April 02, 2021

Gustavo Reyes
Safeguards & Security Specialist, Idaho National Laboratory

Fission Battery Initiative

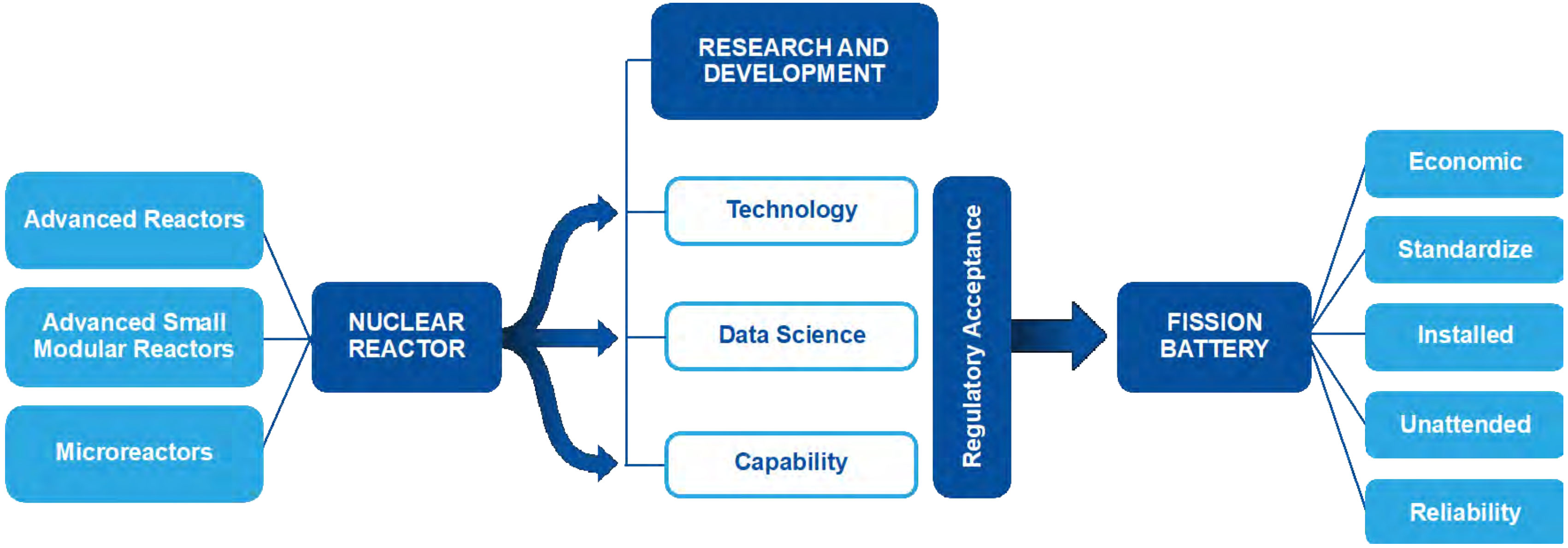
Nuclear Science and Technology

Idaho National Laboratory

Fission Battery Initiative

Vision: Developing technologies that enable nuclear reactor systems to function as batteries.

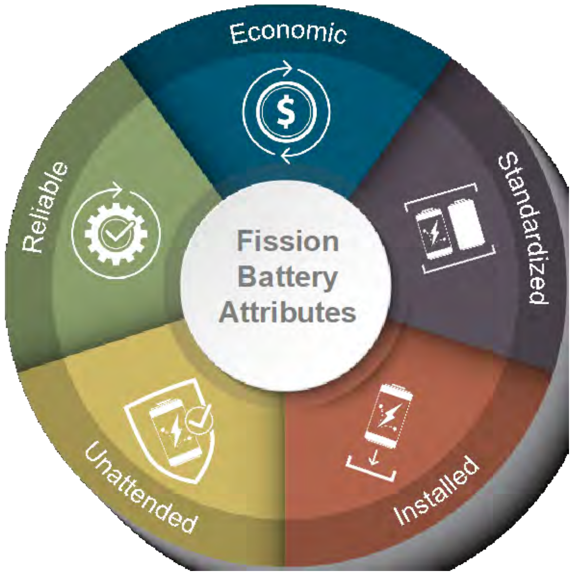
Outcome: Deliver on research and development needed to provide technologies that achieve key fission battery attributes and expand applications of nuclear reactors systems beyond concepts that are currently under development.



Research and development to enable nuclear reactor technologies to achieve fission battery attributes

Fission Battery Attributes

- **Economic** – Cost competitive with other distributed energy sources (electricity and heat) used for a particular application in a particular domain. This will enable flexible deployment across many applications, integration with other energy sources, and use as distributed energy resources.
- **Standardized** – Developed in standardized sizes, power outputs, and manufacturing processes that enable universal use and factory production, thereby enabling low-cost and reliable systems with faster qualification and lower uncertainty for deployment.
- **Installed** – Readily and easily installed for application-specific use and removal after use. After use, fission batteries can be recycled by recharging with fresh fuel or responsibly dispositioned.
- **Unattended** – Operated securely and safely in an unattended manner to provide demand-driven power.
- **Reliable** – Equipped with systems and technologies that have a high level of reliability to support the mission life and enable deployment for all required applications. They must be robust, resilient, fault tolerant, and durable to achieve fail-safe operation.



Fission Battery Workshop Series

- **Jointly INL and National University Consortium are organizing workshops across five areas:**
  - Market and Economic Requirements for Fission Batteries and Other Nuclear Systems
  - Technology Innovation for Fission Batteries – Next workshop is February 24, 2021
  - Transportation and Siting for Fission Batteries – March 15, 2021
  - Domestic & International Safeguards & Security for Fission Batteries – April 02, 2021
  - Safety and Licensing of Fission Batteries – April 16, 2021

- **Expected outcomes:**
  - Each workshop outcomes are expected to outline the goals of each fission battery attribute

Today's agenda

Session 1: Nuclear Safeguards
(Session Chair: Gustavo Reyes, INL)

02 April 2021
All U.S. Eastern Time

10:00	Opening Statement and Introduction	Gustavo Reyes (INL)
10:10	International Computer Security Strategy – IAEA Pub	Trent Nelson (IAEA)
10:20	Safeguards Ideas on Microreactors/FB	Frederik Reitsma (USNC)
10:30	Pragmatic Security of Unconventional Power Sources	Shawn Datres (PNNL)
11:00	Panel Discussion 1 *Moderator*: Gustavo Reyes, INL *Panelists*: Trent Nelson, IAEA Frederik Reitsma, USNC Shawn Datres, PNNL	
11:30	Break	15 Minutes
11:45	Target Set Analysis Tools & Needs for FB	Steven Prescott (INL)
12:00	Physical Protection Systems Strategies for FB	Alan Evans (SNL)
12:15	Security Economic Analysis on FB	Pralhad Burli (INL)
12:45	Panel Discussion 2 *Moderator*: Raymond Cao, OSU *Panelists*: Steven Prescott, INL Alan Evans, SNL Pralhad Burli, INL	
13:15	Break	45 minutes

Session 2: Nuclear Security
(Session Chair: Carol Smidts, OSU)

14:00	Opening Statement and Introduction	Carol Smidts (OSU)
14:10	FB's Place in the INS Civilian Nuclear Security Project	Doug Osborn (SNL)
14:20	Additional Physical Security Considerations for FB	Adam Williams (SNL)
14:30	Cyber-Informed Engineering – S&S of FB	Robert Anderson (INL)
14:40	Panel Discussion 3 *Moderator*: Cassiano Endres de Oliveira, UNM *Panelists*: Doug Osborn, SNL Adam Williams, SNL Robert Anderson, INL	
15:10	Break	15 Minutes
15:25	Zero Trust Security for Fission Batteries	Indrajit Ray (CSU)
15:35	Cross-Layer Cyber-Physical Security of FB Control Systems	Quanyan Zhu (NYU)
15:45	Experimental Testbeds & Cyber Hardening of FB	Robert England (INL)
15:55	Panel Discussion 4 *Moderator*: Carol Smidts, OSU *Panelists*: Indrajit Ray, CSU Quanyan Zhu, NYU Robert England, INL	
16:25	Closing Remarks	Gustavo Reyes (INL)
16:35	End	

INL

Idaho National Laboratory

IAEA
International Atomic Energy Agency
Atoms for Peace and Development

International Computer Security Strategy – IAEA Publication

Trent Nelson

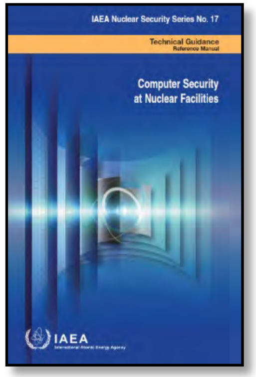
Division of Nuclear Security

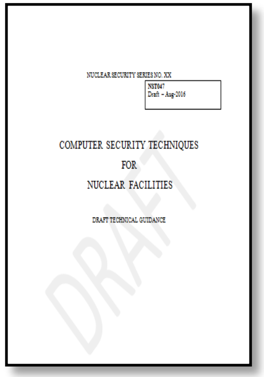
2 April, 2021

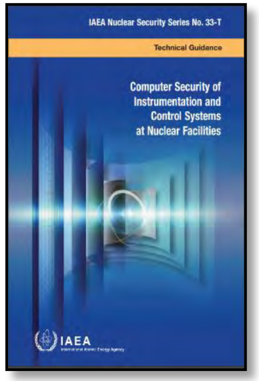
IAEA Role in Computer Security

Raise awareness of the threat of cyber-attacks, and their potential impact on nuclear security & assist Member States, upon request, in improving computer security capabilities at State organizations and licensees through:

- Guidance Development
- Information Exchange







- Training Courses
- Coordinated Research Projects (CRP)

IAEA Nuclear Security Series Publications

Primary information and computer security publications references

IAEA

Fundamentals (PRINCIPLES) – NSS20

- Objectives and principles
- Basis for Nuclear Security Recommendations
- Essentials from international instruments

Recommendations (WHAT) – NSS 13, 14, 15

- General approaches, actions, concepts and strategies
- Applications of Fundamentals
- Suggested Recommendations Level Computer Security Guidance – NST045 Annex

Implementing Guides (HOW) – NSS 23-G & NSS 42-G

- Broad guides on applying Recommendations
- NSS 23-G – Security of Nuclear Information
- **NSS 42-G (NST045) - Computer Security for Nuclear Security**
  - Suggested Recommendations Level CS Guidance – NSS 42 - G Annex

Technical Guides (DETAILS) – NSS 17-T Rev 1 & NSS 33T

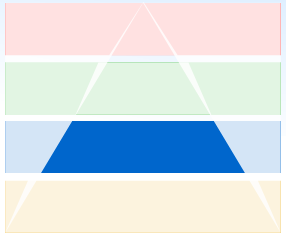
- Reference Manuals, Training Guides, Service Guides
- **NSS 17-T Rev. 1 - Computer Security Techniques for Nuclear Facilities**
- **NSS 33T - Computer Security for I&C Systems at Nuclear Facilities**

Non-serial publications:

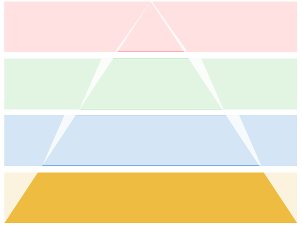
- Computer Security Incident Response Planning **– TDL-005**
- Conducting Computer Security Assessments – **TDL-006**
- **Computer Security Approaches to Reduce Cyber Risk in the Nuclear Supply Chain (2021)**
- Computer security exercises for nuclear security (2021)

Overview of information and Computer Security Publications

State Nuclear Security Regime	• Sensitive Information • Roles and Responsibilities • **Strategy** • The Threat	• NSS23-G • **NSS42-G** (NST045)
Organizational Frameworks for Information Protection	• **Laws and Regulation** • Information Security Policy • Computer Security Programme (CSP) • Risk Informed Approach • Security Culture	• NSS23-G • **NSS42-G** (NST045)
Nuclear Facility CSP Implementation	• Facility Analysis: Functions and Systems	• NSS17-T Rev 1 (NST047)
Risk Assessment	• **Vulnerability Analysis** • **Risk Determination** • **Sensitive Information and Sensitive Digital Asset (SDA) Identification**	• **NSS17-T Rev 1** (NST047)
Digital Asset Protection	• **Computer Security Measure** Implementation	• **NSS17-T Rev 1** (NST047) • **NSS33-T**

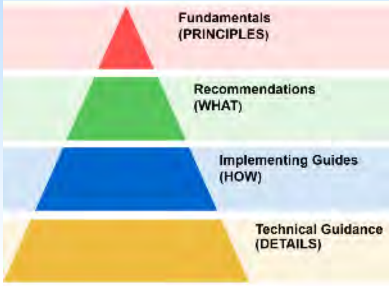


Implementing



Technical Guidance

NSS 13 – Physical Protection of Nuclear Material and Nuclear Facilities



- Contains some guidance on Information and Computer Security recommendations.
- Recommends both a information security (e.g. traditional classification of information) and function based approach (e.g. protection from cyber-attack).

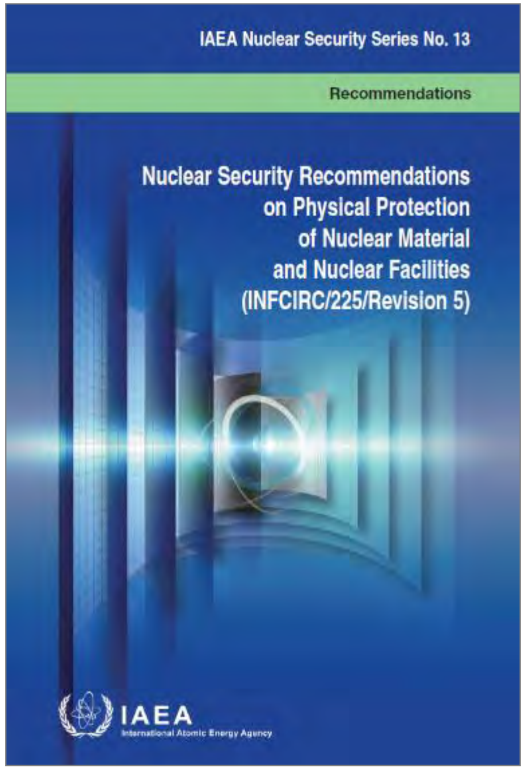
“4.10. Computer based systems used for

- *physical protection*,
- *nuclear safety*, and
- *nuclear material accountancy and control*

should be protected against compromise

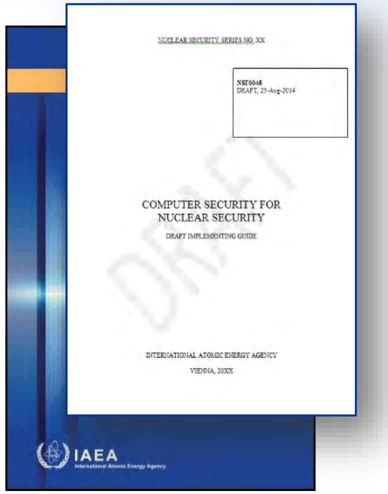
(e.g. **cyber attack, manipulation or falsification**)

consistent with the threat assessment or design basis threat.”

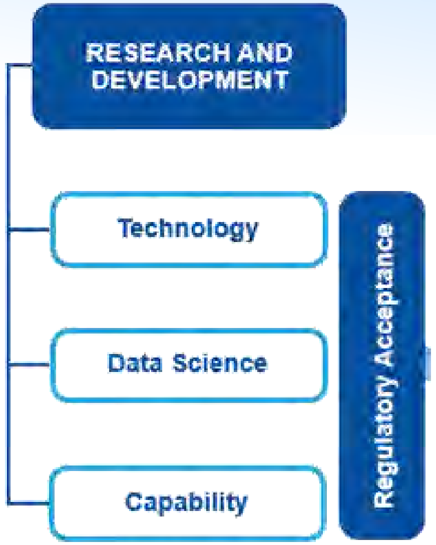


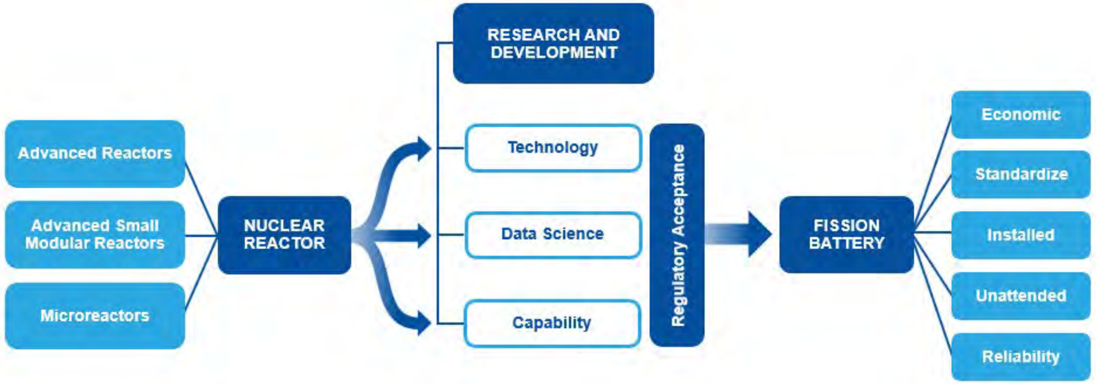
NSS 42-G (draft NST-045) – Computer Security for Nuclear Security State Level Guidance

- NSS 42-G provides guidance on developing and implementing **computer security requirements** for Nuclear security
  - State roles, responsibilities, and strategy
  - Computer Security Program
- NSS 42-G Cross Cutting guidance NSS13, 14, and 15
- Defines the need for a State level Strategy
- Focuses on Recommendations (requirements) **Annex 1 – Suggested recommendation Level Guidance** on Computer Security for Nuclear Security Requirements/Regulation



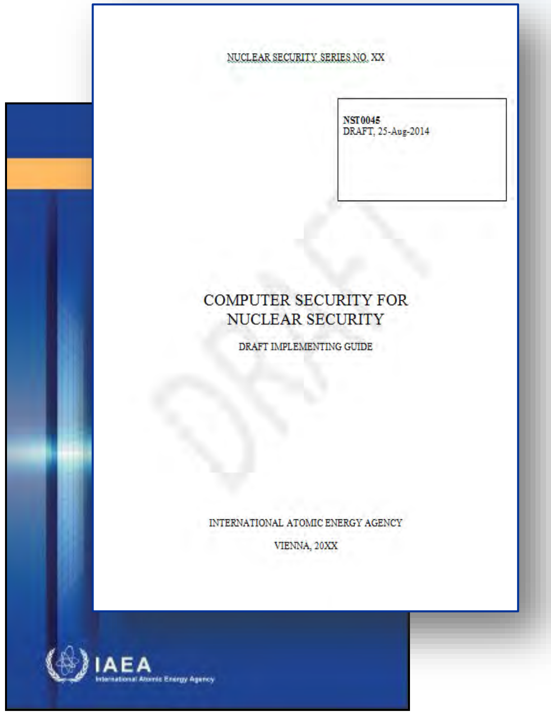
To be Published in Q2 2021





NSS 17-T Rev 1 (draft NST047) – Computer Security Techniques for Nuclear Facilities

- Technical Guidance
- Interfaces with the State/CA (NSS 42-G) and I&C (NSS 33-T)
- Follows the lifecycle of facility
- Provides guidance on:
  - **CS Risk Management Program** (facility & systems)
  - **Defensive Computer Security Levels and Zones**
  - Policies and Procedures


NUCLEAR SECURITY SERIES NO. XX

NST0045
DRAFT, 25-Aug-2014

COMPUTER SECURITY FOR NUCLEAR SECURITY

DRAFT IMPLEMENTING GUIDE

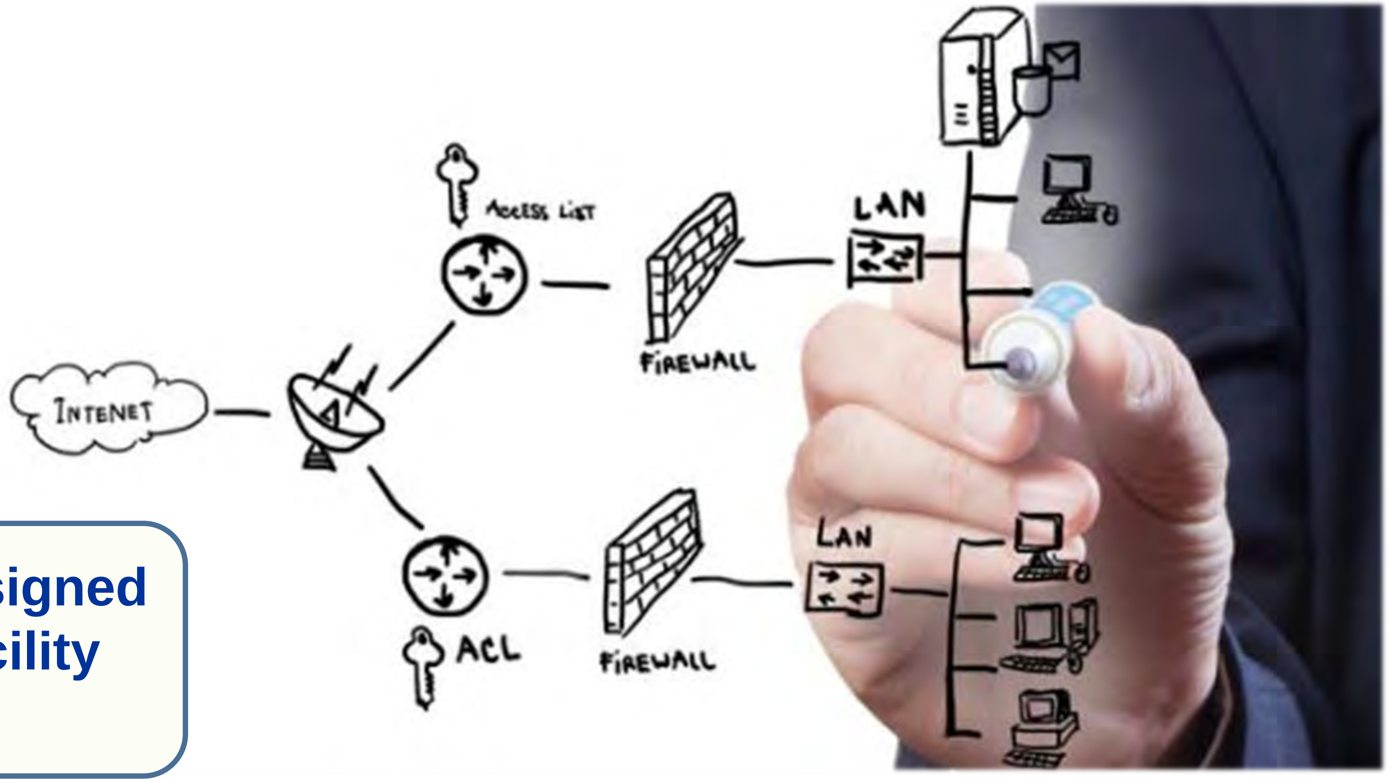
INTERNATIONAL ATOMIC ENERGY AGENCY

VIENNA, 20XX

To be Published in Q2 2021

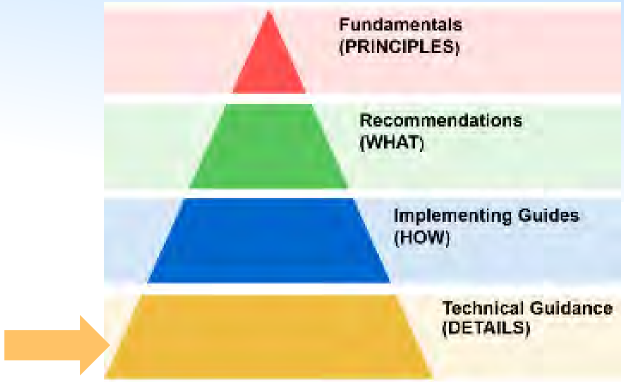
Defensive Computer Security Architecture (DCSA)

The operator should specify an overall DCSA for the computer security of I&C systems in which all I&C systems are assigned a security level and protected according to the applicable requirements.



