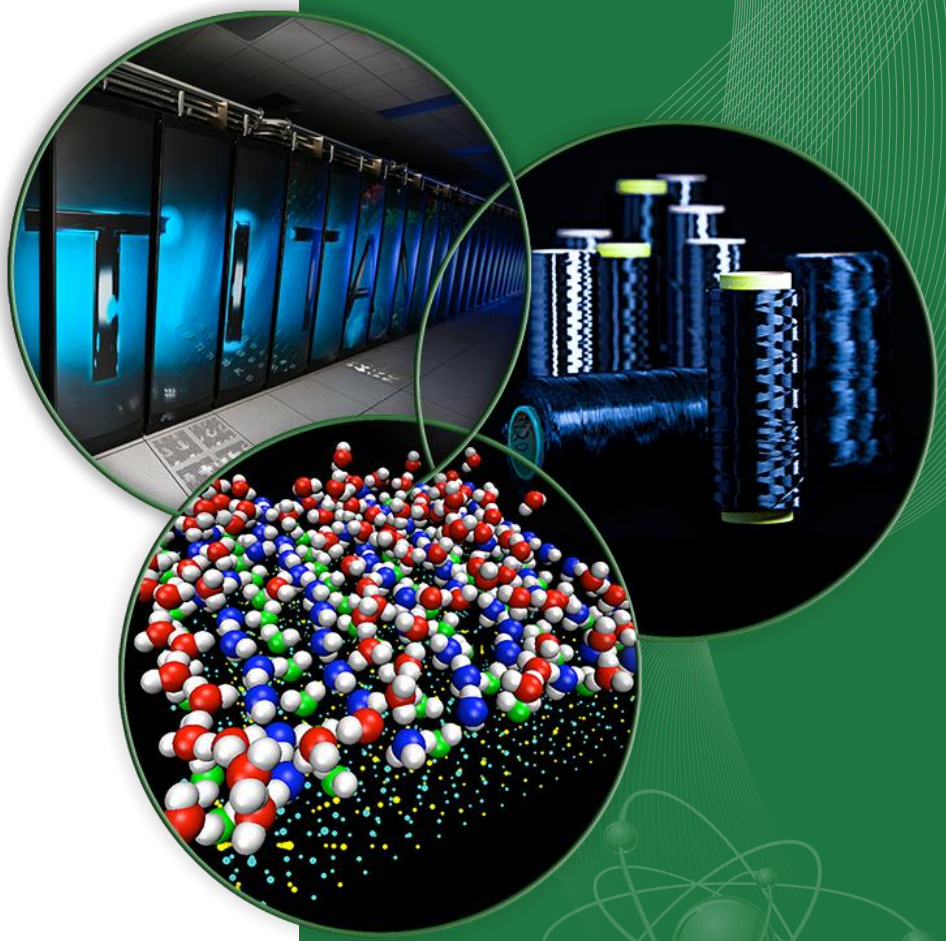
Cyber Security Assessment of the SNS ICS



