



Commie Byrum

Physical Security Pathway Lead

crbyru@sandia.gov

Physical Security Pathway

2024 LWRS Program Spring Review Meeting

April 30, 2024

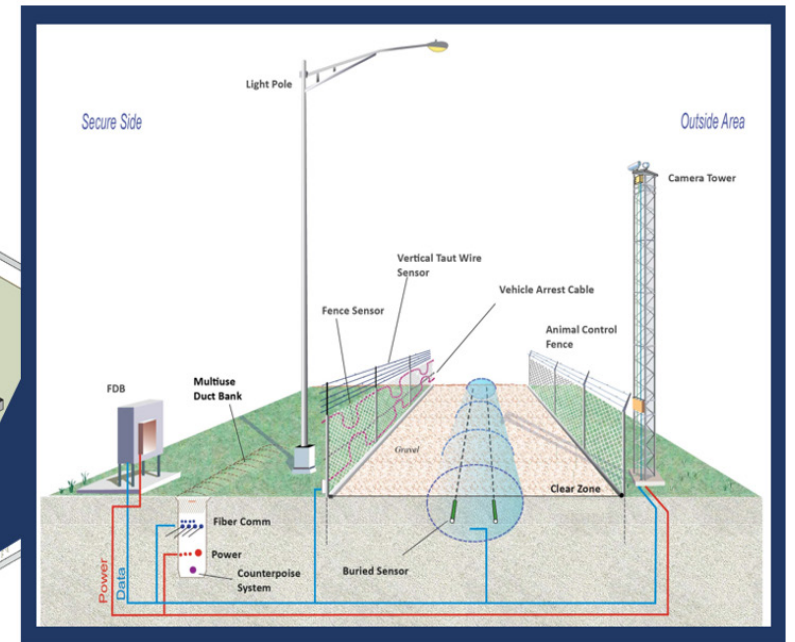
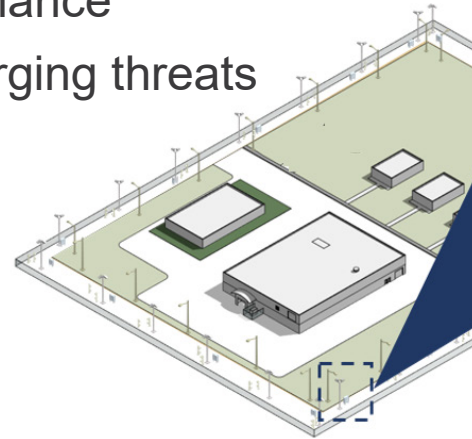


Summary – Physical Security Challenges

Fundamental architectures for physical security systems have changed little over the last 50 years

Challenges:

- Increasing labor costs
- Primarily compliance-based instead of performance-based
- Fixed infrastructure, which is costly and inflexible
- High nuisance alarm rates reduce performance
- Difficulty to adapt current systems to emerging threats
- Response relies on human variability



Perimeter intrusions detection system

Physical Security Pathway's Motivation and Overview

Why is LWRS focusing on Physical Security?

- Physical security accounts for approximately 20% of staffing at nuclear power plants
- There are many ways to reduce this percentage while maintaining security systems effectiveness

Physical Security research aims to create tools, technologies and capabilities for performance-based, risk-informed decision making with the following objectives:

- Develop mitigation strategies enhance the technical basis necessary for stakeholders to reevaluate physical security postures while meeting regulatory requirements
- Analyze the existing physical security regime and current best practices, compare/contrast insights with alternative methods that leverage advanced modeling and simulation, modern technologies, and novel techniques to address the design basis threat and regulatory requirements

Main research focus areas:

- Advanced Security Technologies
- Risk-Informed Physical Security
- Advanced Security Sensor and Barrier Systems



Force-on-force exercise



Unattended opening performance test

Summary – LWRS Physical Security Pathway Goals

Next generation security systems must leverage commercial investments integrated with advanced government technologies and methodologies to revolutionize current-day functions while addressing the 21st century evolving threats

Goals:

- Reduce need for costly infrastructure upgrades:
 - Design / Installation
 - Sustainment
 - Labor
- Leverage commercial technologies
- Threat agnostic
- Adaptable systems and technology management processes to minimize future system-wide overhauls
- Reduce nuisance alarm rates
- Increased survivability for security forces
- Common evaluation of overall physical protection system effectiveness
- Decision making based on performance-based, risk-informed security

Major Activities and Accomplishments

- Stakeholder Engagement Meetings
 - DEPO, Explosive, Adversary Timeline and Vulnerability Assessment Workshops
- Advanced Security Technologies
 - Remotely Operated Weapons System (ROWS) modeling of Riverbend and Monticello
- Risk-Informed Physical Security
 - Unattended openings – first report on performance-based risk-informed security
 - Conducted preliminary analyses for developing a dynamic risk-informed security methodology with Palo Verde
 - Expanded performance test data collection (security sensors, ballistics, and explosives)
 - Access for NRC licensees to 4 DOE Security System Desk References
- Advanced Security Sensor and Barrier Systems
 - Identified cost effective solution for microwave sensor testing
 - Completed two pilot studies of deliberate motion analytics with DC Cook and Waterford-III
 - Developed a shot detection capability for cameras and multiplexor boxes