The DCSA is designed to preserve facility functions

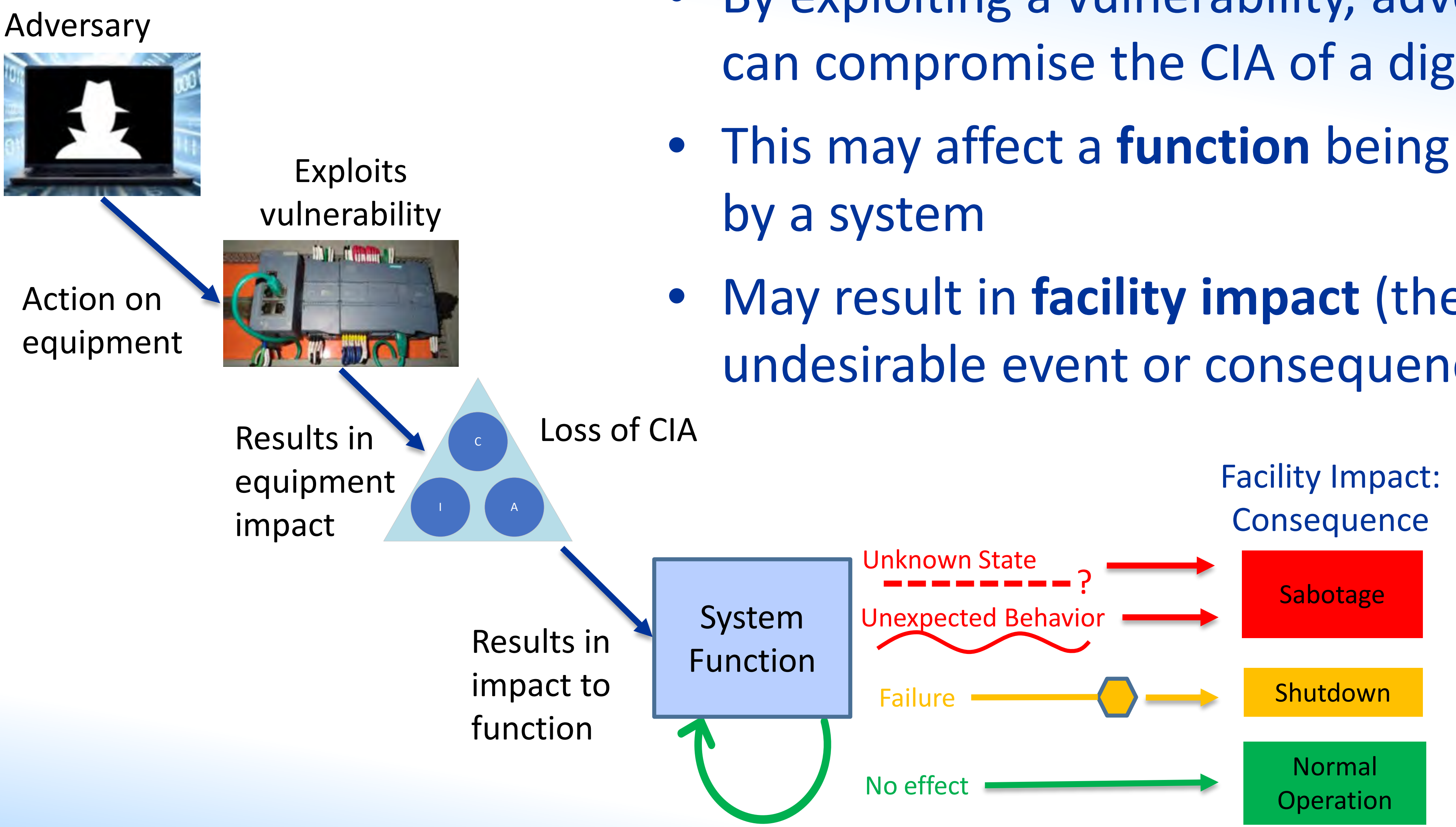
NSS 33-T – Computer Security of I&C Systems at Nuclear Facilities



- Nuclear I&C designers have robust processes in place to ensure systems provide for safe, reliable, and deterministic behavior.
- NSS 33-T aims to **overlay computer security considerations** on top of these processes to meet safety and security objectives.
- Nuclear I&C Systems provide safety functions:
  - May be targeted by adversaries for sabotage resulting in Unacceptable or High Radiological Consequences (URC or HRC)
  - A cyber-attack can cause an initiating event and/or can undermine the performance of a safety function

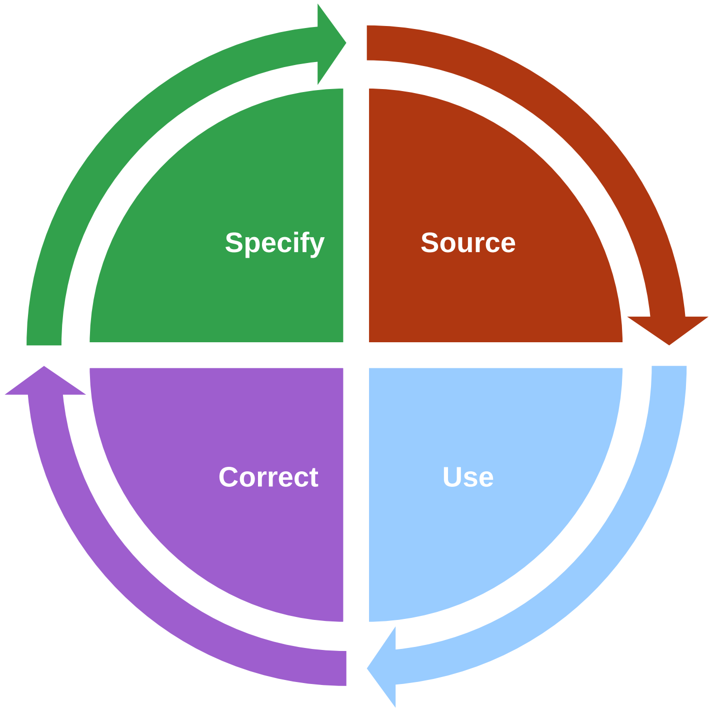
NSS 33-T – Computer Security of I&C Systems at Nuclear Facilities

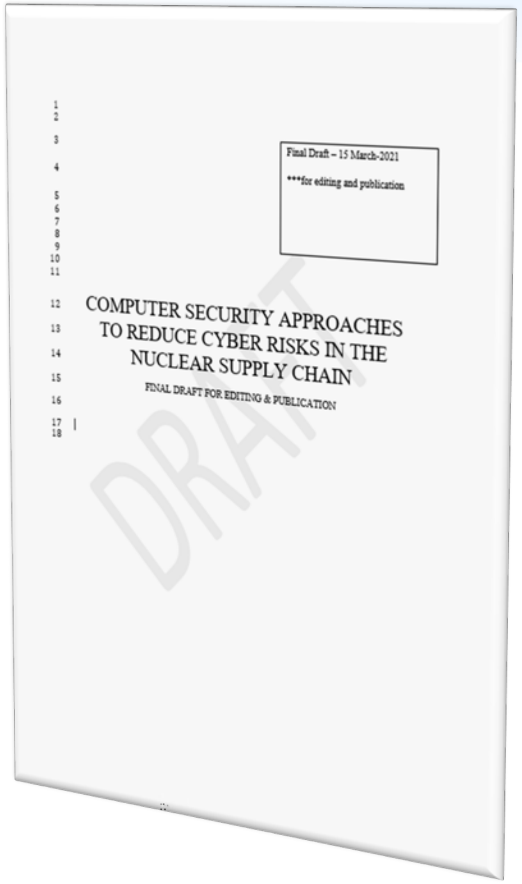
- By exploiting a vulnerability, adversaries can compromise the CIA of a digital asset
- This may affect a **function** being performed by a system
- May result in **facility impact** (the undesirable event or consequence)



Introduce a NEW - Computer Security Approaches To Reduce Cyber Risks in the Nuclear Supply Chain (non-serial publication – Q3 2021)

- Document History
- Objective - provide guidance to manage computer security risk in the supply chain
  - Supply Chain Complexity
  - Guidance on Computer Security
  - Supply Chain Attack Surface
  - Four Staged Approach to Supply Chain





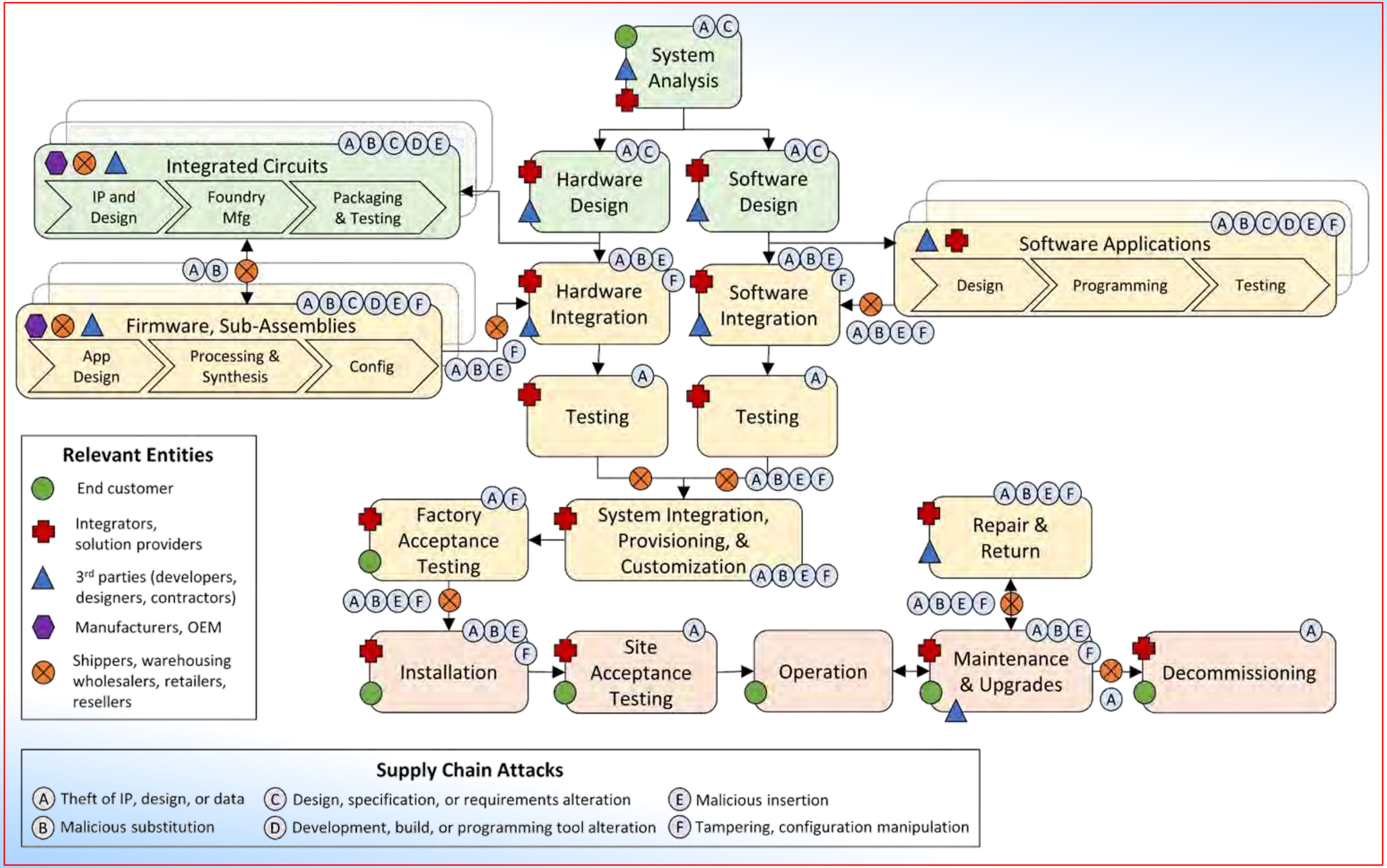
Final Draft – 15 March 2021
***for editing and publication

COMPUTER SECURITY APPROACHES TO REDUCE CYBER RISKS IN THE NUCLEAR SUPPLY CHAIN

FINAL DRAFT FOR EDITING & PUBLICATION

DRAFT

Supply Chain Attack Touchpoints



IAEA
International Atomic Energy Agency
Atoms for Peace and Development

Trent Nelson
Nuclear Security Information Officer
International Atomic Energy Agency
Vienna International Centre
A-1400 Wien
Austria
Tel: +43 (1) 2600-26424
t.nelson@iaea.org

Thank you!

The Role of the IAEA

Nuclear security is a *national responsibility*

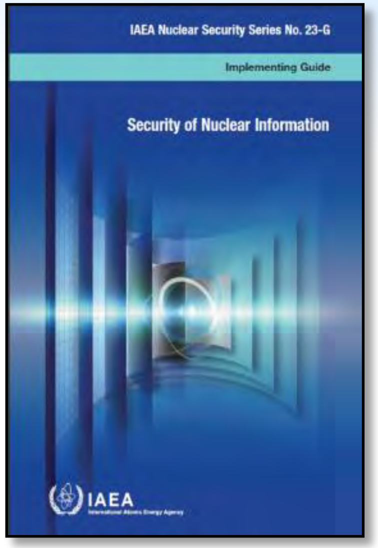
The IAEA:

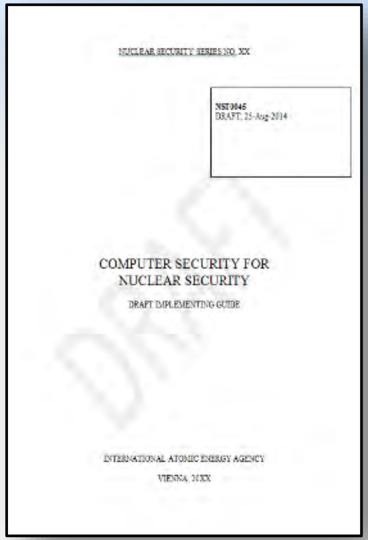
- Supports States, upon request, in their efforts to establish and maintain ***effective nuclear security*** through assistance in capacity building, guidance or standards, human resource development and risk reduction

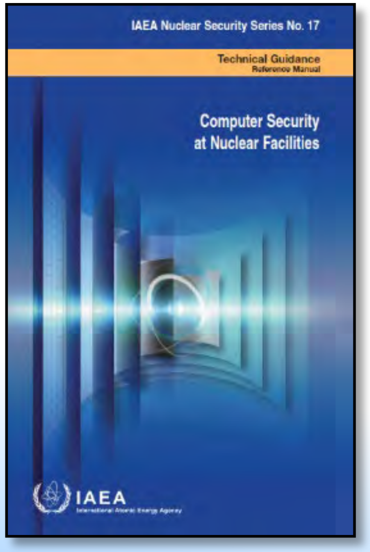
- Facilitates adherence to implementation of international legal instruments related to nuclear security

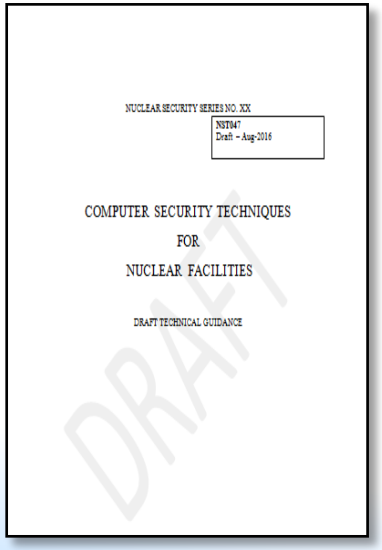
NSS Information and Computer Security Publications

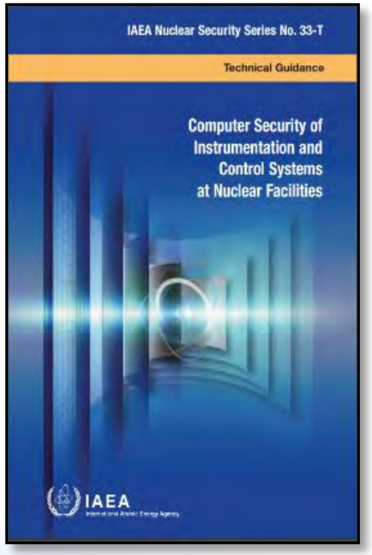
- NSS 23-G Security of Nuclear Information
- NSS 42-G (2021, draft NST045) Computer Security for Nuclear Security









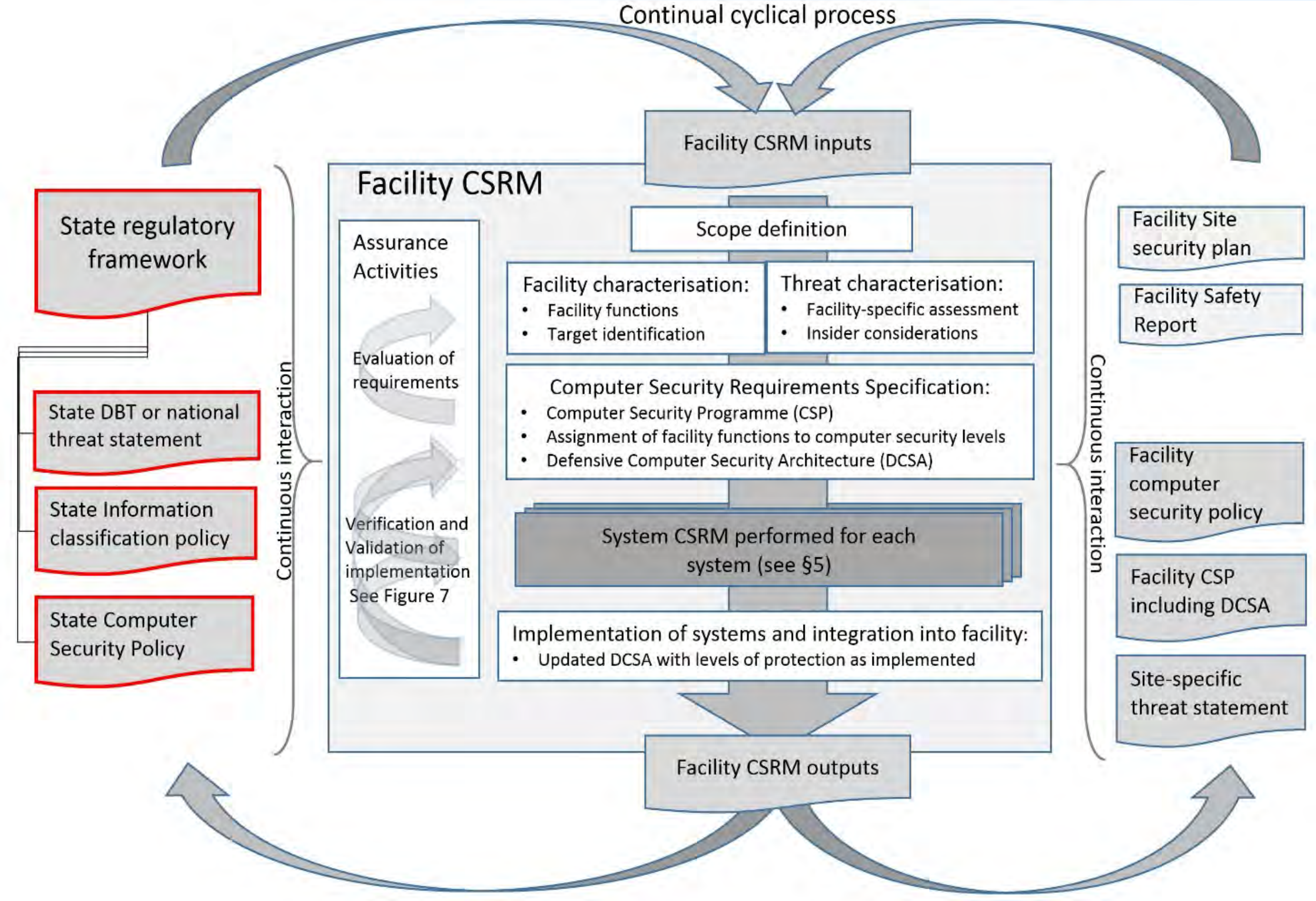


- NSS 17 - Computer Security at Nuclear Facilities
- NSS 17-T Rev 1 (2021, NST047) - Computer Security Techniques for Nuclear Facilities
- NSS 33-T Computer Security of I&C Systems at Nuclear Facilities

NSS 17-T Rev 1 (draft NST047) – Computer Security Techniques for Nuclear Facilities

Facility Computer Security Risk Management (FCSRM)

- IAEA guidance describe how to establish systems and programmes to manage the risks of a cyber-attack:
  - across a State (NSS 42-G);
  - within a nuclear facility (NSS 17-G Rev 1);
- This diagram shows interaction with safety and security while highlighting distinct processes occurring for Computer Security.



Safeguards ideas on microreactors / fission batteries

Frederik Reitsma

Director for Analysis

frederik.reitsma@usnc.com

ULTRA SAFE NUCLEAR CORPORATION

www.usnc.com

info@usnc.com

Twitter: @UltraSafeNuke

Menu of the day

– Who is Ultra Safe Nuclear Corporation

– The Micro Modular Reactor (MMR)

– Micro- SMRs and Fission Batteries: Why the distinction? Are they the same?