Karen S. White

10/18/15

ORNL is managed by UT-Battelle
for the US Department of Energy

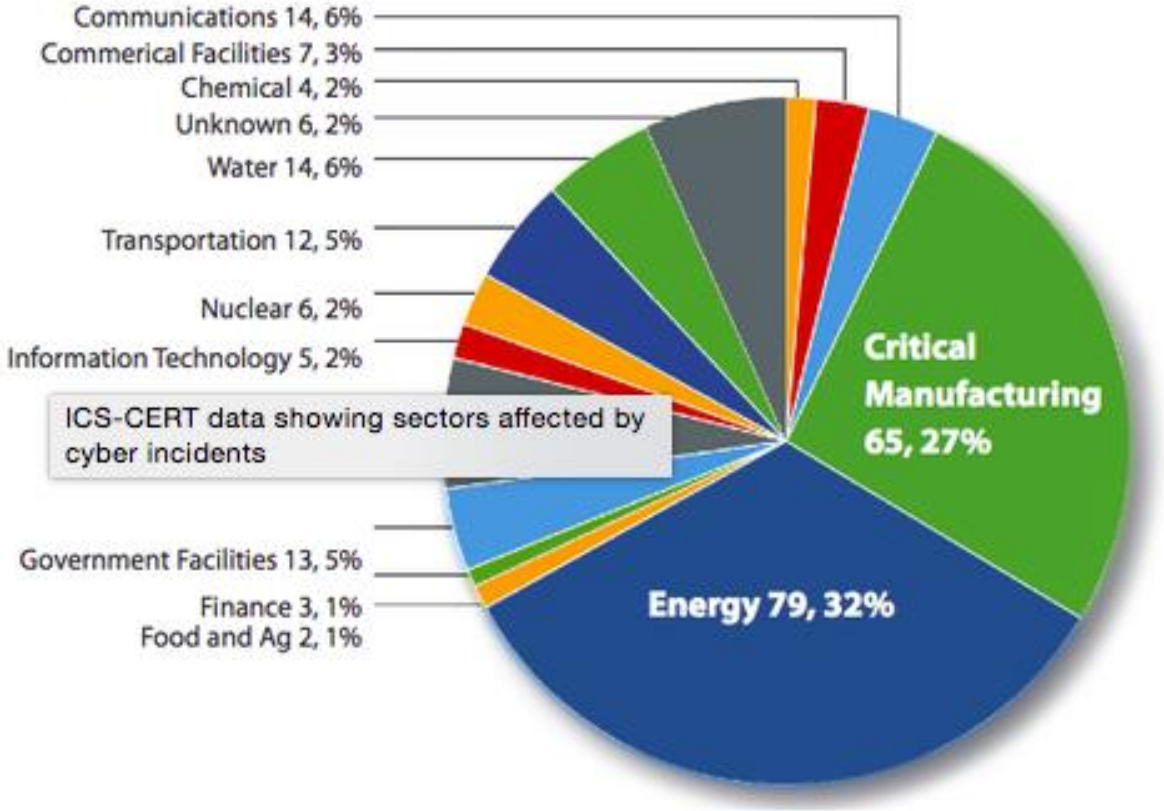
OAK RIDGE National Laboratory

Background

- News reports detailing increasing cyber attacks on industrial control systems led to ORNL management concerns
- ORNL COO directed the Office of Independent Oversight (IO) to conduct an assessment of cyber security of industrial control systems at ORNL
- The objective of this assessment was to perform a cyber security review of ORNL ICS at high risk nuclear and accelerator facilities to safely determine the vulnerabilities, risk and mitigations in place

Attacks on Industrial Control Systems

- US Department of Homeland Security ICS-CERT responded to 245 attacks on US industrial control systems in FY14



US Government a popular target

Forbes / Tech

The Little Black Book of Billionaire Secrets

JUN 11, 2015 @ 09:12 PM 14,994 VIEWS

Federal Union Says OPM Data Breach Hit Every Single Federal Employee

Records: Energy Department struck

Steve Reilly, USA TODAY 4:24 p.m. EDT September 11, 2015

USA TODAY producer Shannon Rae Green talks with investigative reporter Steve Reilly about the more than 150 times that cyber attackers successfully compromised the security of U.S. Department of Energy computer systems. USA TODAY

Attackers successfully compromised U.S. Department of Energy computer systems more than 150 times between 2010 and 2014, a review of federal records obtained by USA TODAY finds.