Notional Modeling of External ROWS Placements



Aluminum and stainless-steel test spheres

Desired Impactful Outcomes within 3 years

Provide the technical basis for unattended openings (2D and 3D)
Provide access to technical documents from DOE's Office of Security and NNSA

- Fleet-wide application of risk-informed access / delay timelines for adversary and response force
- Support deployment of ROWS to at least one candidate site
- Pilot an integrated approach to dynamic force-on-force and reactor system response modeling
- Pilot the integration of human factors data and modeling for adversary and response force
- Support deployment of advanced sensor and delay technologies
 - Sensor fusion (water intakes)
 - Deliberate motion analytics (DMA)
 - Jam-resilient, cyber-hardened wireless (carbon wireless)
 - Ballistic detection for cameras and multiplexer boxes
 - Economical retrofits for added delay to vital areas



Active radar (blue) and thermal camera (yellow) fused through DMA showing both nuisance data and adversary track data; the red dots are the alarm indication.

Nuclear Industry Engagement

ROWS	UAO Unattended Openings	DMA Deliberate Motion Analytics	Water Intake Sensors	Dynamic Risk Framework	DOE VA Method Vulnerability Assessment	CARBON Wireless	Delay	DOE SBIR Small Business Innovative Research	DOE NEUP Nuclear Energy University Program
Entergy	Entergy	Entergy	TVA	APS	Constellation	Xcel Energy	APS	ARES	Ohio State
Xcel Energy	Xcel Energy	AEP	Xcel Energy	Southern Nuclear	Xcel Energy	NRC	Constellation	RhinoCorps	
Constellation	Constellation	Xcel Energy	Constellation	PWROG	NextEra/FPL				
NRC	NEI	NRC	PSEG	RhinoCorps	NEI				
	Stars Alliance			NRC	RhinoCorps				
	Dominion								
	SNC								
	NextEra								
	NRC								



Examples of tactical breaching and attack tools

Updates to DOE Security System Design References (SSDRs)

- DOE Environment, Health, Safety and Security (EHSS) EHSS-50 review of SSDRs
- Access Delay Volume 1 and 2
- Vulnerability assessment
- Entry control and contraband detection

- All SSDRs are limited distribution Unclassified Controlled Nuclear Information (UCNI)
- Available upon request after NRC review and approval of SSDRs:
 - NRC-approved data sources
 - NRC public notification process

- Remote Weapons System Safety Standard
 - Work in progress



Sustaining National Nuclear Assets

lwrs.inl.gov

Physical Security Pathway Milestone Reports

Research Thrust Area	Report Name	Report Number
Advanced Security Technologies	<i>Enhanced force-on-force modeling to support the technical basis of an advanced remote operated weapons technology for use at a candidate nuclear power plant site</i>	-
	<i>Technical Basis for Remote Operated Weapon System Deployment at Nuclear Power Plants</i>	Sandia R&A: 1197224
	<i>Remote Operated Weapon System Deployment at Nuclear Power Plants – Excerpt for Commercial Nuclear Power Plants</i>	Sandia R&A: 1208137
	<i>ROWS Tower Structural Response to Bulk Explosive Attacks</i>	SAND2020-12697 PE
	<i>Force-on-force Modeling of Remote Operated Weapon Systems for use at a Candidate Nuclear Power Plant Site</i>	-
	<i>Continued Dante Study of Physical Security Upgrades at Nuclear Power Plant Sites</i>	-
	<i>Technical Basis for Remote Operated Weapon System Deployment at Nuclear Power Plants – Revision 1</i>	Sandia R&A: 1630475
	<i>FY23 Mid-Year Update of ROWS Modeling Physical Security Updates</i>	Sandia R&A: 1630477
	<i>Technical Basis for Remote Operated Weapon System Deployment at Nuclear Power Plants – Revision 2</i>	Sandia R&A: 1701849
	<i>Model-based Solution for the use in a Remote Operated Weapon System Simulator using a Formal Deployment Strategy Plan</i>	Sandia R&A: 1710377
	<i>Technical Basis for Remote Operated Weapon System Deployment at Nuclear Power Plants – Revision 3</i>	Sandia R&A: 1722289