– The IAEA guidance – what can we learn

– Safeguards and proliferation resistance aspects – Some thoughts

Ultra Safe Nuclear Corporation

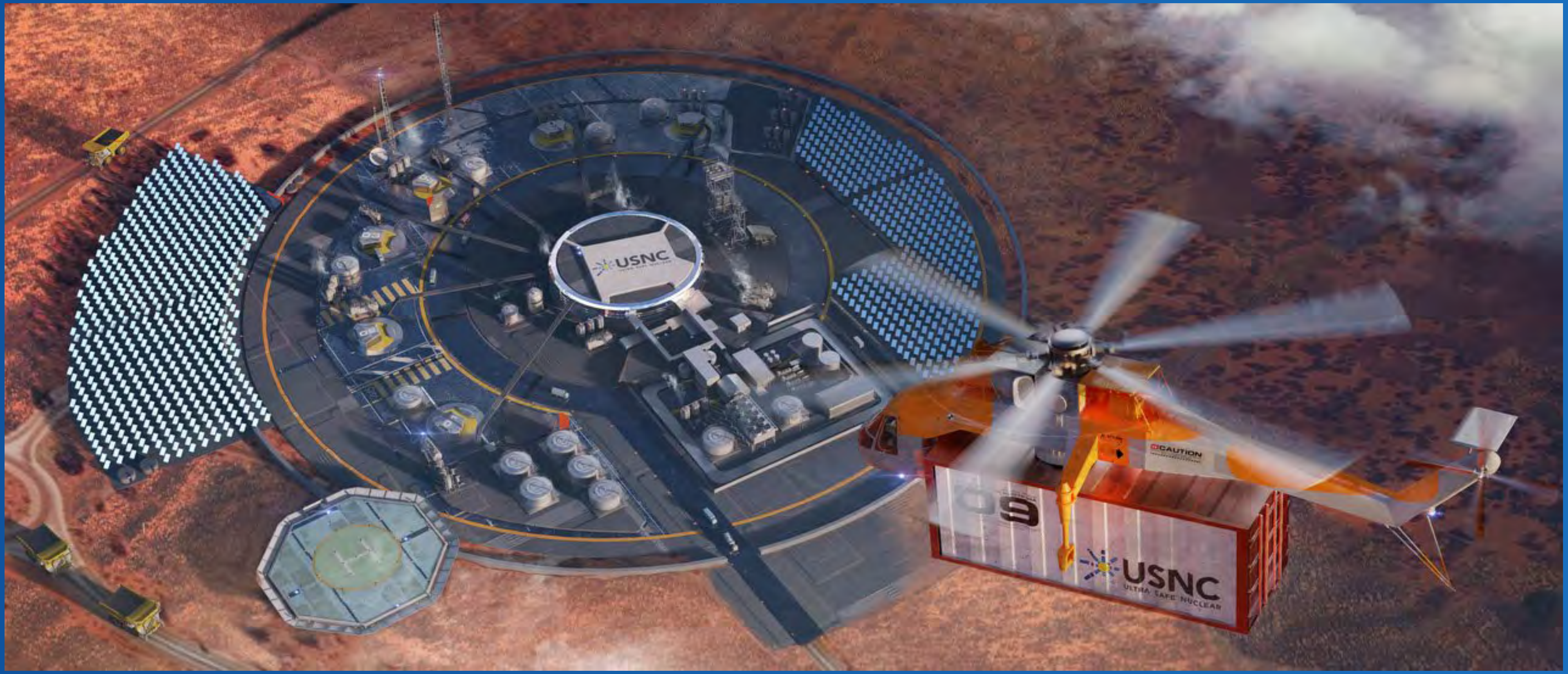
Clean Reliable Power **Anywhere**

Started 2011 / 100+ employees today

Private Investment:
2010-2019: 20M
2019-2020: 30M
2021-2024: 500M

What is unique about USNC:

- Technology (ultra safe fuel and reactor design) – safe to public, environment and investment
- Small size of individual project, infinite scalability of model –
- Aim to be the first micro reactor power (commercial partnership with Ontario Power
- Clear path to near-term profitability



www.usnc.com

Progress to executing Canada's First SMR Project

- Vendor design review with the CNSC is entering Phase 2.
- First agreement to site at CNL/AECL signed
- Active application for an Environmental Assessment and License to Prepare Site
- GFP Partnership established with OPG to build, own, and operate the plant
- Plan to bring Canada's first SMR into operation …. coming soon!

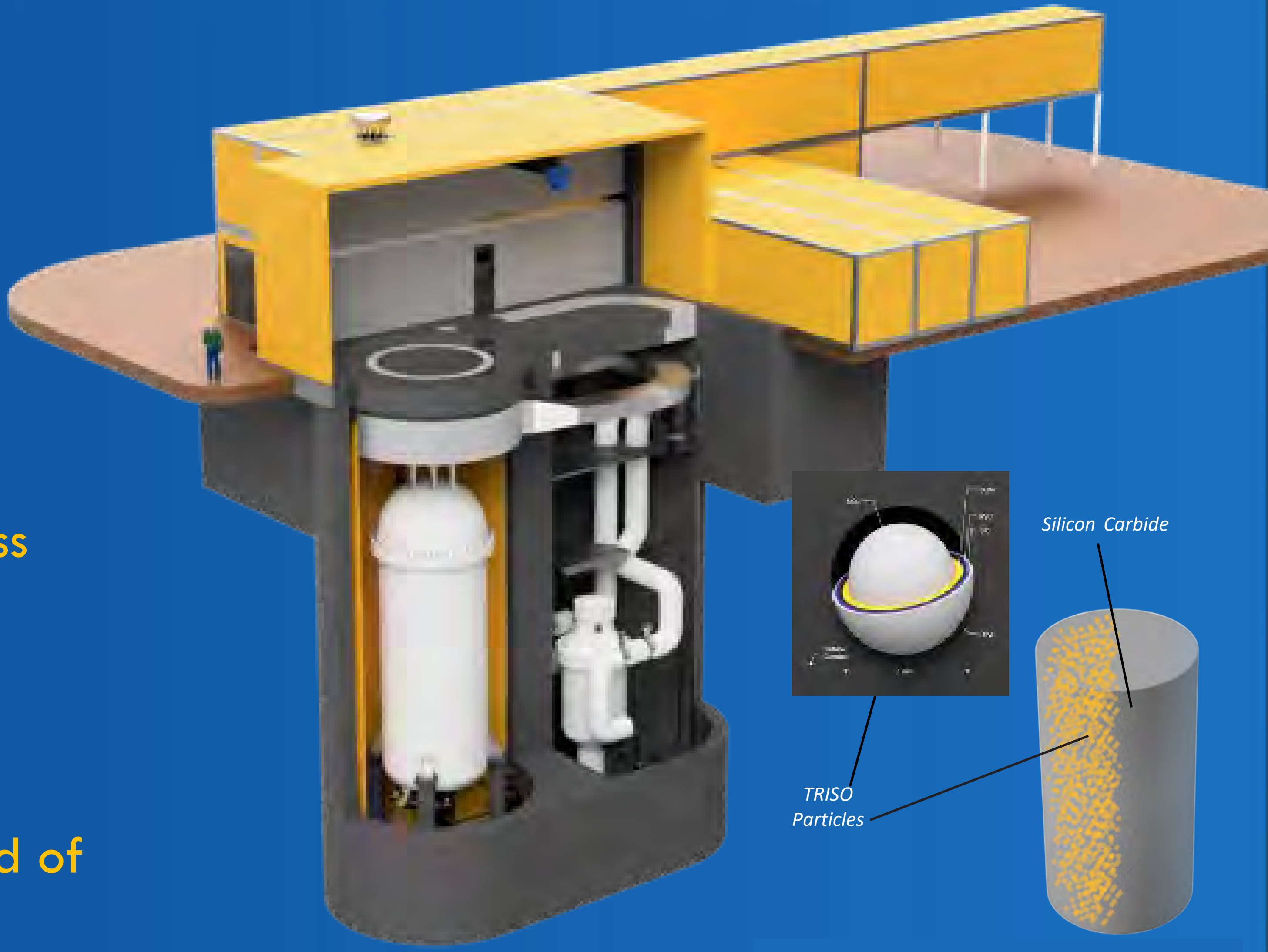
GLOBAL FIRST POWER

USNC ULTRA•SAFE•NUCLEAR

ONTARIO POWER GENERATION

The MMR reactor Unit

- Micro-modular containerized construction
- Mass manufactured
- Rapid deployment on site
- Designed for power and/or process heat
- Fully load-compliant
- Can produce hydrogen
- Simple, safe disposal of fuel at end of life
- **MELT-DOWN PROOF**



Fully Ceramic Micro-encapsulated (FCM^{TM}) fuel

USNC
ULTRA SAFE NUCLEAR

Safeguards: IAEA relevant documents

- safeguards by design (SBD)
  - provides State authorities, designers, equipment providers and prospective purchasers of nuclear facilities with guidance to facilitate the implementation of international safeguards.
  - international safeguards is fully integrated into the design process of a nuclear facility
  - engage the IAEA as soon as possible in the design process
  - enable optimum solutions balancing economic, operational, safety and security factors
  - facilitating design information verification; nuclear material accounting verification; the implementation of containment and surveillance measures.
- Examples of innovative solutions
  - Principles of bulk handling facilities (like enrichment facilities) used for molten salt reactors or pebble bed reactors
  - Use real time process information, joint use of equipment and instrumentation; or sharing of images from surveillance devices (all verified as authentic)
  - A design that supports safeguards use of containment, authentication of data, and continuity of knowledge – limited “opportunities” to divert material or break continuity of knowledge, i.e. no blind spots…
- different safeguards agreements (state dependent) so need to engage early with all the stake holders
- many advanced techniques being researched… such as antineutrino detectors

- IAEA NUCLEAR ENERGY SERIES No. NP-T-2.8 INTERNATIONAL SAFEGUARDS IN NUCLEAR FACILITY DESIGN AND CONSTRUCTION
- IAEA NUCLEAR ENERGY SERIES NO. NP-T-2.9 INTERNATIONAL SAFEGUARDS IN THE DESIGN OF NUCLEAR REACTORS
- INTERNATIONAL NUCLEAR VERIFICATION SERIES NO. 1 (REV. 2) SAFEGUARDS TECHNIQUES AND EQUIPMENT: 2011 EDITION

Micro reactors and FB – What is different ?

MICRO REACTOR ATTRIBUTES

- Economic: Cost competitive - ditto
- Standardized: - ditto
- Installed: Faster installation (months) – not so easy to removal after use. Mixture of long core life, regular re-fueling or even online.
- Unattended: - somewhat ditto (perhaps in future fully unattended or remotely).
- Reliable: - yes – maintenance shutdown planned. Longer lifetimes?

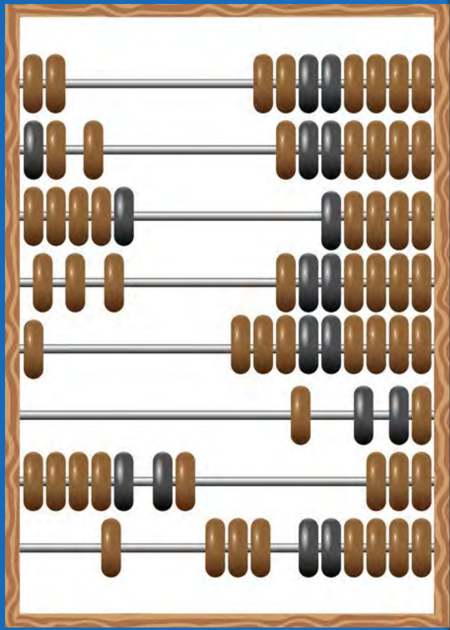
Closer to SMRs and traditional reactors in design… (in general)

FISSION BATTERY ATTRIBUTES

- Economic: Cost competitive with other distributed energy sources (electricity and heat) used for a particular application in a particular domain. This will enable distributed energy resources through flexible deployment across many applications and integration with other energy sources.
- Standardized: Developed in standardized sizes and power outputs with a manufacturing process that enables universal use and factory production. This will lower costs and produce more reliable systems that achieve faster qualification.
- Installed: Readily and easily installed for use and removal after use. After use they can be recycled by recharging with fresh fuel or responsibly dispositioned.
- Unattended: Operate securely and safely while unattended to provide demand-driven power.
- Reliable: Systems and technologies must have a high level of reliability to provide a long life and enable wide-scale deployment for applications. To support the concept of remote monitoring, they must be robust, resilient, fault tolerant, and durable, and provide advance notification when replacement is needed.

Aspects of safeguards …. Some thoughts…

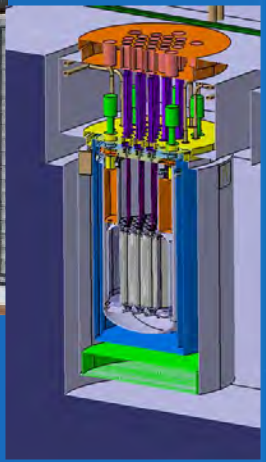
- The safeguards agreements signed with the IAEA may be slightly different depending on the member state
  - A Comprehensive Safeguards Arrangement (CSA) (INFCIRC/153 will be in place
  - Many member states has an Additional protocol (AP) signed with the IAEA.
  - For weapon states some facilities may be under safeguards on a voluntary basis. For non-nuclear weapon states all facilities is subject to safeguards
- Accurately determining the mass of uranium in the fuel assemblies / core
  - With coated particles fuel not so easy / no homogeneous material the weigh or count
  - important for mass balances
  - continuity of knowledge



- the physical design of the reactor and site layout will make provision for the incorporation of surveillance and monitoring systems to allow the IAEA to independently verify the integrity of the MMR™ fuel inventory during the operating life of the plant.
- The plant design will also incorporate the necessary security and robustness requirements to prevent sabotage and the unauthorized removal of nuclear material from the site.

Some thoughts… Significant quantity measures

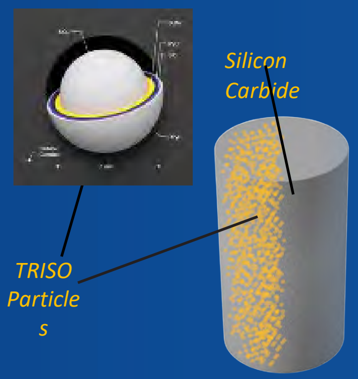
- HALEU to be used by many advanced SMRs / Fission Batteries
  - It is still LEU in IAEA definition of significant quantity measures (SC) …
  - but seems the increased enrichment compared to that currently being used commercially (<5%) does attract some additional attention that the designers / operators may have to include in their considerations.
- Qualitative values examples of significant material quantities
  - (SQ = 75 kg U^{235} as LEU; 8kg Pu; 8kg U^{233}; 25kg ^{235}U in HEU
  - typically higher level of enrichment used (5 - 19.75%)
- Micro SMR / Fission battery SQ's
  - MMR design: 15MWth : Lifetime core loading represents only 3 SQ and ~ 12m^3 volume
  - U-battery: 5 year core life: 10MWth: 0.6 SQ (but reload and spent fuel area on site)
  - Energy Well: 7 years core life: 20MWth: 1.5 SQ (fully loaded core transported/removed)



Advantages and Challenges to fulfil Safeguard requirements

Advantages:

- Less or no onsite handling of fuel
- Sealed unit -> supports safeguards use of containment, authentication of data, and continuity of knowledge
- Smaller quantities of material (only few SQs) – less attractive as a possible source of diversion / theft
- Fuel form often less attractive to processing / extraction of fissile material (TRISO FCM fuel as an example)
- Can be placed below grade – physically protected
- High burnup and in-situ utilization of plutonium



Challenges:

- Fully loaded core transported to site -> requires special measures on continuity of knowledge
- Increased enrichment (HALEU)
- Difficult access or no access to reactor during long cycles/ lifetime. So no traditional regular verification or replacements of seals.
- Remote sites (and a great many of them!)
- Increased deployment
- Very small transportable Fission Batteries may be target for theft / diversion
- Safeguard procedures not well developed for some advanced technologies (molten salt)
- On-load /on-line refueling (like pebble bed reactors or MSRs)
- Niche applications with HEU / fast spectrum / plutonium fueled

…. nothing that we cannot overcome

MMR™ …… ready to build – now

- Fastest possible deployment in current environment
- Advanced + simple enough to get licensed and built fast
- First Gen-IV reactor in North America

Thank YOU

- Use high temperature solid ceramic fuels (FCM) and moderators
  - Keep all radioactive material safely enclosed and contained - at all times
  - Produce the added benefit of highly efficient flexible power utilization
- Limit power density of reactor - reactor lacks internal energy to damage itself
  - All heat dissipates passively by conduction and radiation – no moving parts or fluids
- Physically self-stabilizing w/o controls (solid state); totally noninteracting materials and coolants (helium)
- Safe to environment, people, and investment

Pacific Northwest NATIONAL LABORATORY

Fission Battery Initiative Workshop Series

Pragmatic Security of Unconventional Power Sources

Shawn Datres
National Security Specialist

U.S. DEPARTMENT OF ENERGY BATTELLE
PNNL is operated by Battelle for the U.S. Department of Energy

PNNL-SA-160955

General Safeguard and Security Factors

Factors of the Security Posture:

- Target characteristics
  - o Attractiveness / consequence value
  - o Amount required
  - o Portability
- Threats (regional and local)
- Criticality (as in infrastructure)
- Operations

	Attractiveness Level
WEAPONS Assembled weapons and test devices	A
PURE PRODUCTS Pits, major components, button ingots, recastable metal, directly convertible materials	B
HIGH-GRADE MATERIALS Carbides, oxides, nitrates, solutions (≥25g/L) etc.; fuel elements and assemblies; alloys and mixtures; UF_4 or UF_6 (≥50% enriched)	C
LOW-GRADE MATERIALS Solutions (1 to 25 g/L), process residues requiring extensive reprocessing; Pu-238 (except waste); UF_4 or UF_6 (≥ 20% < 50% enriched)	D
ALL OTHER MATERIALS Highly irradiated[3] forms, solutions (<1g/L), compounds; uranium containing <20% U-235 or <10% U-233[2](any form, any quantity)	E

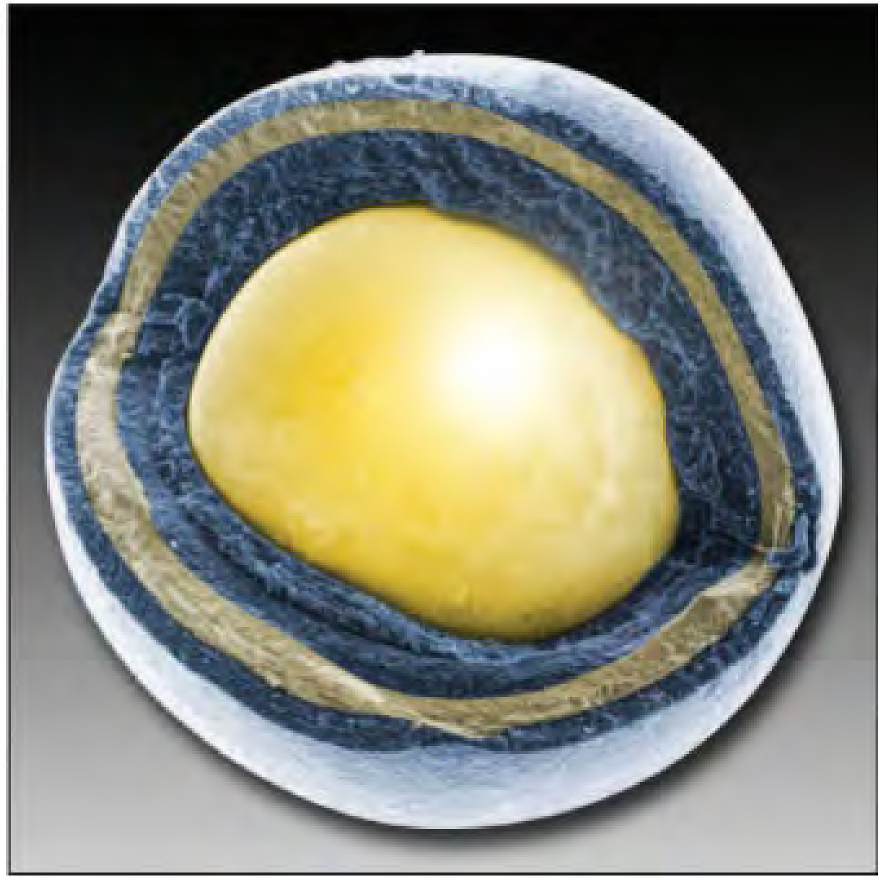
Fission Battery Characteristics

DOE Technology Roadmap (2002):

- Low proliferation risk by design
- Materials with reduced potential for weapons

TRISO Characteristics:

- Pros
  - o Very difficult to reprocess
  - o Low source term
  - o Attractiveness Level E
- Cons
  - o Difficulty of measuring
  - o Bulk vs. item accountancy



Risk-informed Approach

Realistic threats

- Thieves and insiders vs. state authorities and terrorists
- Crucial in determining the security design
- Traditional design basis threat may not be applicable

Criticality

- If the fuel does not present a proliferation risk – what is the battery?
- Is there a redundant power source?
- Risk assessment versus traditional vulnerability assessment?

Operations

- Plug and play?