POLITICS | NATIONAL SECURITY

Government Personnel Cyber Breach Worse Than Previously Thought

Hackers stole fingerprint records of 5.6 million people, Office of Personnel Management says

OAK RIDGE National Laboratory

Approach

- The IO consulted with ORNL IT cyber team to plan review
- IO decided to engage an outside firm to conduct the review
- Assessment team was directed to focus on two areas:
  - The security posture of ICS implementations with respect to threats from the ORNL enterprise network and the ORNL supplied visitor network
  - The security posture of ICS implementations with respect to threats originating from remote access

How SNS prepared

- Conducted self assessment using DHS ICS-CERT Cyber Security Evaluation Tool (CSET) based on NIST 800-82
- Used the results of this analysis to make targeted improvements
  - Completed conversion to more rigorous account management
  - Added Intrusion Detection System
  - Audited all accounts and role authorizations including prox card access to server rooms
- Prepared package of relevant documentation: network diagram, policies, architecture, etc.
- Captured network data requested by assessors

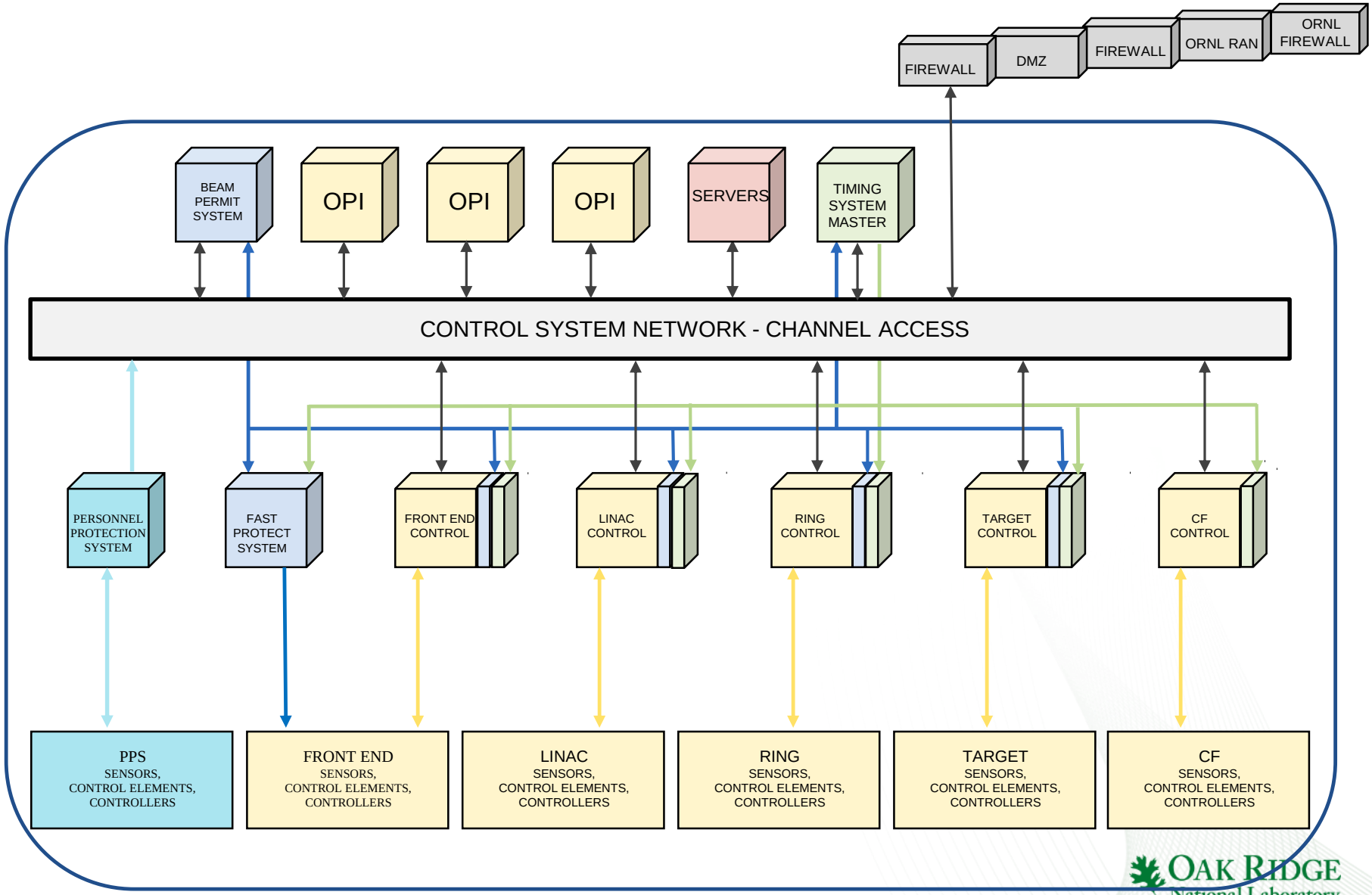
SNS ICS

- Large distributed system based on the Experimental Physics and Industrial Control System (EPICS) framework
- EPICS is developed by a collaboration across many laboratories and used for integrated control at US DOE labs and many others worldwide
- EPICS provides a flexible, layered architecture and integrates a variety of front end platforms
- This scalable, distributed architecture allows new devices, capability, functionality to be added as needed
- Emphasis on commercial, configurable, collaborative solutions

Protection Systems

- Two systems provide protection functions apart from the ICS
- Communication from protection systems to the ICS provides integrated status to operators but is not required for required shutdown to occur