Research Thrust Area	Report Name	Report Number
Advanced Security Sensor and Barrier Systems	<i>Research Roadmap for Advanced Physical Security Sensor/Barrier Technology</i>	SAND2021-9771
	<i>Microwave Responses for Varied Stimuli</i>	SAND2022-4078
	<i>Analog Microwaves and Target Velocity</i>	SAND2022-3543
	<i>Pilot Deployment of the Deliberate Motion Analytics Sensor System at the Donald C. Cook Nuclear Plant</i>	SAND2022-7758 O
	<i>Preliminary Study for Detection of Swimmers at Water Intakes for Nuclear Power Plants</i>	Sandia R&A: 1630070
	<i>Physical Security Meetings at Site 362</i>	SAND2022-3542
	<i>Analog Microwaves and Target Velocity</i>	SAND2022-3543
	<i>Microwave Response for Varied Stimuli</i>	SAND2022-4078
	<i>Pilot Deployment of the Deliberate Motion Analytics Sensor System at the Waterford III Nuclear Plant</i>	SAND2022-14815 R
	<i>Microwave Sensor Performance at “Slow” Setting and Alternate Stainless Steel Test Target for Microwaves</i>	SAND2022-15618 R
	<i>Deliberate Motion Analytics Commercialization and Technology Transfer</i>	Sandia R&A: 1664515
	<i>Access Delay Concepts to Enhance Security for Domestic Nuclear Power Plant Sites</i>	Sandia R&A: 1675952
	<i>Preliminary Study for Detection of Swimmers at Water Intakes for Nuclear Power Plants – Update</i>	Sandia R&A: 1709040
	<i>Deliberate Motion Analytics Commercialization and Technology Transfer – Revision 1</i>	SAND2023-09100 R
	<i>Pilot Deployment of the CARBON Wireless Networking System for Nuclear Power Plants</i>	Sandia R&A: 1722279
<i>Access Delay Technologies to Vital Areas for Domestic Nuclear Power Plant Sites</i>	Sandia R&A: 1722335	

Physical Security Pathway Milestone Reports – continued

Research Thrust Area	Report Name	Report Number
Risk-Informed Physical Security	<i>Domestic Nuclear Power Plant Physical Security Reevaluation – High-Level Project Plan</i>	SAND2018-12483
	<i>Initial Physical Security Assessment of Domestic Nuclear Power</i>	SAND2019-9063
	<i>Joint INL/SNL Physical Security Evaluation</i>	SAND2019-11878
	<i>Current Challenges, Constraints, and Recommendations for Reducing Costs of Physical Security at U.S. Commercial Nuclear Power Plants</i>	INL/EXT-19-54452
	<i>Physical Security Initiative Site Visit of the Monticello Generating Plant – April 16-18, 2019 – Trip Report</i>	INL/EXT-19-54297
	<i>Modeling for Existing Nuclear Power Plant Security Regime</i>	SAND2019-12015
	<i>Lone Pine Nuclear Power Plant Description</i>	SAND2019-12227
	<i>Integration of FLEX Equipment and Operator Actions in Plant Force-On-Force Models with Dynamic Risk Assessment</i>	INL/EXT-20-59510
	<i>Economic Analysis of Physical Security at Nuclear Power Plants</i>	INL/EXT-20-59737
	<i>Methodology and Application of Physical Security Effectiveness Based on Dynamic Force-on-Force Modeling</i>	INL/EXT-20-59891
	<i>September 2019 Physical Security Stakeholder Working Group Meeting</i>	SAND2020-0764
	<i>Light Water Reactor Sustainability Program: November 2019 Physical Security Stakeholder Working Group Meeting</i>	SAND2020-4616
	<i>Evaluate Tools and Technologies that Would Benefit the Advancement of Risk-Informed Models</i>	SAND2020-9055
	<i>Risk Informed Access Delay Timeline Development</i>	SAND2020-9176
	<i>Development of Performance-Based Metrics for Overall Physical Security System Effectiveness</i>	SAND2020-9430
<i>Risk Informed Timeline Tool</i>	SAND2021-9430	

Research Thrust Area	Report Name	Report Number
Risk-Informed Physical Security	<i>A Review of Risk-Informed Approaches for Physical Security</i>	SAND2021-10500
	<i>Performance Testing of Person-Passable Unattended Openings</i>	SAND2021-12792
	<i>Guidance Document for Using Dynamic Force-on-Force Tools</i>	INL/EXT-21-64214
	<i>Integration of Physical Security Simulation Software Applications in a Dynamic Risk Framework</i>	INL/EXT-21-64333
	<i>Security System Desk Reference – Interim Access Delay</i>	SAND2021-15454
	<i>Performance Testing of Person-Passable Unattended Openings – Revision 2</i>	SAND2022-5525
	<i>Enhancing Sites’ Physical Security through a Structured Performance-Based Assessment Framework</i>	Sandia R&A: 1677363
	<i>Evaluation of Physical Security Risk for Potential Implementation of FLEX using Dynamic Simulation Methods</i>	INL/EXT-22-70315
	<i>Plant-Specific Model and Data Analysis using Dynamic Security Modeling and Simulation</i>	INL/RPT-23-73490
	<i>Risk-Informed Security Optimization Recommendations</i>	INL/RPT-23-74548
	<i>Enhancing Sites’ Physical Security through a Vulnerability Assessment Process</i>	Sandia R&A: 1722301