Physical Protection Considerations

Graded approach

- Compliance and performance based
- Basic perimeter
- Two types of intrusion detection
- Assessment
- Delay
- Deterrence is your friend

Notifications to responders

- Redundancy is key

Pacific Northwest
NATIONAL LABORATORY

Thank you

PNNL-SA-160955

References

1. Aoki T., H. Sagara, and CY. Han. 2019. *Material Attractiveness Evaluation of Inert Matrix Fuel for Nuclear Security and Non-proliferation.* Annals of Nuclear Energy, Volume 126, Pages 427-433
2. Bari, Robert. 2012. *Proliferation Resistance and Physical Protection Evaluation Methodology: Objectives, Accomplishments, and Future Directions.* Nuclear Technology, 179:1, 35-44
3. Bathke, G., et al. 2012. *The Attractiveness of Materials in Advanced Nuclear Fuel Cycles for Various Proliferation and Theft Scenarios*. Nuclear Technology, 179:1, 5-30
4. Bunn, Matthew. 2014. *What Types of Nuclear Material Require What Levels of Security?* Nuclear Security Matters. https://www.belfercenter.org/publication/what-kind-material-needs-what-level-security
5. Lamothe, Joseph. 2021. *Prospectus: Mobile Nuclear Power Plant. A Key Attribute for Powering the 21st Century Joint Force.* Strategic Capabilities Office, Department of Defense
6. National Research Council. 2011. *Proliferation Risk in Nuclear Fuel Cycles: Workshop Summary.* Washington, DC: The National Academies Press. https://doi.org/10.17226/13259.
7. Vitali JA., et al. 2018. *Study on the use of Mobile Nuclear Power Plants for Ground Operations.* Deputy Chief of Staff G-4, United States Army
8. Zhuocheng L., et al. 2019. *Safety Analysis of a Small Modular Reactor Using Fully Ceramic Micro-encapsulated Fuel.* Progress in Nuclear Energy, Volume 113, 74-83

April 2, 2021

Steven Prescott
Scientific Software
Engineer

Target Set Analysis Tools & Needs for Fission Batteries

Idaho National Laboratory

Current Target Set Analysis

Determining Target Sets

- Based on Vital Equipment List & Probabilistic Risk Assessment (PRA)
- Smallest Cut Sets – Fewest locations that cause core damage without failure probability
- Expert Analysis – How adversary may fail items (Tasks) Regulatory Guidance 5.81

Protection Strategy Design & Evaluation

- NRC Requirements & Guidance (10 CFR 73, NUREG/CR-7145, etc)
- Force-on-Force Drills & Inspections
- Strategy/Simulation Software
  - Table Top – Expert review for attack scenarios and defense
  - Simulation – AI game engine

Current & Fission Battery Limitations

Determining Target Sets

- PRA has no/very limited time dependency – (targets hit = failure)
- Adjust model to prevent Cut Set truncation
- PRA focus on failures, what about additions?
- New cyber issues

Protection Strategy Design & Evaluation

- Need new regulatory guidance for simulation, autonomous and passive systems, risk measurement metrics
- No, limited, or difficulty in Including operator actions (Current Methods)
- Offsite response
- Need more capabilities in Force-on-Force simulation
- Current methods are costly, very conservative, and difficult to maintain

Overcoming The Limitations

Non PRA or Cut Set Options

PRA & Cut Sets don't include things people can do to a system, just what failure probabilities are modeled

- Adding heat
- Block natural circulation

AI Player

- Provide Rules & Options (Expert Judgement)
- Link to Digital Twin
- "Learn" to find attack options & targets

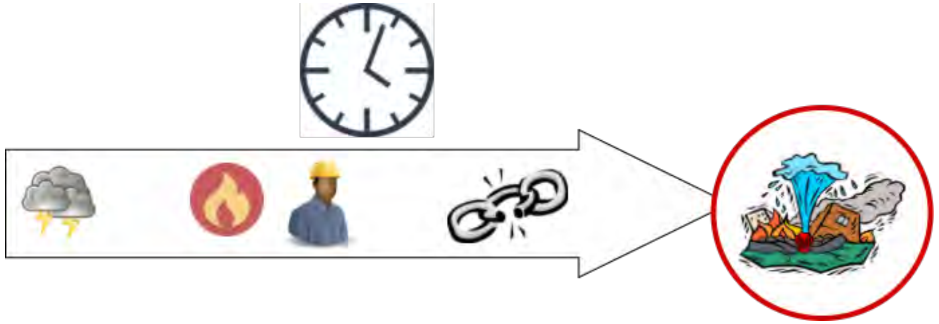
Success Criteria

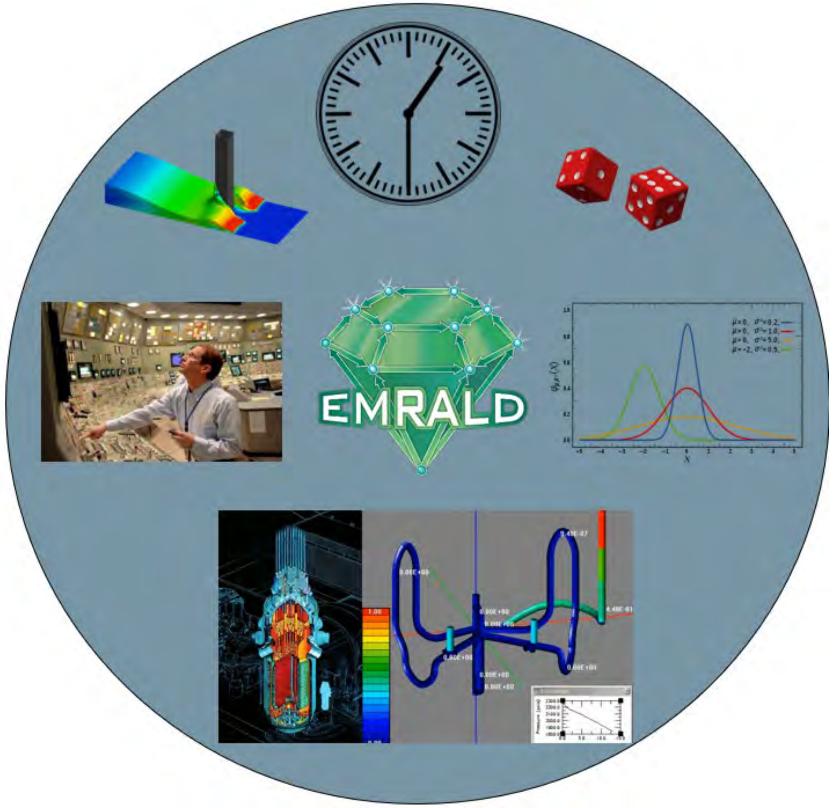
- Minimal components, actions, or criteria for "Success Set"
- System Theoretic Process Analysis (STPA)

Time Dependency - Dynamic PRA

Recent Dynamic PRA tools add the timing aspect (EMRALD, RAVEN, ADAPT)

- What and When things happen
- Couple with physics systems for consequence (i.e. Thermal Hydraulics)
- NRC useful for "Passive System Reliability" https://www.nrc.gov/docs/ML1906/ML19066A389.pdf
- Risk and reliability modeling for autonomous controls





https://www.youtube.com/watch?v=RmCz3vJklVw&list=PLX2nBoWRisnXWhC2LD9j4jV0iFzQbRcFX&index=1

NRC Security Requirements

- Biggest unknown
- Shifting to Risk Informed (need approved measurement methods - RIMES)
- Need approval of Simulations/AI for target sets & scenario evaluation

Protection Requirements

- Site Dependent? – Marine, remote community, paper plant, etc.
- Guards (none, so what to show instead?)
- Enclosure or Robustness?

Delay Requirements

- Minimal time for offsite response?
- Theft protection?

Dynamic PRA with Force-on-Force

EMRALD & (AVERT, Simajin, SCRIBE 3D)

- Add adversary and operator procedures during/after an attack
- Evaluate addition of flex equipment
- Offsite response
- Determine if strategy/technology changes with fewer guards maintains effectiveness (Defense in Depth)
- Human reliability/time adjustments

EMRALD

EMRALD.inl.gov

Simulate New Technology in Force-on-Force Simulation

What defense & deterrence measures will be used for fission batteries

- Remote weapons - probably not
- Robust Barriers/Design
- Non-lethal delay/deter (Sticky Foam?)
- Auto intrusion detection/assessment (Spot Dog?)
- ???

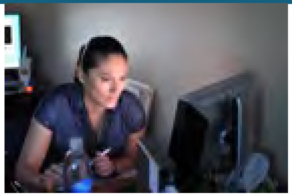
Simulation Capabilities

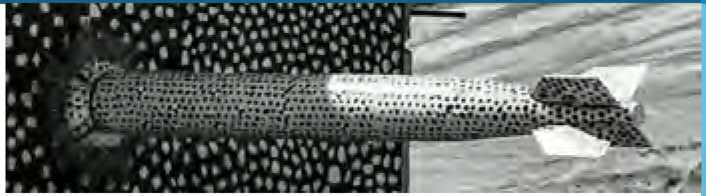
- How and what aspects of the measures do you model
- Time to add & validate
- Reliability Analysis

Idaho National Laboratory

Sandia National Laboratories

Physical Protection System Strategies for Fission Batteries





Alan Evans – Sandia National Laboratories

International Nuclear Security Engineering

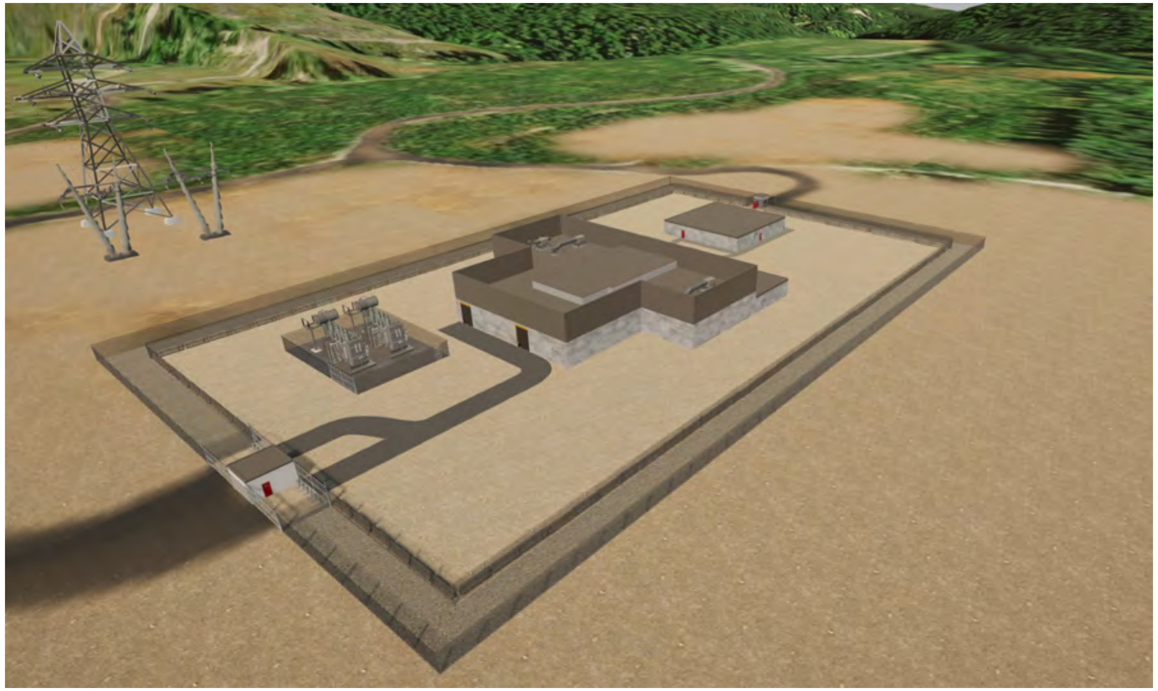
U.S. DEPARTMENT OF ENERGY NNSA National Nuclear Security Administration

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

SAND2021-3510 C

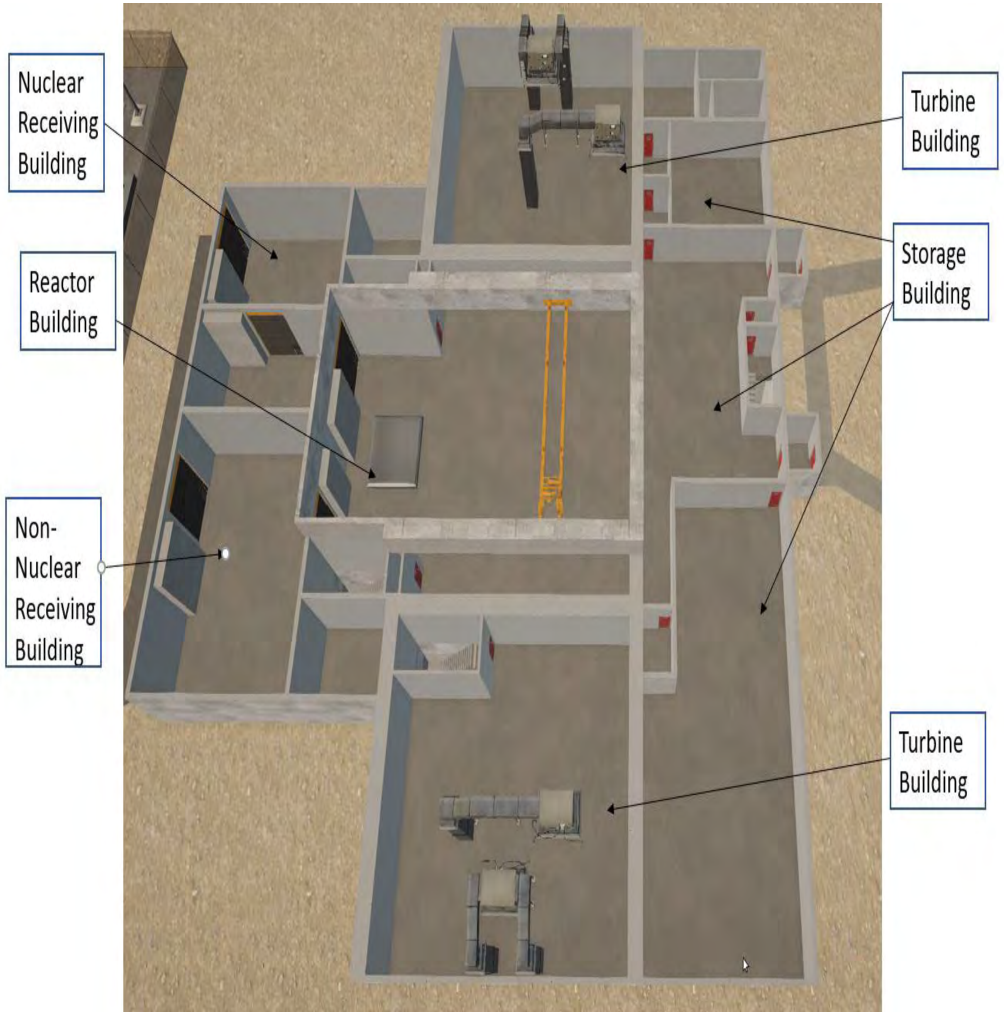
Outline

- Small Modular Reactor and Advanced Reactor (SMR/AR) Physical Protection Systems
- Implications for Fission Battery Systems
- Additional Considerations



SMR/AR Physical Protection System Considerations

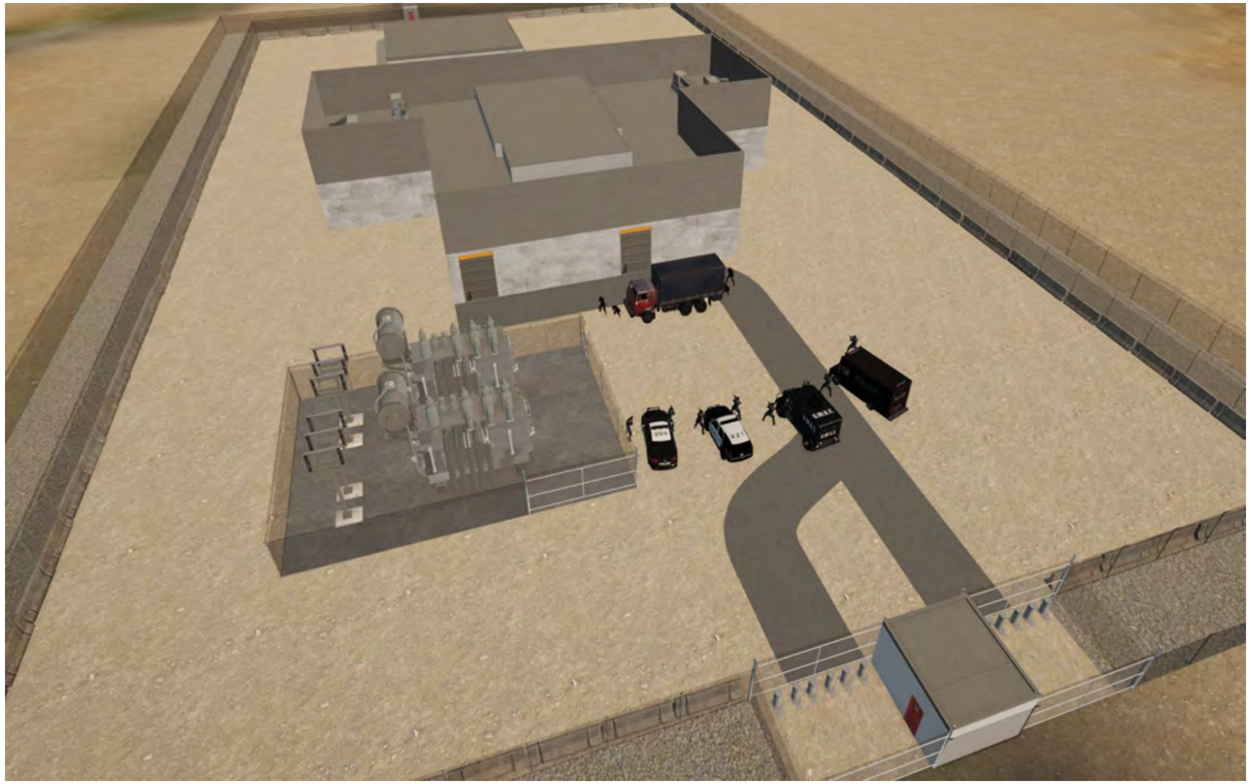
- Studies of Physical Protection System (PPS) Applications for SMR/AR
  - Integral Pressurized Water Reactors
  - Pebble-Bed Reactors
  - Microreactors
- Understanding of Physical Protection System Postures
  - Offsite Response Force
  - Increased Detection
  - Increased Delay
  - Use of Advanced Technologies



Work funded under DOE – Advanced Reactor Safeguards & Security Program

Implications for Fission Battery Systems

- How do we apply lessons learned from fixed-site security to transport security of fission battery systems?
  - Implement inherent PPS capabilities to fission battery system
  - Access delay
  - Detection
- Transitioning fission battery from transportation to fixed-site operation?
  - Underground operation
  - Several layers of detection and delay
  - Coordination with local law enforcement to provide proper response



Work funded under DOE – Advanced Reactor Safeguards & Security Program

Additional Considerations

- Extreme Weather Event Implications
  - Are offsite responders effected by weather events?
  - Can adversaries leverage extreme weather events?
  - Deployable compensatory measures to provide adequate security
- Compensatory Measures
  - Material in transport
  - System in Transport

Questions

References

SAND2021-0768

Section Break Slide

April 02, 2021

Pralhad Burli

Advanced Reactor and Small Module Reactor Security Economic Analysis

INL-NUC Fission Battery Safeguards & Security Workshop

Idaho National Laboratory

Objectives

- To develop a capability and tool that vendors and utilities can use to perform economic analysis for reducing O&M costs related to nuclear security
- The tool will be sufficiently generic to be used on multiple AR/SMR designs and will be flexible enough to consider cost differences in different countries

Physical Security Costs

- Capital Costs
  - Physical barriers (fences, gates)
  - Technological Installations (CCTV cameras, sensors, alarms)
  - Vehicles
  - Weapons and ammunition
  - Other equipment
- Recurring Costs
  - Wages
  - Technical Training
  - Operation and Maintenance
  - Information security/ Cyber Security
  - Regulatory/Compliance Costs/Annual Reviews
  - Liaison with law enforcement/ intelligence agencies

Economic Analysis

Model Inputs

Cost/Investments	
Capital Costs	1550000
Equipment	1500000
Installation	50000
Project Life	15
Salvage Value	0

Operational Costs	
Personnel	$ 311,230.07
# of personnel	1
Equipment O&M	20000
Software and Servicing	20000
Ammunition	

Benefits/Cost Savings	
Avoided Personnel Costs	$ 622,460
# of personnel reduced	2
Other Avoided costs	$ -
O&M	
Ammunition	
Avoided Casualties	

Discount Rate	0.08
Inflation	0.025
Tax rate	0.35
Depreciation	0.15

Years

Cashflow Analysis	0	1	2	3	4	5	6	7
Revenues/Benefits		$ 622,460	$ 638,022	$ 653,972	$ 670,321	$ 687,080	$ 704,257	$ 721,863
Costs	$ (1,550,000)	$ 331,230	$ 339,511	$ 347,999	$ 356,699	$ 365,616	$ 374,756	$ 384,125
EBITDA		$ 291,230	$ 298,511	$ 305,974	$ 313,623	$ 321,464	$ 329,500	$ 337,738
Depreciation		$ 232,500	$ 197,625	$ 167,981	$ 142,784	$ 121,366	$ 103,161	$ 87,687
EBIT		$ 58,730	$ 100,886	$ 137,992	$ 170,839	$ 200,097	$ 226,339	$ 250,050
Taxes		$ 20,556	$ 35,310	$ 48,297	$ 59,794	$ 70,034	$ 79,219	$ 87,518
EBIT(1-Taxes)		$ 38,175	$ 65,576	$ 89,695	$ 111,045	$ 130,063	$ 147,120	$ 162,533
Add Depreciation		$ 232,500	$ 197,625	$ 167,981	$ 142,784	$ 121,366	$ 103,161	$ 87,687
Net Cash Flow	$ (1,550,000)	$ 270,675	$ 263,201	$ 257,676	$ 253,829	$ 251,430	$ 250,282	$ 250,220
Discount Factor	1	0.925925926	0.85733882	0.793832241	0.735029853	0.680583197	0.630169627	0.583490395
Discounted CF	$ (1,550,000)	$ 250,625	$ 225,652	$ 204,552	$ 186,572	$ 171,119	$ 157,720	$ 146,001

Cashflow Analysis	8	9	10	11	12	13	14	15
Revenues/Benefits	$ 739,909	$ 758,407	$ 777,367	$ 796,802	$ 816,722	$ 837,140	$ 858,068	$ 879,520
Costs	$ 393,728	$ 403,572	$ 413,661	$ 424,002	$ 434,603	$ 445,468	$ 456,604	$ 468,019
EBITDA	$ 346,181	$ 354,836	$ 363,706	$ 372,799	$ 382,119	$ 391,672	$ 401,464	$ 411,500
Depreciation	$ 74,534	$ 63,354	$ 53,851	$ 45,773	$ 38,907	$ 33,071	$ 28,111	$ 23,894
EBIT	$ 271,647	$ 291,482	$ 309,856	$ 327,026	$ 343,212	$ 358,601	$ 373,353	$ 387,607
Taxes	$ 95,076	$ 102,019	$ 108,449	$ 114,459	$ 120,124	$ 125,510	$ 130,674	$ 135,662
EBIT(1-Taxes)	$ 176,570	$ 189,463	$ 201,406	$ 212,567	$ 223,088	$ 233,091	$ 242,680	$ 251,944
Add Depreciation	$ 74,534	$ 63,354	$ 53,851	$ 45,773	$ 38,907	$ 33,071	$ 28,111	$ 23,894
Net Cash Flow	$ 251,105	$ 252,817	$ 255,257	$ 258,340	$ 261,995	$ 266,162	$ 270,790	$ 275,838
Discount Factor	0.540268885	0.500248967	0.463193488	0.428882859	0.397113759	0.367697925	0.340461041	0.315241705
Discounted CF	$ 135,664	$ 126,471	$ 118,233	$ 110,798	$ 104,042	$ 97,867	$ 92,194	$ 86,956