- Machine Protection System shuts off the beam when predefined conditions are detected that may damage the machine
- Personnel Protection System shuts off the beam if entry to the accelerator enclosure is attempted during beam operations

SNS ICS Architecture



SNS ICS Isolation

- Isolated behind a firewall with limited exemptions
- No wireless access points on ICS network
- DMZ allows limited remote access for authorized staff using three factor authentication
- Read-only access is provided inside ORNL
- System is run in isolation mode (air gapped) when ORNL experiences elevated cyber security threats
  - No remote access or monitoring
  - Control and monitoring from dedicated control room only
- Controls system data
  - Includes code and real-time process variable values
  - No sensitive, confidential, classified or PII

SNS ICS System Administration

- System is administered in partnership with ORNL ITSD staff
  - Linux machines – Controls Group
  - Windows machines and network – ITSD
- System leverages ITSD cyber services and experts
  - UCAMS – passwords
  - ORNL external firewall
  - Two factor authentication
  - Intrusion Detection System
  - System log monitoring and analysis
  - Cyber incident response and investigation

SNS ICS Cyber Security

- Challenge is to achieve the proper balance between meeting control system requirements and keeping system secure
- Many specialized devices are needed to control unique accelerator subsystems
  - Devices generally do not offer cyber protection mechanisms available in typical enterprise IT solutions
- Access limited to authorized, trained staff
  - Accelerator operators and physicists
  - Accelerator subsystem support technicians and engineers

Assessment

- Assessment team
  - Reviewed provided documents and PCAP data
  - Interviewed ORNL ITSD and SNS staff
  - Toured facilities
  - Conducted wireless assessment