NPV	664465
IRR	15%

Depreciation Calculation

	0	1	2	3	4	5	6	7
Beginning Value		$ 1,550,000	$ 1,317,500	$ 1,119,875	$ 951,894	$ 809,110	$ 687,743	$ 584,582
Depreciation		$ 232,500	$ 197,625	$ 167,981	$ 142,784	$ 121,366	$ 103,161	$ 87,687
Ending Value	$ 1,550,000	$ 1,317,500	$ 1,119,875	$ 951,894	$ 809,110	$ 687,743	$ 584,582	$ 496,894

	8	9	10	11	12	13	14	15
Beginning Value	$ 496,894	$ 422,360	$ 359,006	$ 305,155	$ 259,382	$ 220,475	$ 187,404	$ 159,293
Depreciation	$ 74,534	$ 63,354	$ 53,851	$ 45,773	$ 38,907	$ 33,071	$ 28,111	$ 23,894
Ending Value	$ 422,360	$ 359,006	$ 305,155	$ 259,382	$ 220,475	$ 187,404	$ 159,293	$ 135,399

EBITDA: Earnings Before Interest, Taxes, Depreciation, and Amortization
EBIT: Earnings Before Interest and Taxes

Output | Capital and O&M Costs | Personnel Costs | +

Economic Analysis

Posture 1
Posture 2
Posture 3
:
:
Posture N

Model Inputs

Cost/Investments	
Capital Costs	1550000
Equipment	1500000
Installation	50000
Project Life	15
Salvage Value	0

Operational Costs	
Personnel	$ 311,230.07
# of personnel	1
Equipment O&M	20000
Software and Servicing	20000
Ammunition	

Benefits/Cost Savings	
Avoided Personnel Costs	$ 622,460
# of personnel reduced	2
Other Avoided costs	$ -
O&M	
Ammunition	
Avoided Casualties	

Discount Rate	0.08
Inflation	0.025
Tax rate	0.35
Depreciation	0.15

Years

Cashflow Analysis	0	1	2	3	4	5	6	7
Revenues/Benefits		$ 622,460	$ 638,022	$ 653,972	$ 670,321	$ 687,080	$ 704,257	$ 721,863
Co[illegible]ts	$ (1,550,000)	$ 331,230	$ 339,511	$ 347,999	$ 356,699	$ 365,616	$ 374,756	$ 384,125
[illegible]		$ 291,230	$ 298,511	$ 305,974	$ 313,623	$ 321,464	$ 329,500	$ 337,738
[illegible]		$ 232,500	$ 197,625	$ 167,981	$ 142,784	$ 121,366	$ 103,161	$ 87,687
[illegible]		$ 58,730	$ 100,886	$ 137,992	$ 170,839	$ 200,097	$ 226,339	$ 250,050
Ta[illegible]		$ 20,556	$ 35,310	$ 48,297	$ 59,794	$ 70,034	$ 79,219	$ 87,518
EBIT(1-Taxes)		$ 38,175	$ 65,576	$ 89,695	$ 111,045	$ 130,063	$ 147,120	$ 162,533
Add Depreciation		$ 232,500	$ 197,625	$ 167,981	$ 142,784	$ 121,366	$ 103,161	$ 87,687
Net Cash Flow	$ (1,550,000)	$ 270,675	$ 263,201	$ 257,676	$ 253,829	$ 251,430	$ 250,282	$ 250,220
Discount Factor	1	0.925925926	0.85733882	0.793832241	0.735029853	0.680583197	0.630169627	0.583490395
Discounted CF	$ (1,550,000)	$ 250,625	$ 225,652	$ 204,552	$ 186,572	$ 171,119	$ 157,720	$ 146,001

Cashflow Analysis	8	9	10	11	12	13	14	15
Revenues/Benefits	$ 739,909	$ 758,407	$ 777,367	$ 796,802	$ 816,722	$ 837,140	$ 858,068	$ 879,520
Co[illegible]ts	$ 393,728	$ 403,572	$ 413,661	$ 424,002	$ 434,603	$ 445,468	$ 456,604	$ 468,019
[illegible]	$ 346,181	$ 354,836	$ 363,706	$ 372,799	$ 382,119	$ 391,672	$ 401,464	$ [illegible]
[illegible]	$ 74,534	$ 63,354	$ 53,851	$ 45,773	$ 38,907	$ 33,071	$ 28,111	$ [illegible]
[illegible]	$ 271,647	$ 291,482	$ 309,856	$ 327,026	$ 343,212	$ 358,601	$ 373,353	$ [illegible]
Ta[illegible]	$ 95,076	$ 102,019	$ 108,449	$ 114,459	$ 120,124	$ 125,510	$ 130,674	$ 135,662
EBIT(1-Taxes)	$ 176,570	$ 189,463	$ 201,406	$ 212,567	$ 223,088	$ 233,091	$ 242,680	$ 251,944
Add Depreciation	$ 74,534	$ 63,354	$ 53,851	$ 45,773	$ 38,907	$ 33,071	$ 28,111	$ 23,894
Net Cash Flow	$ 251,105	$ 252,817	$ 255,257	$ 258,340	$ 261,995	$ 266,162	$ 270,790	$ 275,838
Discount Factor	0.540268885	0.500248967	0.463193488	0.428882859	0.397113759	0.367697925	0.340461041	0.315241705
Discounted CF	$ 135,664	$ 126,471	$ 118,233	$ 110,798	$ 104,042	$ 97,867	$ 92,194	$ 86,956

NPV	664465
IRR	15%

Depreciation Calculation

	0	1	2	3	4	5	6	7
Beginning Value		$ 1,550,000	$ 1,317,500	$ 1,119,875	$ 951,894	$ 809,110	$ 687,743	$ 584,582
Depreciation		$ 232,500	$ 197,625	$ 167,981	$ 142,784	$ 121,366	$ 103,161	$ 87,687
Ending Value	$ 1,550,000	$ 1,317,500	$ 1,119,875	$ 951,894	$ 809,110	$ 687,743	$ 584,582	$ 496,894

	8	9	10	11	12	13	14	15
Beginning Value	$ 496,894	$ 422,360	$ 359,006	$ 305,155	$ 259,382	$ 220,475	$ 187,404	$ 159,293
Depreciation	$ 74,534	$ 63,354	$ 53,851	$ 45,773	$ 38,907	$ 33,071	$ 28,111	$ 23,894
Ending Value	$ 422,360	$ 359,006	$ 305,155	$ 259,382	$ 220,475	$ 187,404	$ 159,293	$ 135,399

EBITDA: Earnings Before Interest, Taxes, Depreciation, and Amortization
EBIT: Earnings Before Interest and Taxes

Output | Capital and O&M Costs | Personnel Costs | +

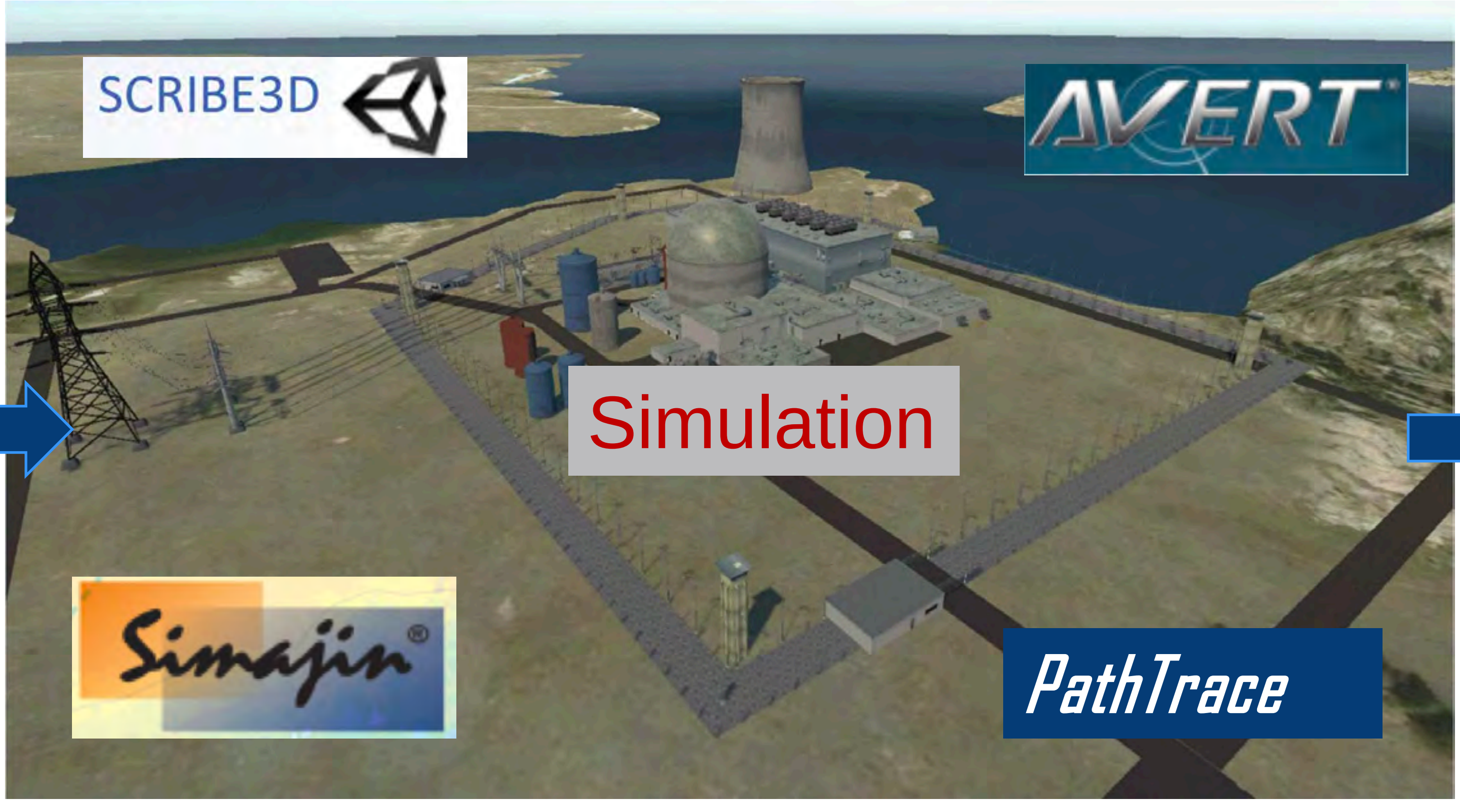
NPV: Net Present Value; IRR: Internal Rate of Return

NPV 1
NPV 2
NPV 3
:
NPV N

IRR 1
IRR 2
IRR 3
:
IRR N

Posture Effectiveness

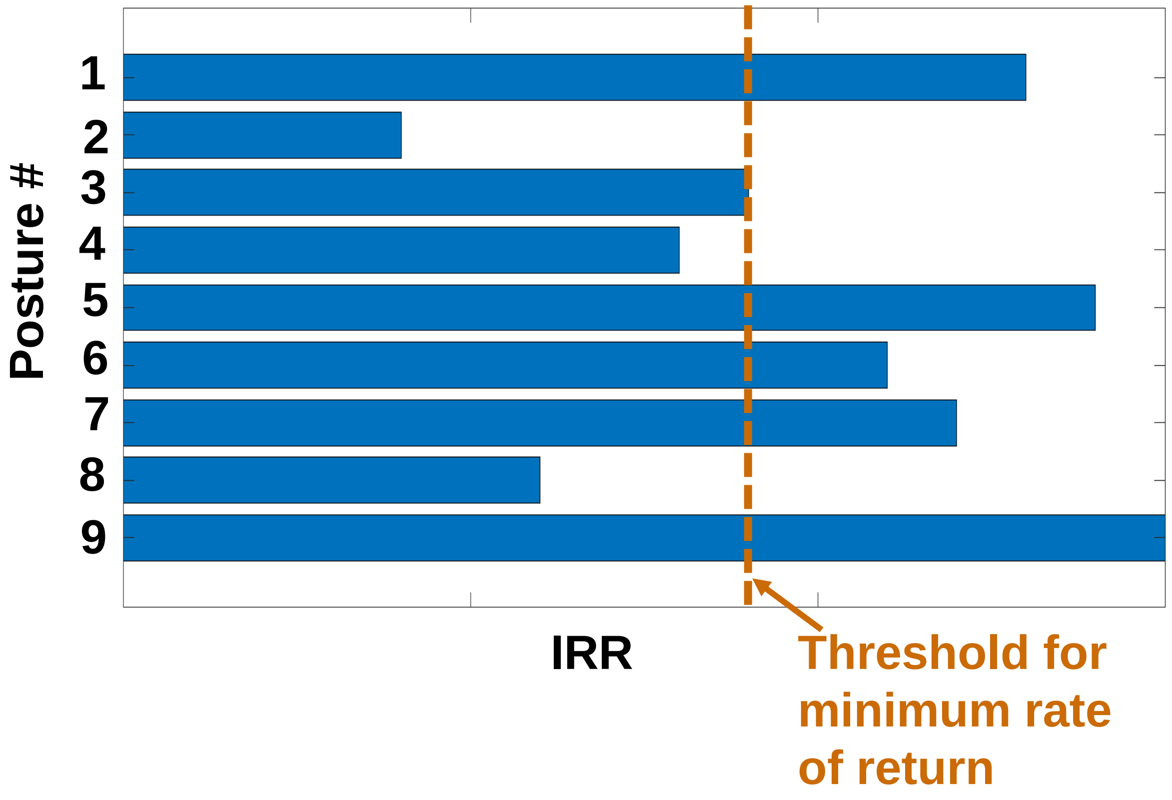
Posture 1
Posture 2
Posture 3
:
:
Posture N

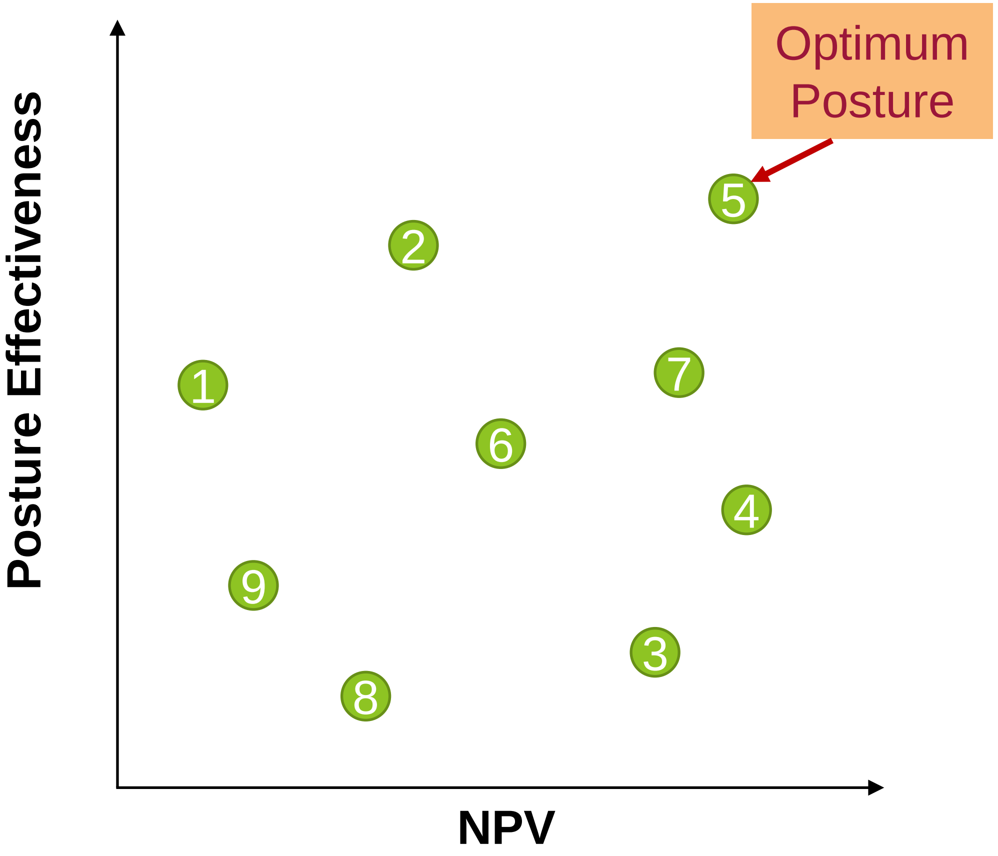


Posture Effectiveness

- Probability of effectiveness
- Timelines
- Probability of interruption
- Consequence-based effectiveness

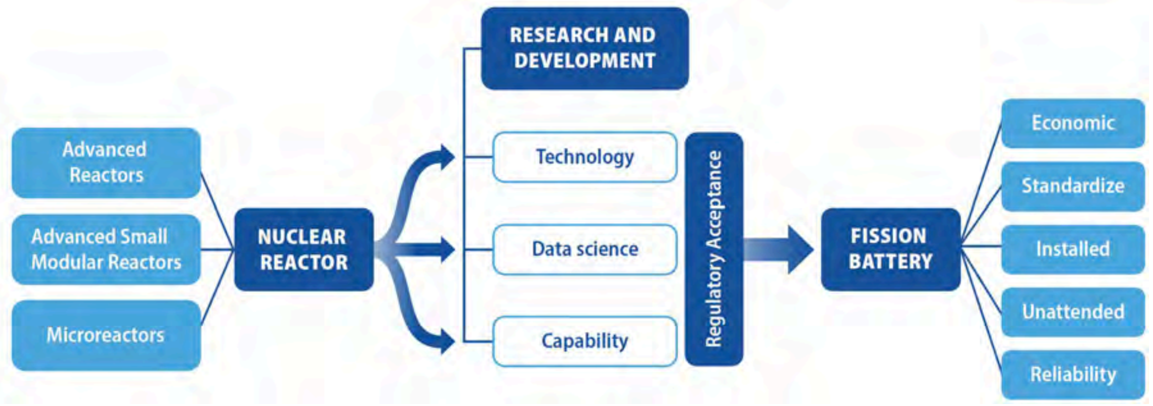
Identify Optimum Postures





Fission Battery Security

- Fission Battery Initiative envisions zero armed guards for fission battery installations
- Long term economic feasibility of security must be achieved and demonstrated for success of fission battery
- Remote and unattended nature of fission battery poses unique challenge for physical security assessment
- Prescriptive nature of current regulatory requirements would need to be addressed



Fission battery initiative research and development approach to deliver technologies that endow nuclear reactors with battery attributes

Team

- Vaibhav Yadav
- Pralhad Burli
- Andrew Foss
- Gustavo Reyes

- Bobby Middleton
- Alan Evans

- Thomas Harrison

Idaho National Laboratory

April 02, 2021

Carol Smidts, Ph.D.
Professor, The Ohio State University

Fission Battery Initiative

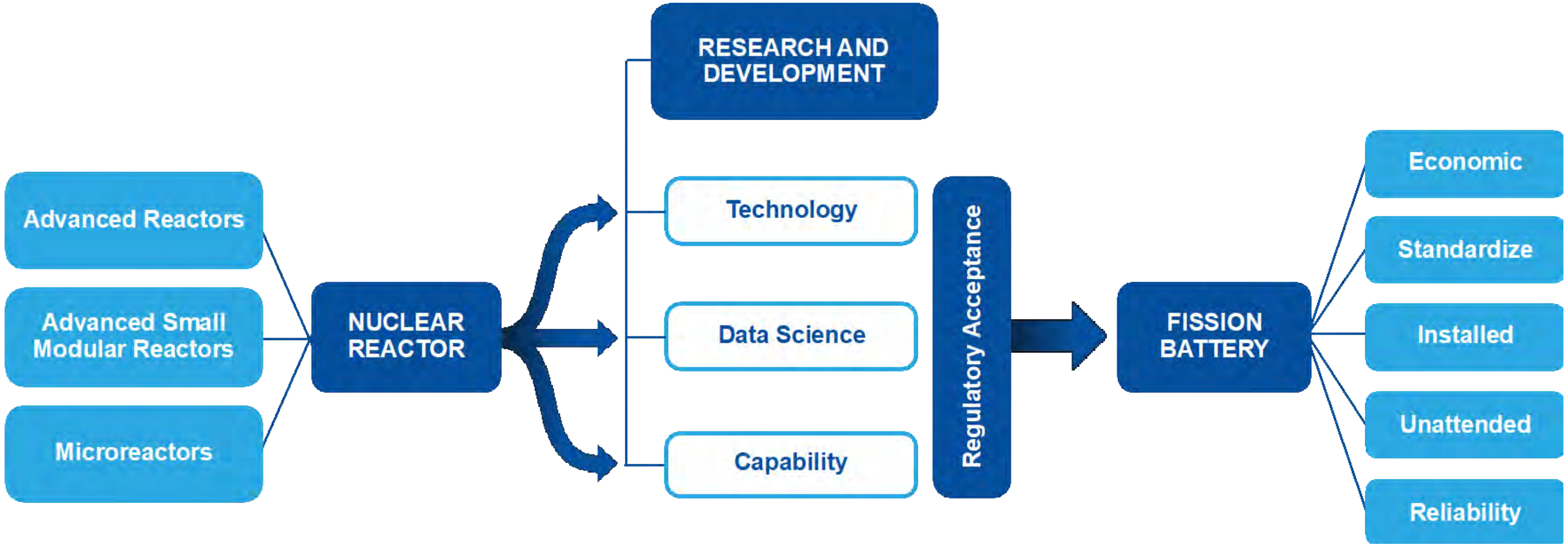
Nuclear Science and Technology

Idaho National Laboratory

Fission Battery Initiative

Vision: Developing technologies that enable nuclear reactor systems to function as batteries.

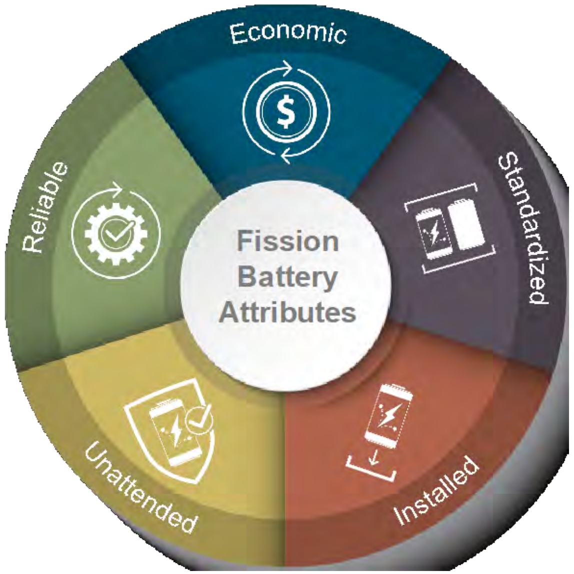
Outcome: Deliver on research and development needed to provide technologies that achieve key fission battery attributes and expand applications of nuclear reactors systems beyond concepts that are currently under development.



Research and development to enable nuclear reactor technologies to achieve fission battery attributes

Fission Battery Attributes

- **Economic** – Cost competitive with other distributed energy sources (electricity and heat) used for a particular application in a particular domain. This will enable flexible deployment across many applications, integration with other energy sources, and use as distributed energy resources.
- **Standardized** – Developed in standardized sizes, power outputs, and manufacturing processes that enable universal use and factory production, thereby enabling low-cost and reliable systems with faster qualification and lower uncertainty for deployment.
- **Installed** – Readily and easily installed for application-specific use and removal after use. After use, fission batteries can be recycled by recharging with fresh fuel or responsibly dispositioned.
- **Unattended** – Operated securely and safely in an unattended manner to provide demand-driven power.
- **Reliable** – Equipped with systems and technologies that have a high level of reliability to support the mission life and enable deployment for all required applications. They must be robust, resilient, fault tolerant, and durable to achieve fail-safe operation.



Fission Battery Workshop Series

- **Jointly INL and National University Consortium are organizing workshops across five areas:**
  - Market and Economic Requirements for Fission Batteries and Other Nuclear Systems
  - Technology Innovation for Fission Batteries – Next workshop is February 24, 2021
  - Transportation and Siting for Fission Batteries – March 15, 2021
  - Domestic & International Safeguards & Security for Fission Batteries – April 02, 2021
  - Safety and Licensing of Fission Batteries – April 16, 2021

- **Expected outcomes:**
  - Each workshop outcomes are expected to outline the goals of each fission battery attribute

Today's agenda

Session 1: Nuclear Safeguards
(Session Chair: Gustavo Reyes, INL)

02 April 2021
All U.S. Eastern Time

10:00	Opening Statement and Introduction	Gustavo Reyes (INL)
10:10	International Computer Security Strategy – IAEA Pub	Trent Nelson (IAEA)
10:20	Safeguards Ideas on Microreactors/FB	Frederik Reitsma (USNC)
10:30	Pragmatic Security of Unconventional Power Sources	Shawn Datres (PNNL)
11:00	Panel Discussion 1 *Moderator*: Gustavo Reyes, INL *Panelists*: Trent Nelson, IAEA Frederik Reitsma, USNC Shawn Datres, PNNL	
11:30	Break	15 Minutes
11:45	Target Set Analysis Tools & Needs for FB	Steven Prescott (INL)
12:00	Physical Protection Systems Strategies for FB	Alan Evans (SNL)
12:15	Security Economic Analysis on FB	Pralhad Burli (INL)
12:45	Panel Discussion 2 *Moderator*: Raymond Cao, OSU *Panelists*: Steven Prescott, INL Alan Evans, SNL Pralhad Burli, INL	
13:15	Break	45 minutes

Session 2: Nuclear Security
(Session Chair: Carol Smidts, OSU)

14:00	Opening Statement and Introduction	Carol Smidts (OSU)
14:10	FB's Place in the INS Civilian Nuclear Security Project	Doug Osborn (SNL)
14:20	Additional Physical Security Considerations for FB	Adam Williams (SNL)
14:30	Cyber-Informed Engineering – S&S of FB	Robert Anderson (INL)
14:40	Panel Discussion 3 *Moderator*: Cassiano Endres de Oliveira, UNM *Panelists*: Doug Osborn, SNL Adam Williams, SNL Robert Anderson, INL	
15:10	Break	15 Minutes
15:25	Zero Trust Security for Fission Batteries	Indrajit Ray (CSU)
15:35	Cross-Layer Cyber-Physical Security of FB Control Systems	Quanyan Zhu (NYU)
15:45	Experimental Testbeds & Cyber Hardening of FB	Robert England (INL)
15:55	Panel Discussion 4 *Moderator*: Carol Smidts, OSU *Panelists*: Indrajit Ray, CSU Quanyan Zhu, NYU Robert England, INL	
16:25	Closing Remarks	Gustavo Reyes (INL)
16:35	End	

Idaho National Laboratory

National Nuclear Security Administration

Fission Battery's Place in the INS Civilian Nuclear Security Project

Presenter: Douglas M. Osborn, PhD

INS
International Nuclear Security
Reducing Risk of Nuclear Terrorism

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2021-2896 PE

Nuclear Security
in Civil Nuclear Context

National Nuclear Security Administration

INS Civil Nuclear Security Project

Building relationships with U.S. nuclear energy industry vendors & embarking countries on nuclear security topics to support:

- Restoring U.S. leadership in nuclear
- Advancing peaceful uses
- Upholding the global nuclear security regime

IAEA Milestones Approach to Nuclear Infrastructure for Nuclear Power
(IAEA Nuclear Energy Series NG-G-3.1 Rev.1)

Tools Under Development

- Economic costs and benefits of security
- Identifying sabotage target sets for advanced reactors
- Physical Protection Systems Design Training- Design Evaluation Process Outline (DEPO) Methodology Videos

Standard Nuclear Security Tools

Tool Examples:

- SCRIBE 3D (tabletop exercises)
- PATHTRACE (pathway analysis)
- JCATS (combat simulation instrument)

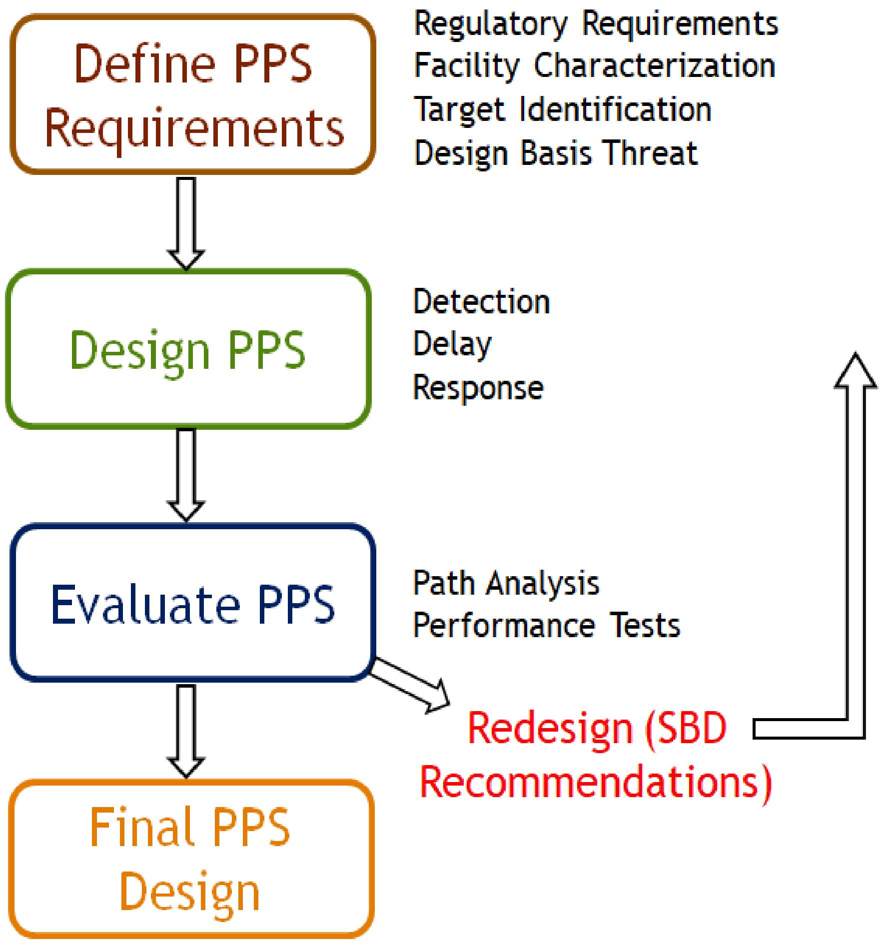
INS
International Nuclear Security
Reducing Risk of Nuclear Terrorism

Design Evaluation Process Outline (DEPO) Methodology

Define physical protection system (PPS) requirements - Study the existing facility and its plans to learn all of the operations, conditions, and important physical features that affect the PPS. Then conduct a detailed study of the range of adversaries that the physical protection system must successfully counter. Finally, identify the most important areas or materials that must be protected from the adversary.

Design a PPS - Either identify the existing physical protection elements for potential upgrading or design a new protection system using elements of detection, delay, and response that are effective against the capabilities of the potential adversary.

Evaluate the PPS design - Given the information about the facility, threat, targets, and physical protection system, use accepted analysis techniques to obtain a measure of the protection system's effectiveness. Redesign and reanalysis may be required if the measure of effectiveness is not satisfactory.



Online Security Training – Design Evolution Process Outline

National Nuclear Security Administration

The Design Evaluation Process Outline (DEPO) is a systems engineering method that has been applied to nuclear security since the 1970's. DEPO is a performance-based methodology to design and evaluate physical protection systems (PPS) against the threat of unauthorized removal of nuclear materials or radiological sabotage.

- Traditional DEPO training is a 5-day in-person training course with field exercises
- The classroom lecture materials were converted into a 16 module (~14 hour) online training course

https://nstc.sandia.gov/training/smr-depo-course

MODULE	TITLE
1	Intro to the DEPO Process
2	Overview of Physical Protection Principles
3	Regulatory Requirements and Risk Management
4	Target and Vital Area Identification
5	Threat Definition
6	Facility Characterization
7	Intro to Design of PPS
8	Intrusion Detection Systems
9	Alarm Assessment Systems
10	Delay System Design
11	Access Control
12	Prohibited Items
13	Alarm Communications & Display and Response
14	Computer Security
15	Performance Testing
16	Intro to Evaluation of PPS

Collaborations with U.S. AR community – Interests & Feedback

National Nuclear Security Administration

Pilot studies

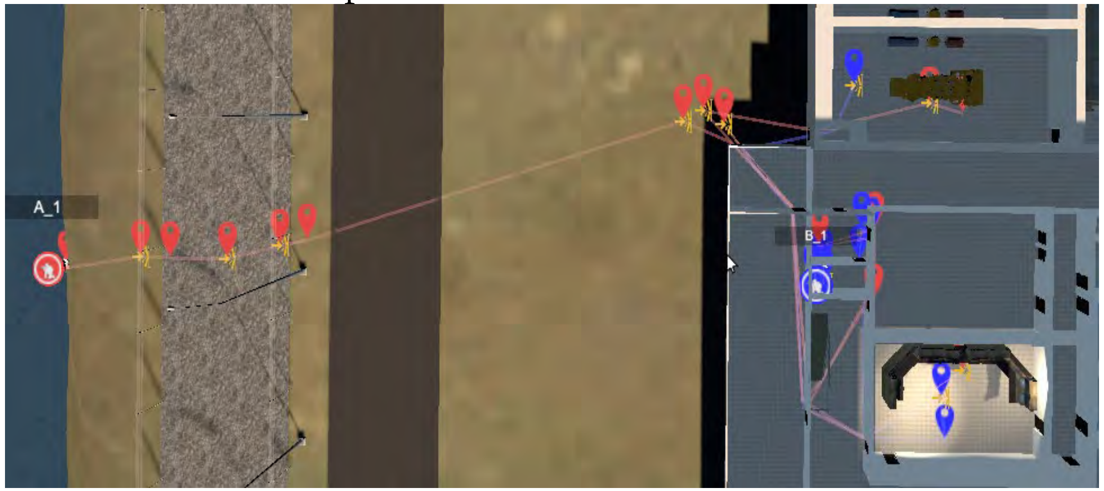
- Novel approach to AR Target Set Identification
- Security Economic Analysis Tool
- Other topics of interest to AR community?

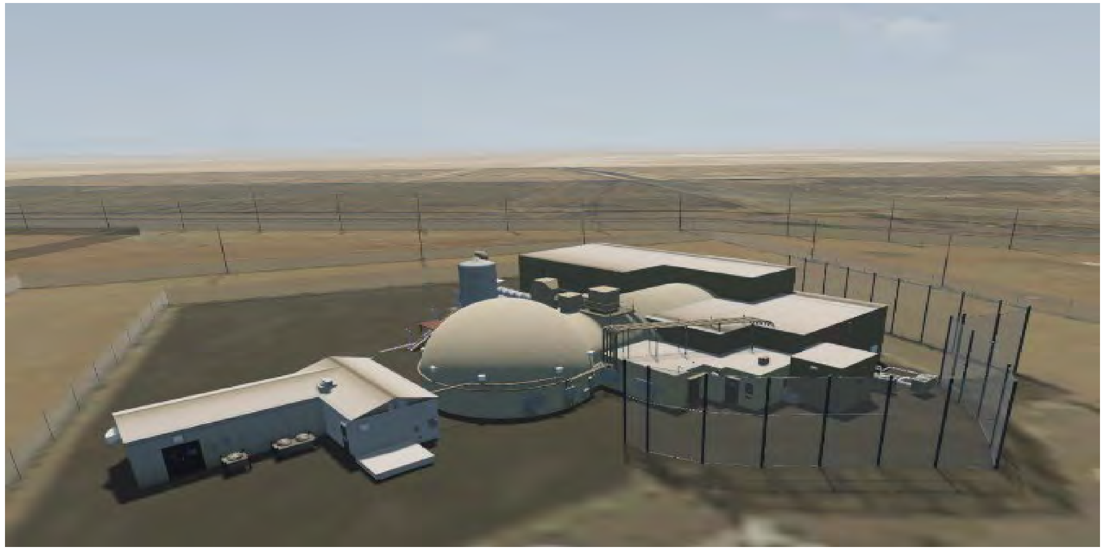
Engagements with U.S. AR vendors on Lab Technical consults/SeBD

Provide testing capabilities for next generation security technologies and methods

- SMR/AR Testing and Training (SMARTT) Platform

Example of Scribe3D attack scenario





Visualization of SMARTT Platform in Scribe3D

Questions

April 2, 2021

Mr. Bob Anderson
Cybersecurity Specialist

Cyber-Informed Engineering

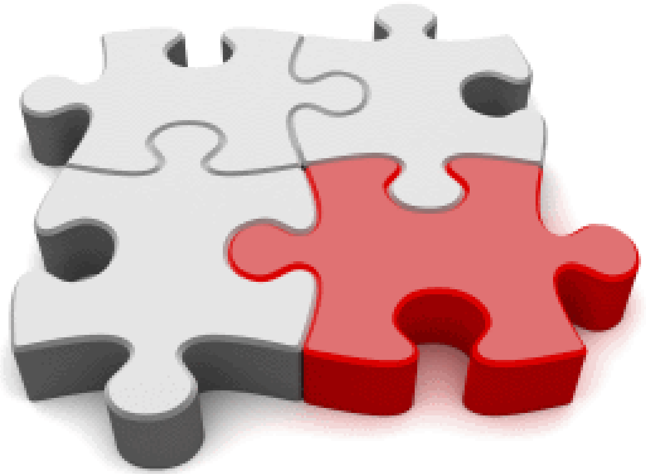
Safeguards and Security of Fission Batteries

Idaho National Laboratory

Cybersecurity Objectives & Risk Management

Cyber-Informed Engineering (CIE)

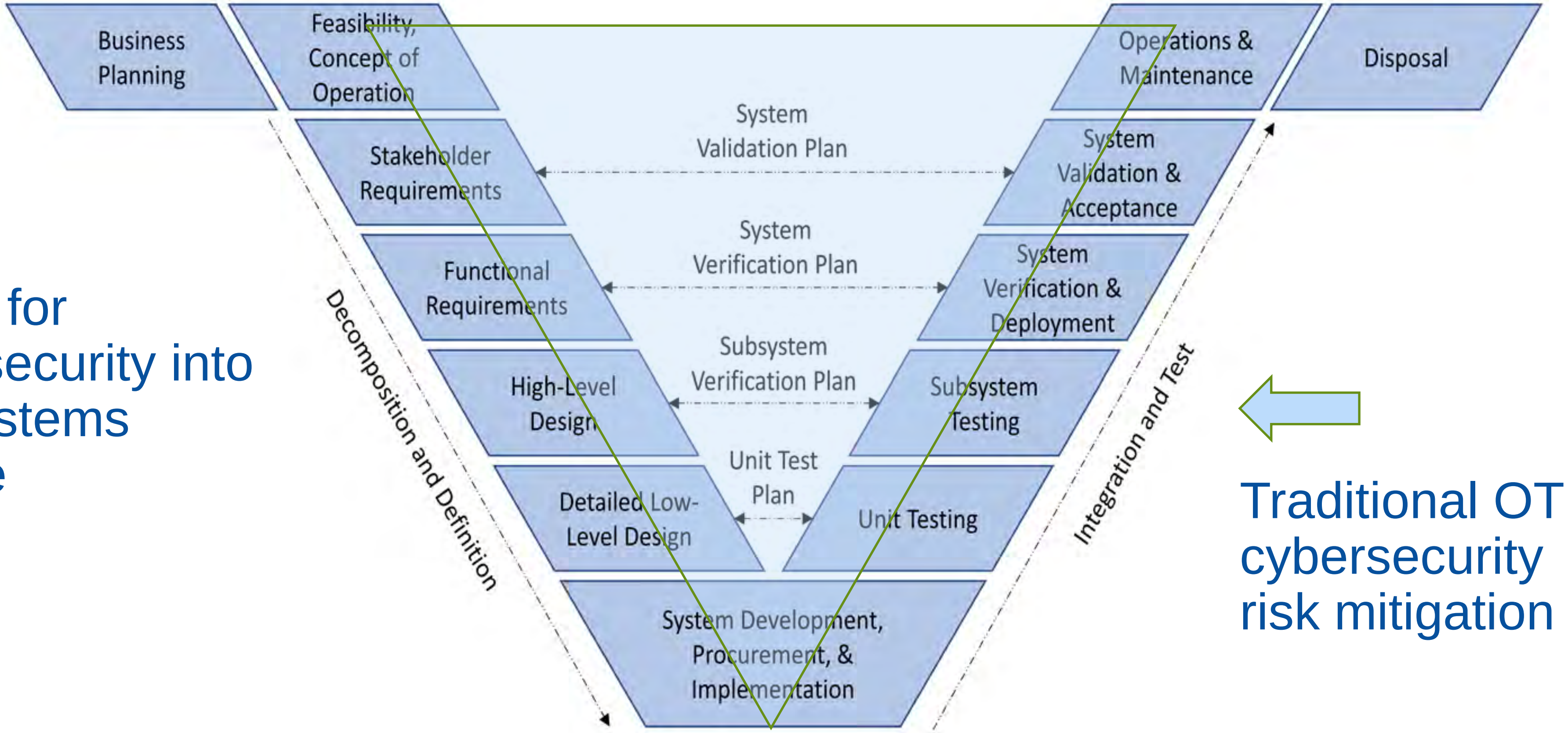
- A systematic approach for including cybersecurity as a foundational element of engineering risk management for functions aided by digital technology
- Integrating cybersecurity risk mitigation into the entire engineering lifecycle, cradle to grave
- Applies both engineering solutions and information technology to minimize the cyber-attack surface



Completes the engineering puzzle by inserting the cyber piece

Engineering or Project Lifecycle

- CIE as a framework for incorporating cybersecurity into all aspects of the systems engineering lifecycle

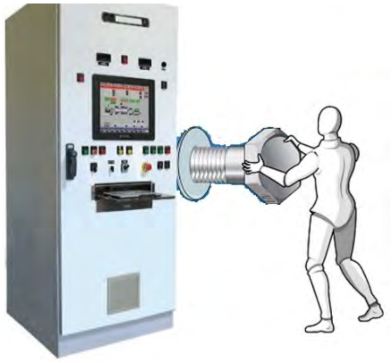


Traditional OT cybersecurity risk mitigation

Why CIE for Fission Batteries?

- Traditional engineering methods do not account for cybersecurity risk
  - Potential to "engineer-out" some security risks
- Unique characteristics such as:
  - Mobile
  - Remote communications
  - Wireless
  - Autonomous operations
- Greater supply chain risk
- BOP? Physical security?