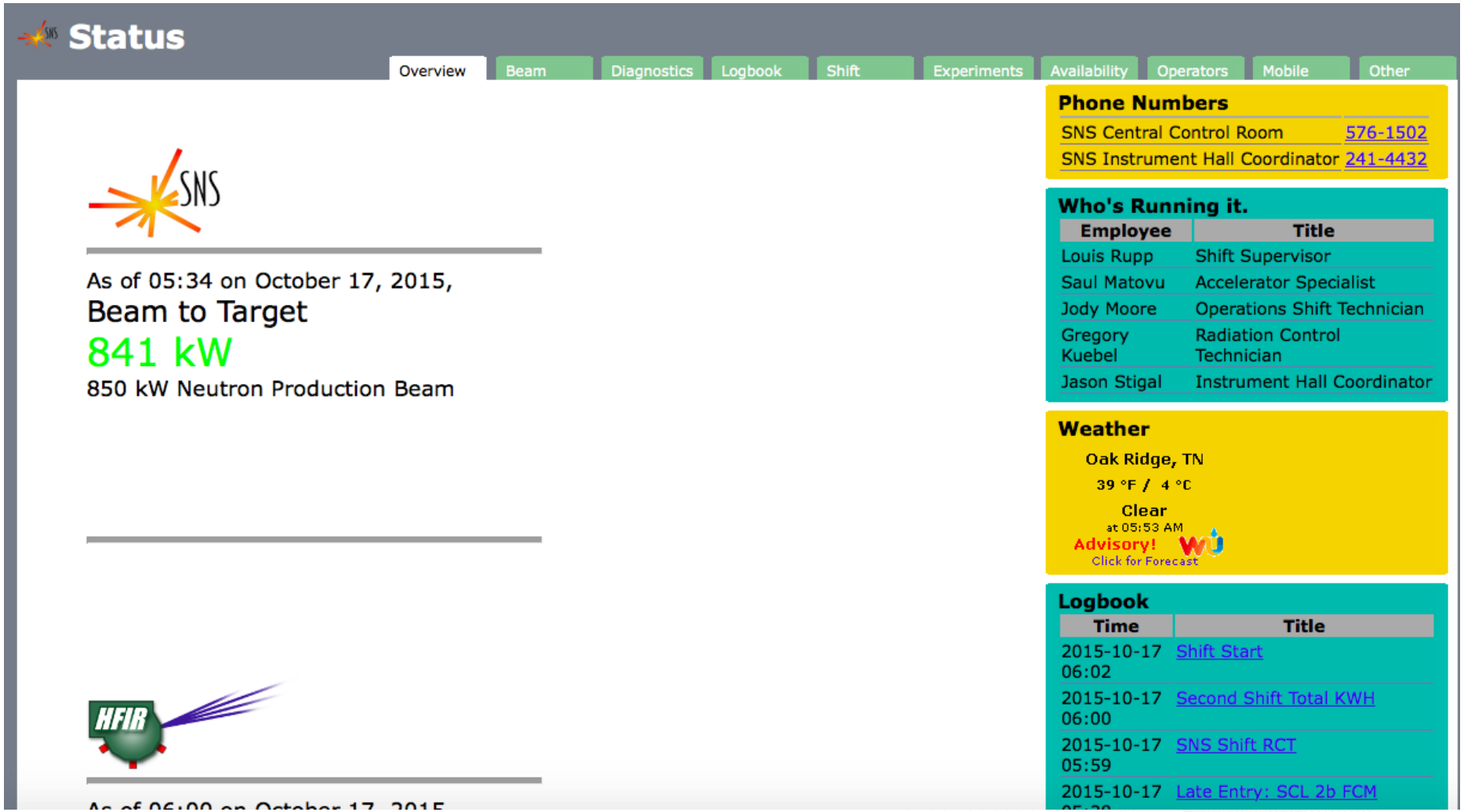
Review Summary

- Overall the HFIR network is in good shape but there is room for improvement
- SNS is doing a good job of securing their systems and equipment
- The decision to align controls with NIST Special Publication 800-82, *Guide to Industrial Control System (ICS) Security* puts SNS and HFIR on the right track to providing consistent, verifiable security
- The wireless assessment of the SNS facility did not turn up any unknown access points. Unknown access points were identified on the HFIR network

Opportunities for Improvement - SNS

- Until moving to a tool for maintaining the PLC logic files, extra care should be taken to verify any changes in the PLC logic before it is put into use
- Move the logbook status entries behind the password system already in place or enforce policy to restrict sensitive information from being placed on the publicly readable logbook
- The EPICS system should have some form of security assessment performed

External Website



Relevant Enterprise Recommendation

- Use digital signatures to verify that an e-mail is legitimate for functions like authorizing Prox card access

Conclusion

- Announcement of the upcoming review motivated us to take a more careful look at our cyber security provisions
- We were able to make some improvements based on our self assessment
- Improved self imposed policies and formalized existing practices
- ICS-CERT good resources for free on-line tools and training