Airgaps are NOT a silver bullet for cyber security!
-Andrew Ginter



Cyber-Informed Engineering Notional Elements

Cybersecurity Risk Management

Secure-by-Design Elements

- Engineering Risk Treatment
- Secure Architecture
- Design Simplification
- Resilient Design
- Active Defense

Organizational Elements

- Interdependencies
- Digital Asset Inventory
- Cyber Secure & Resilient Supply Chain
- Incident Response Planning
- Cybersecurity Culture and Training

Idaho National Laboratory

COLORADO STATE UNIVERSITY

Zero Trust Security for Fission Batteries

Indrajit Ray

Colorado State University

Indrajit.Ray@Colostate.Edu

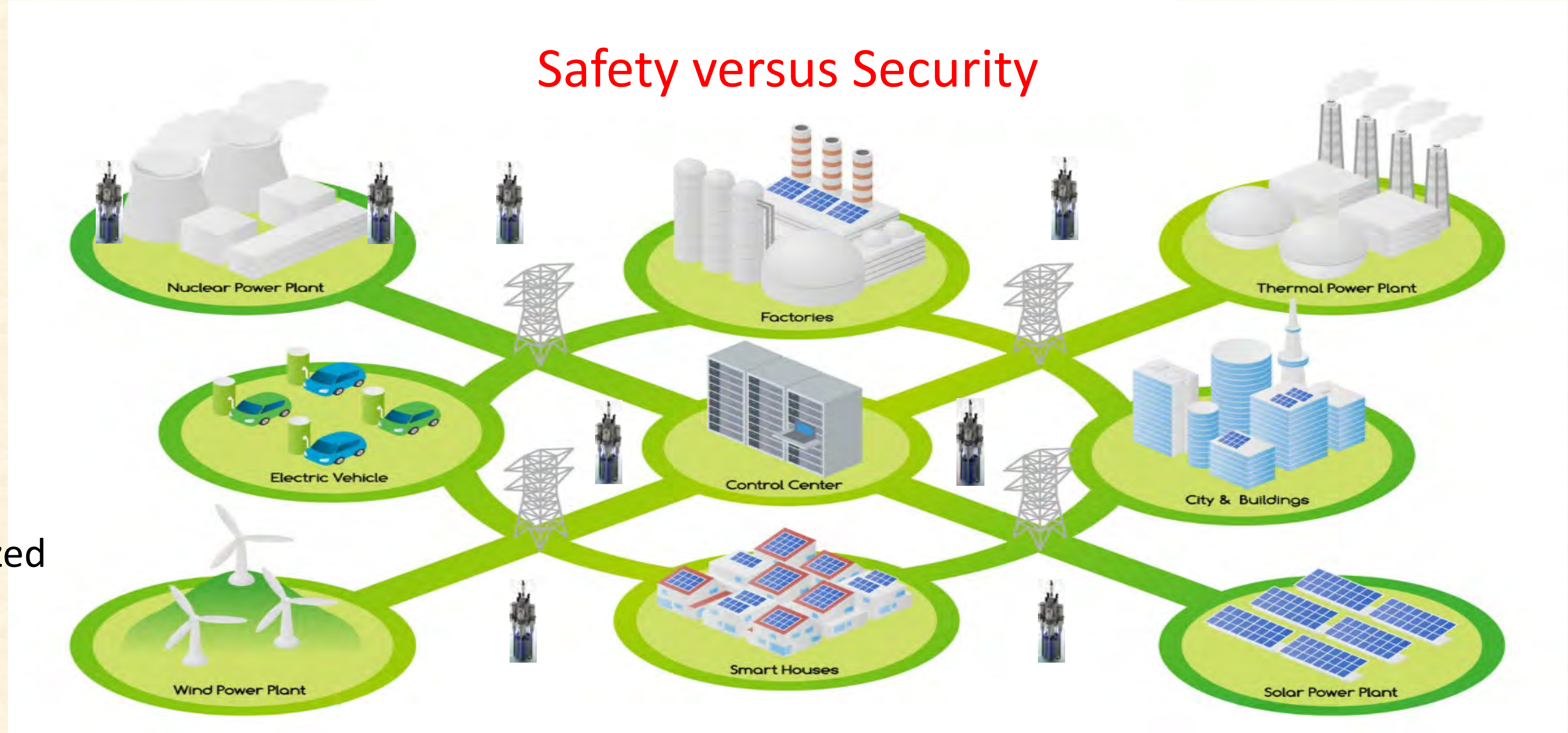
COLORADO STATE UNIVERSITY

Fission Batteries Need to Integrate in a Broader Energy Ecosystem

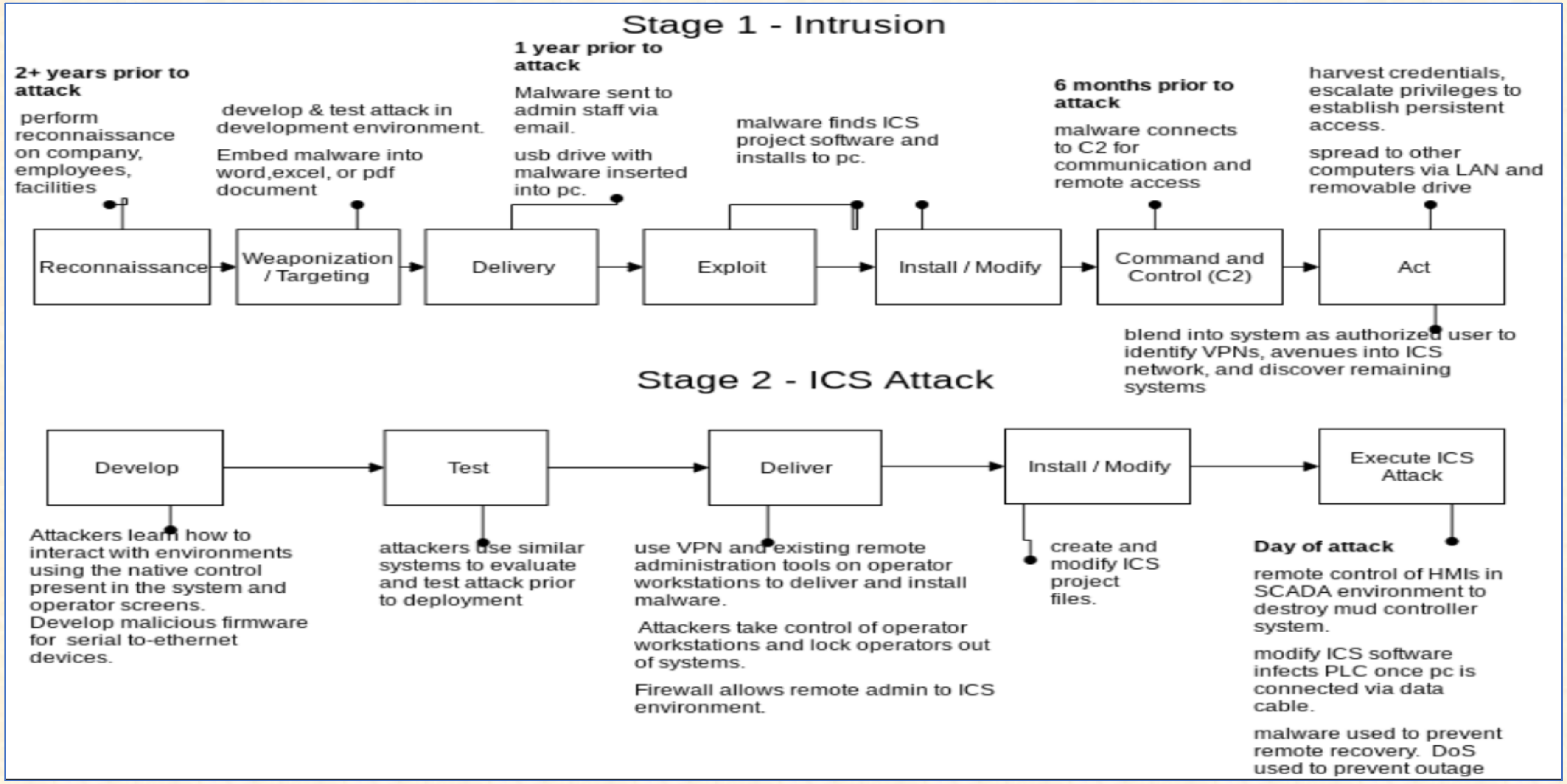
Long term autonomous operation in potentially remote areas

Reduced reliance on human oversight and intervention

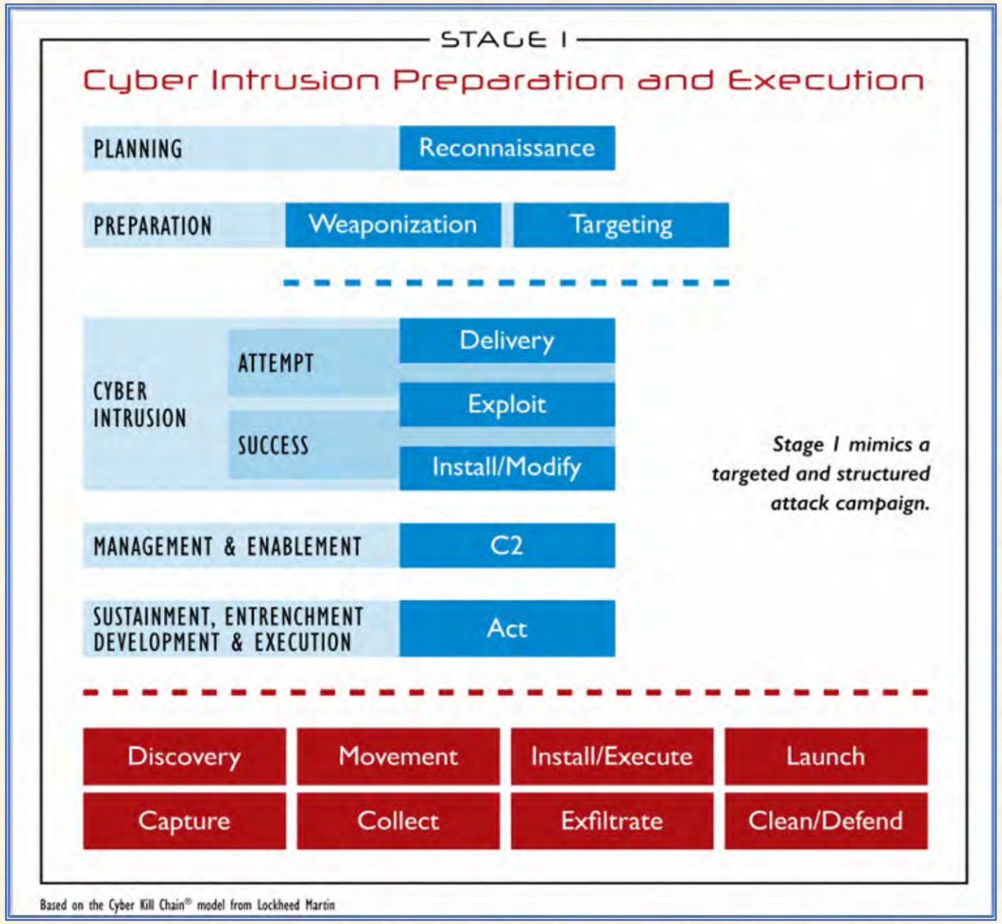
Potential for unauthorized physical access

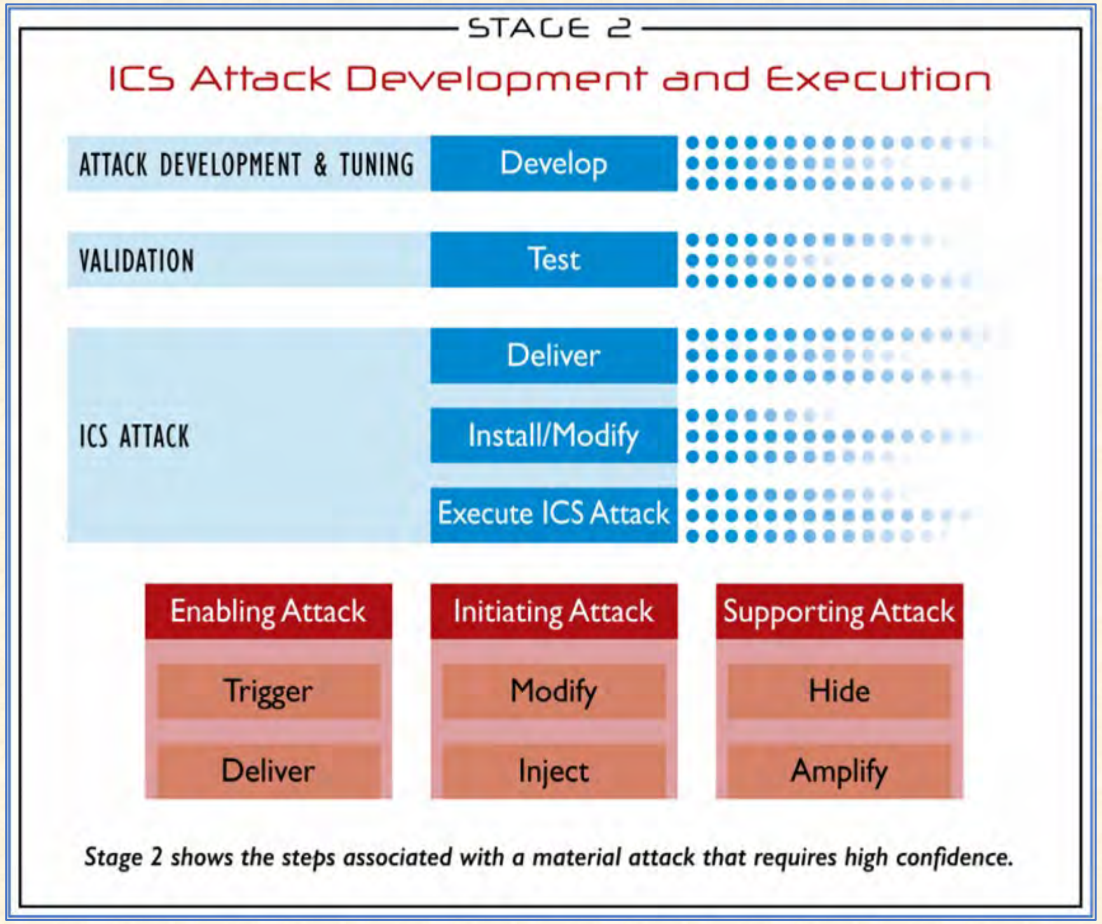


Long-term Autonomous Operation Provides More Opportunities for Cyber Attacks



Access to High Fidelity Simulators and Testbeds Helps Attacker Refine Strategy*





*Based on the Cyber Kill Chain model from Lockheed Martin

COLORADO STATE UNIVERSITY

Fission Battery Threat Landscape

- External threats
  - Hostile governments, Terrorist groups, Individuals
  - Aim to cause physical damage, operational disruption, intellectual property theft
- Insider threats
  - Disgruntled employees, contractors
  - Aim to cause operational disruptions, failures, intellectual property theft
- Human errors
  - Incorrect configurations, failure to monitor, PLC programming errors
- Software threats
  - Adversarial AI, malware in PLC

Cyber Security Needs (1)

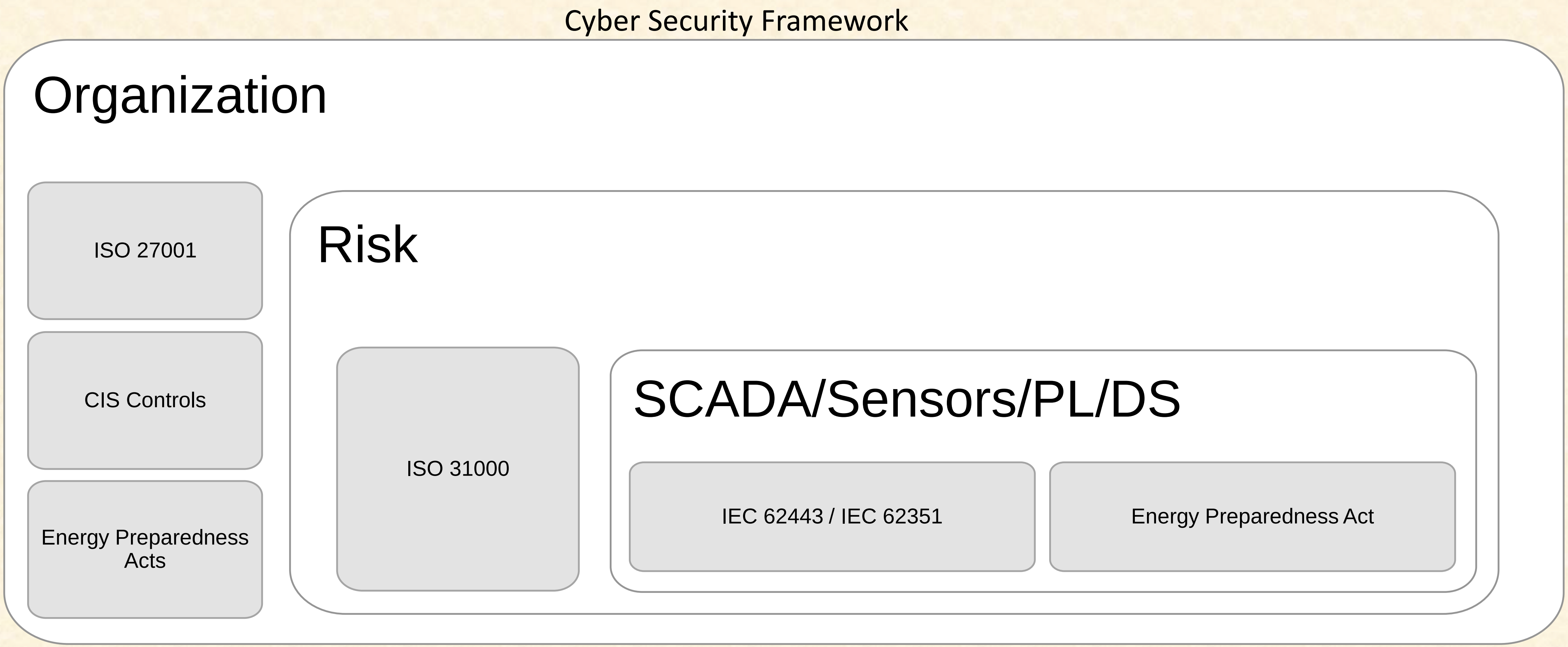
- Need to move away from a static "security perimeter-based" paradigm for protection to dynamic, fine-grained protection of individual fission battery assets
  - Zero trust architecture – NIST SP 800-207
- Need to dynamically adjust access control policies based on perceived threats and risks
  - Continuously limit access to what is needed based on evaluating what the perceived risk is
  - Continuously evaluate trustworthiness of access requester to make decisions

Cyber Security Needs (2)

- Need for local autonomy
  - For authentication when physical as well as remote access is needed
  - For access control decisions

Need for non-binary notions of trustworthiness and approaches to measure the same

Available Techniques That Might Help

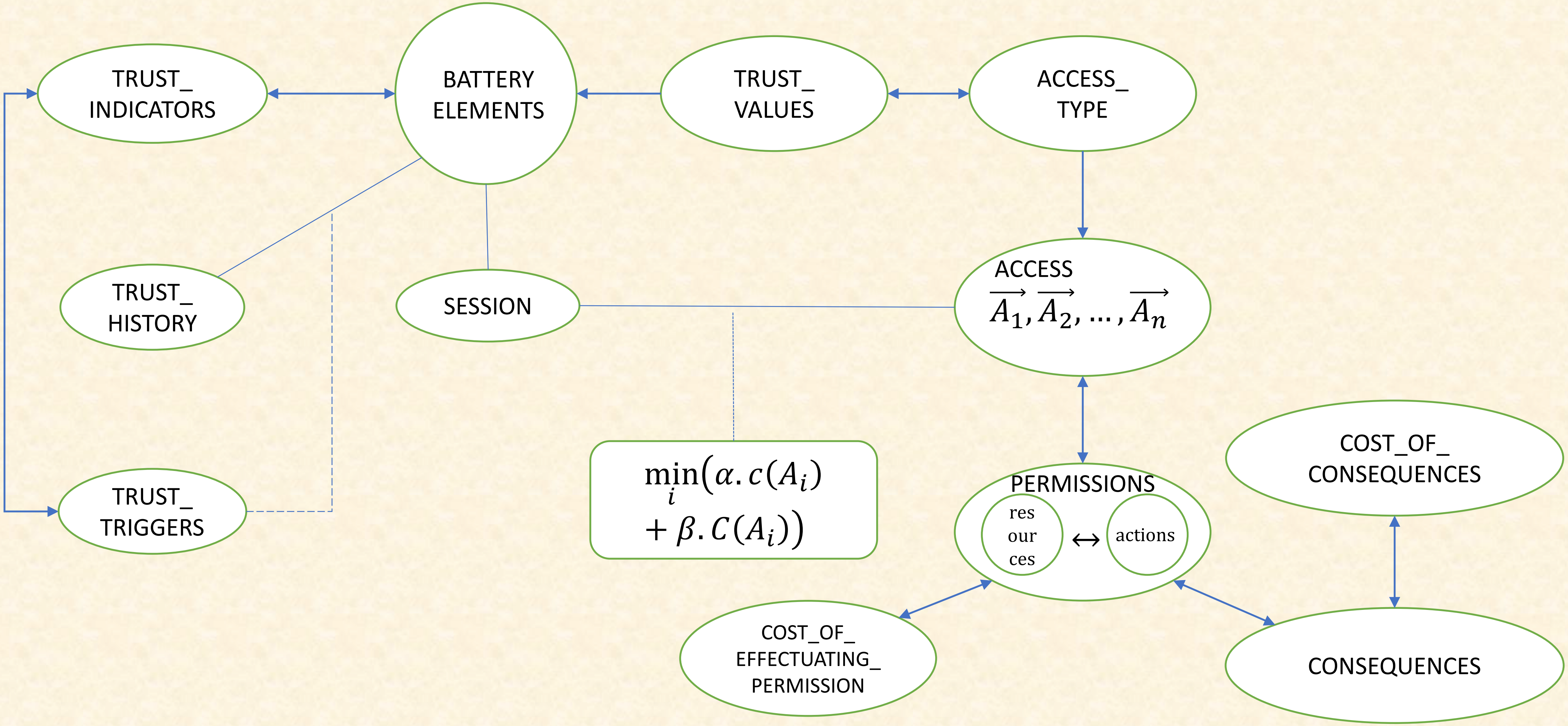


Security Solutions

AVAILABLE SOLUTION	OPEN CHALLENGES
• Risk Management & Assessment • Asset Inventory • Software Management • Software / Firmware Patching • Perimeter Defense • Network Segmentation • Secure Remote Connection • Monitoring	• Perimeter-less Defense • Trust Estimation • Dynamic, Risk-centric Authorization • Adaptable Access Control • Moving Target Defense

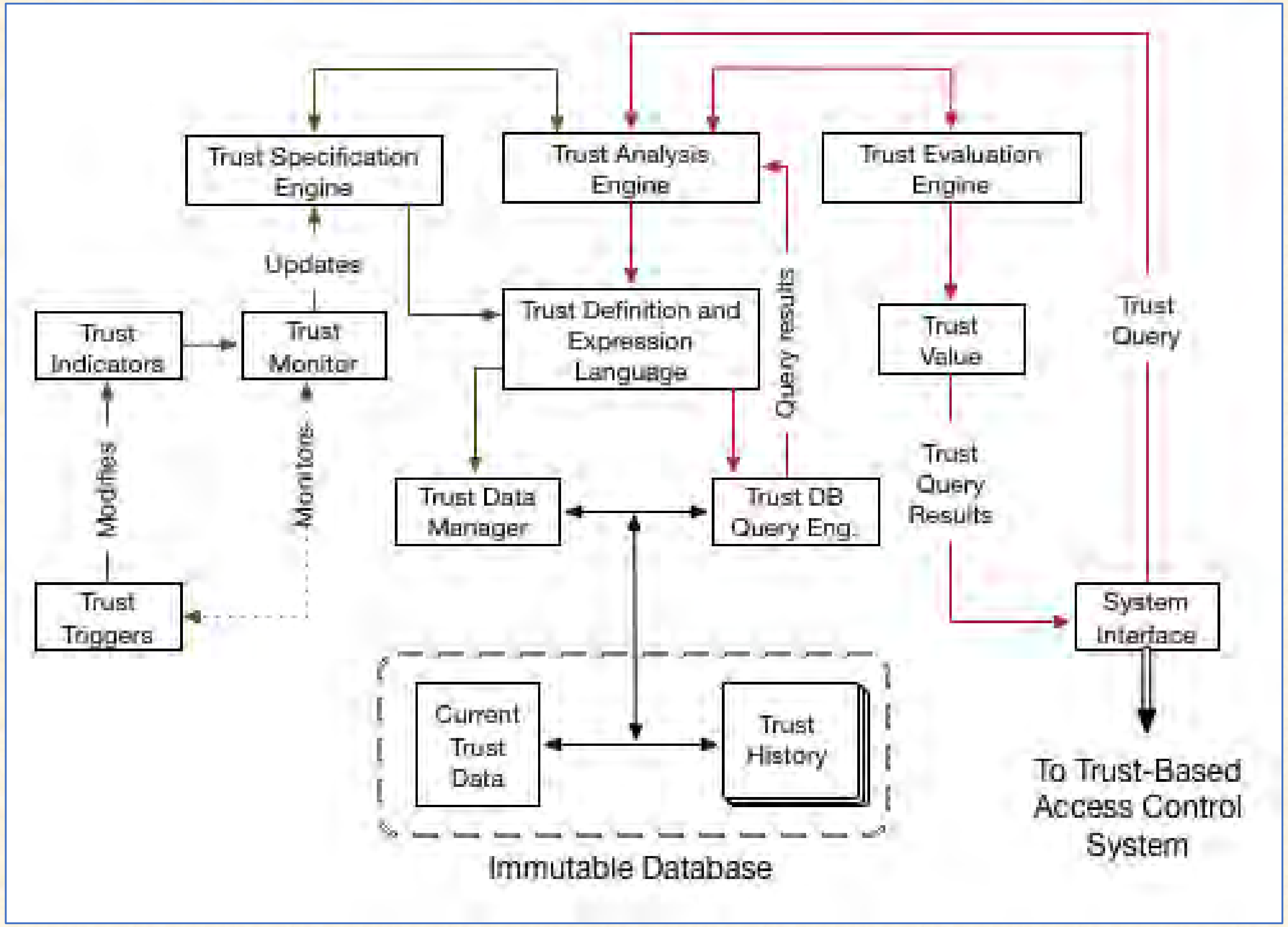
COLORADO STATE UNIVERSITY

Trust Based Access Control Model For ICS

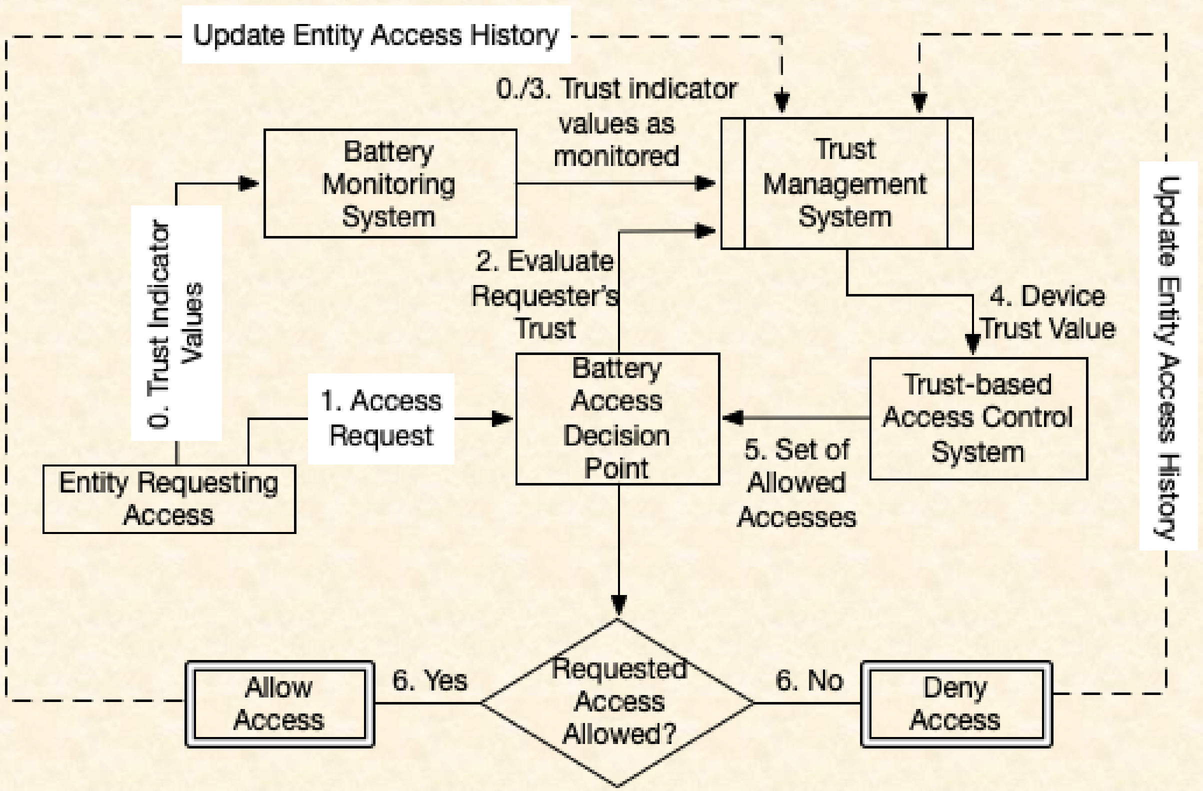


COLORADO STATE UNIVERSITY

Locally Autonomous Trust Management System

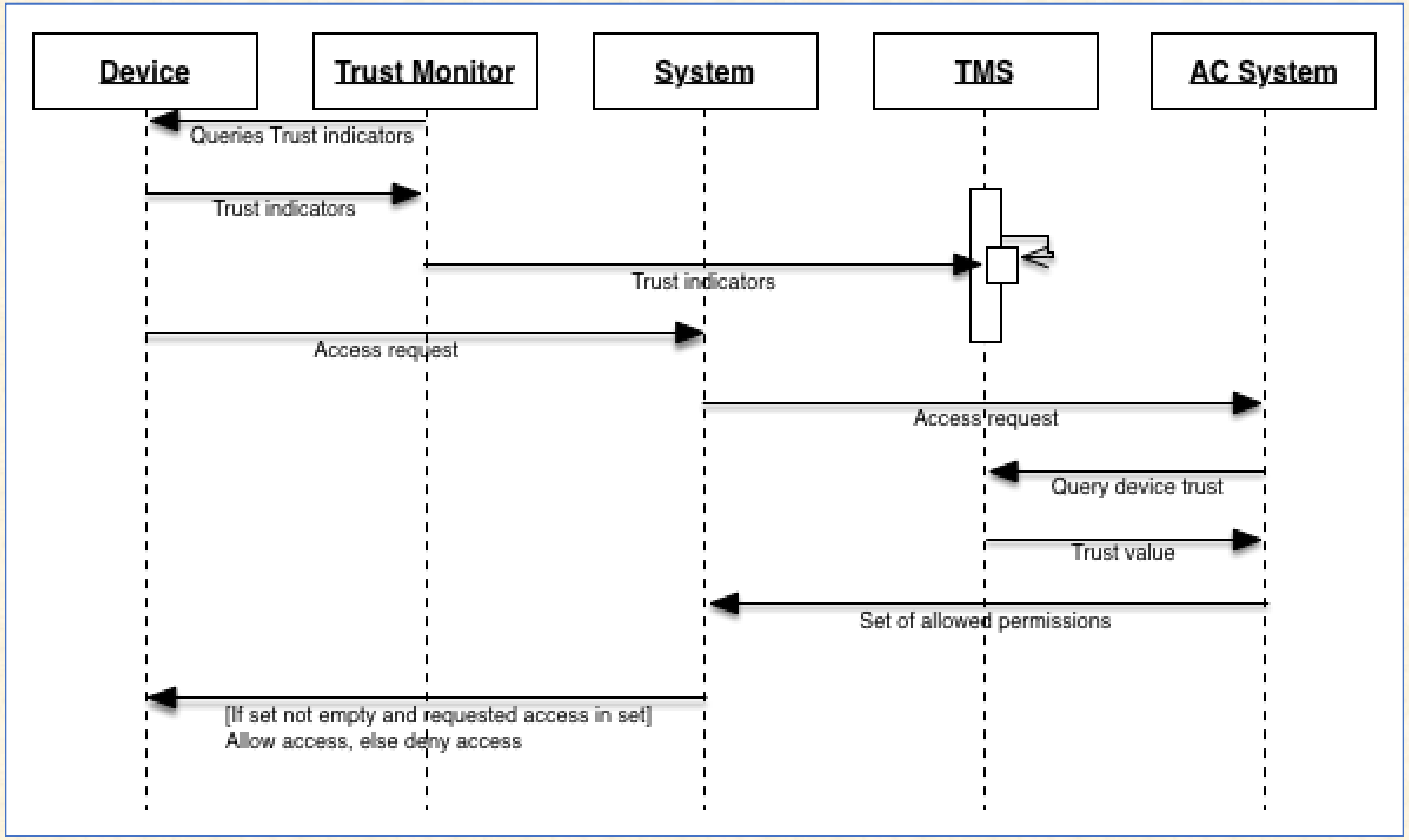


Fission Battery Hybrid Zero-Trust Framework



- Trust Management System
  - Trust Model
  - Trust Evaluation Engine
- Trust Based Access Control System
  - Decision Engine to select applicable set of policies
- Assumption: Every component in battery has a unique identifier that is strongly tied to the component

Trust Based Access Control Protocol



Questions

Cross-Layer Cyber-Physical Security of Fission Battery Control Systems

Quanyan Zhu

Tandon School of Engineering
New York University

Workshop on Safeguards and Security of Fission Batteries

April 2, 2021

NYU | Systems and Control Group

CUSP CENTER FOR URBAN SCIENCE+PROGRESS

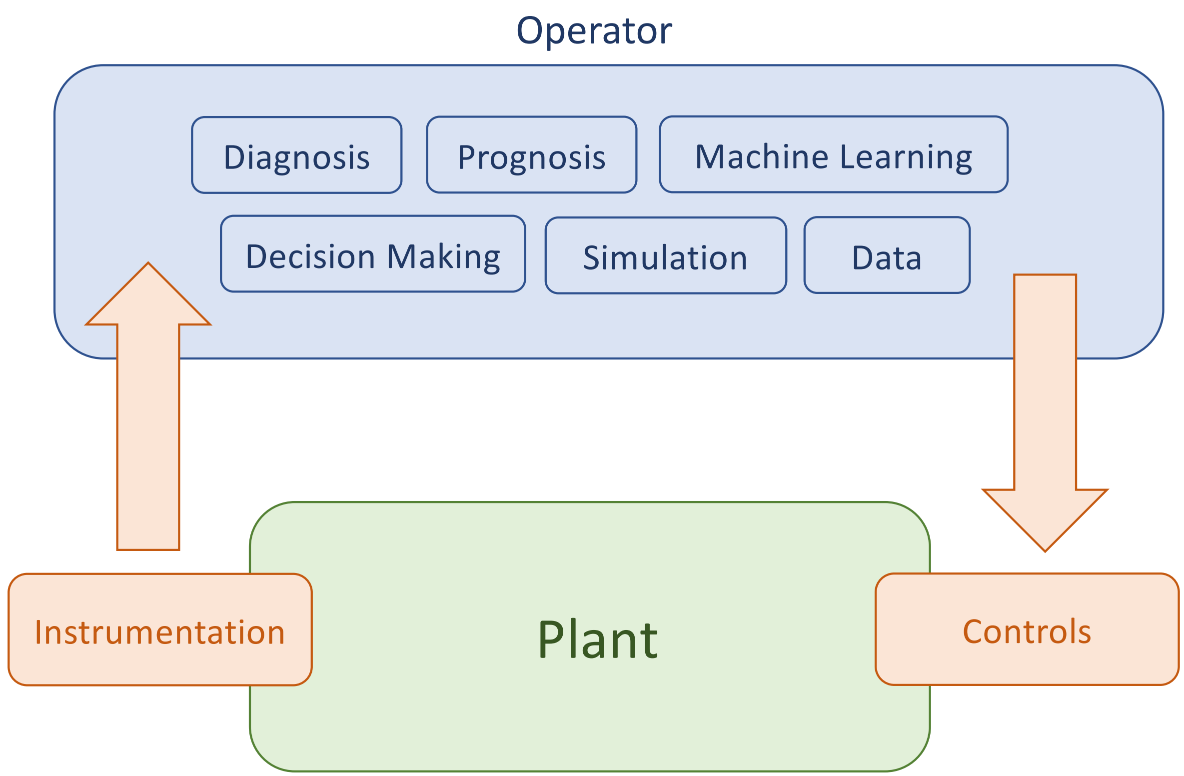
CENTER FOR CYBER SECURITY

Fission Battery Attributes

Unattended: Operated securely and safely in an unattended manner to provide demand-driven power.

Reliable: Equipped with systems and technologies that have a high level of reliability to support the mission life and enable deployment for all required applications. They must be robust, resilient, fault tolerant, and durable to achieve fail-safe operation.

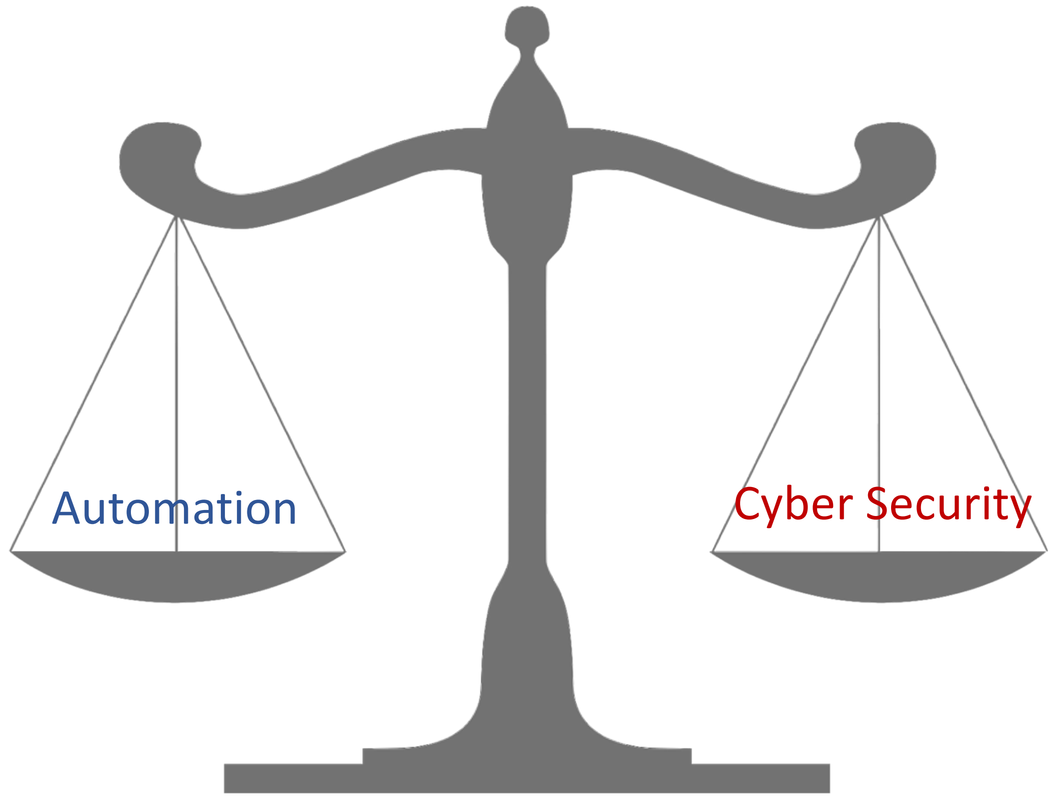
Toward Autonomous Operations

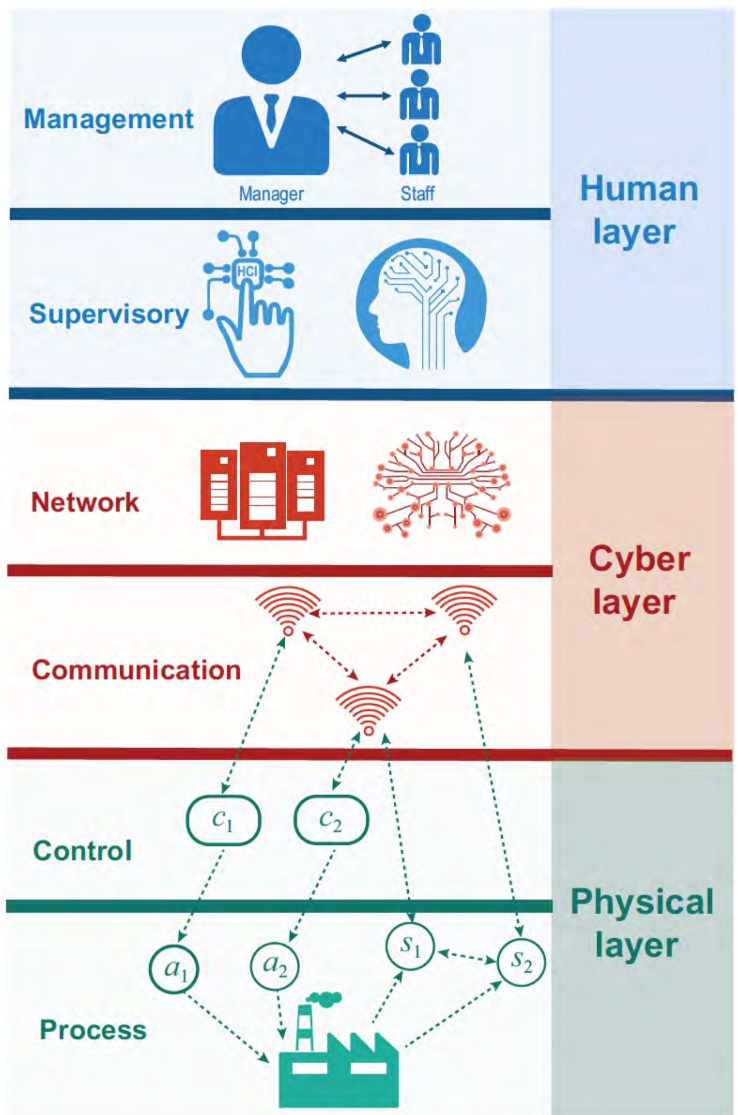


Automation is the key to achieve the attributes of being economic, unattended, and reliable.

- Operators for fission batteries are costly.
- Constrained cost of operation, maintenance, and design.
- Most fission battery customers are not in energy business: We need less operator intervention and enable unattended operations.

More intelligence introduces security vulnerabilities.





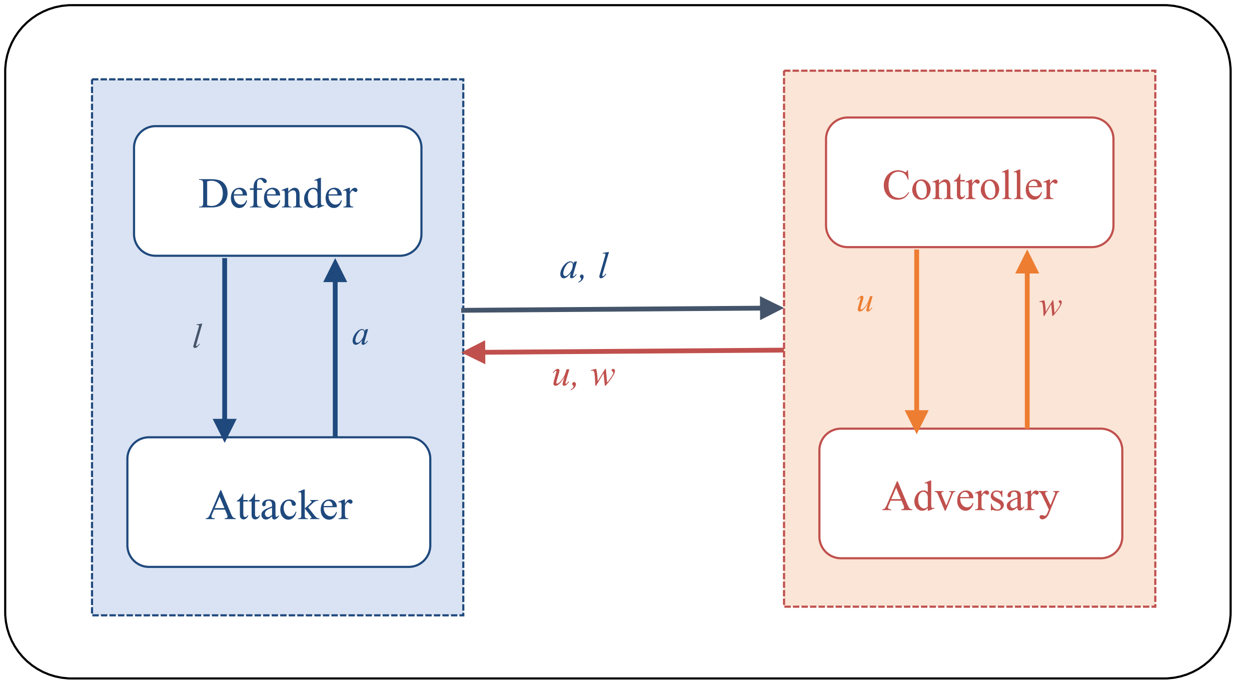
Multi-Layer Perspective of Autonomy

Human Vulnerabilities: Social engineering, human errors, etc.

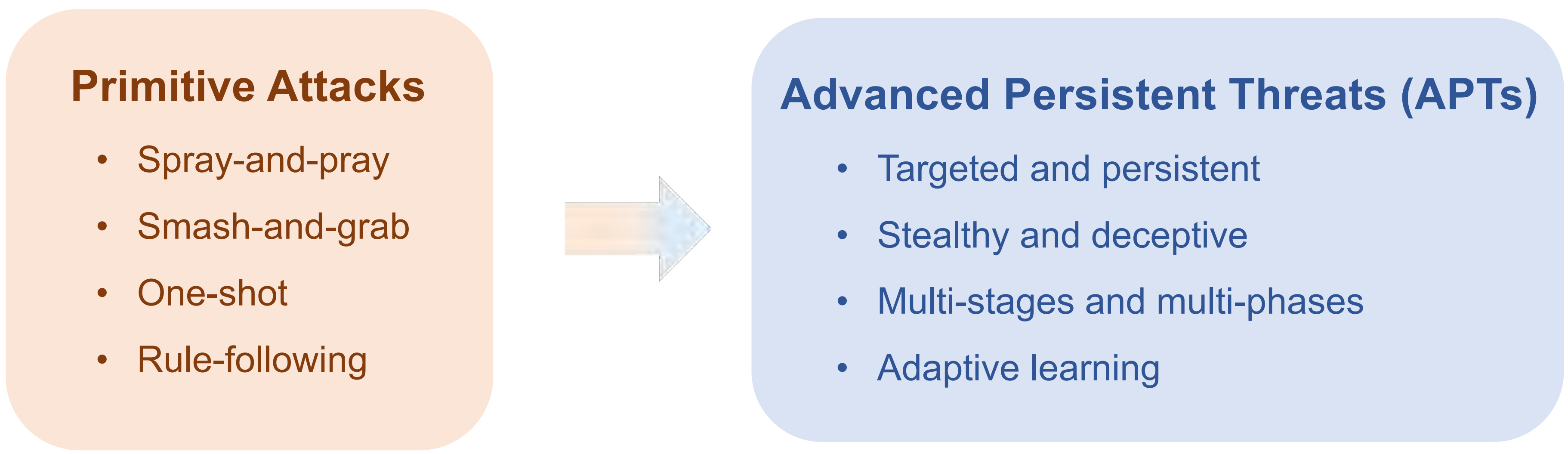
Cyber Vulnerabilities: Adversarial AI, Advanced Persistent Threats, etc.

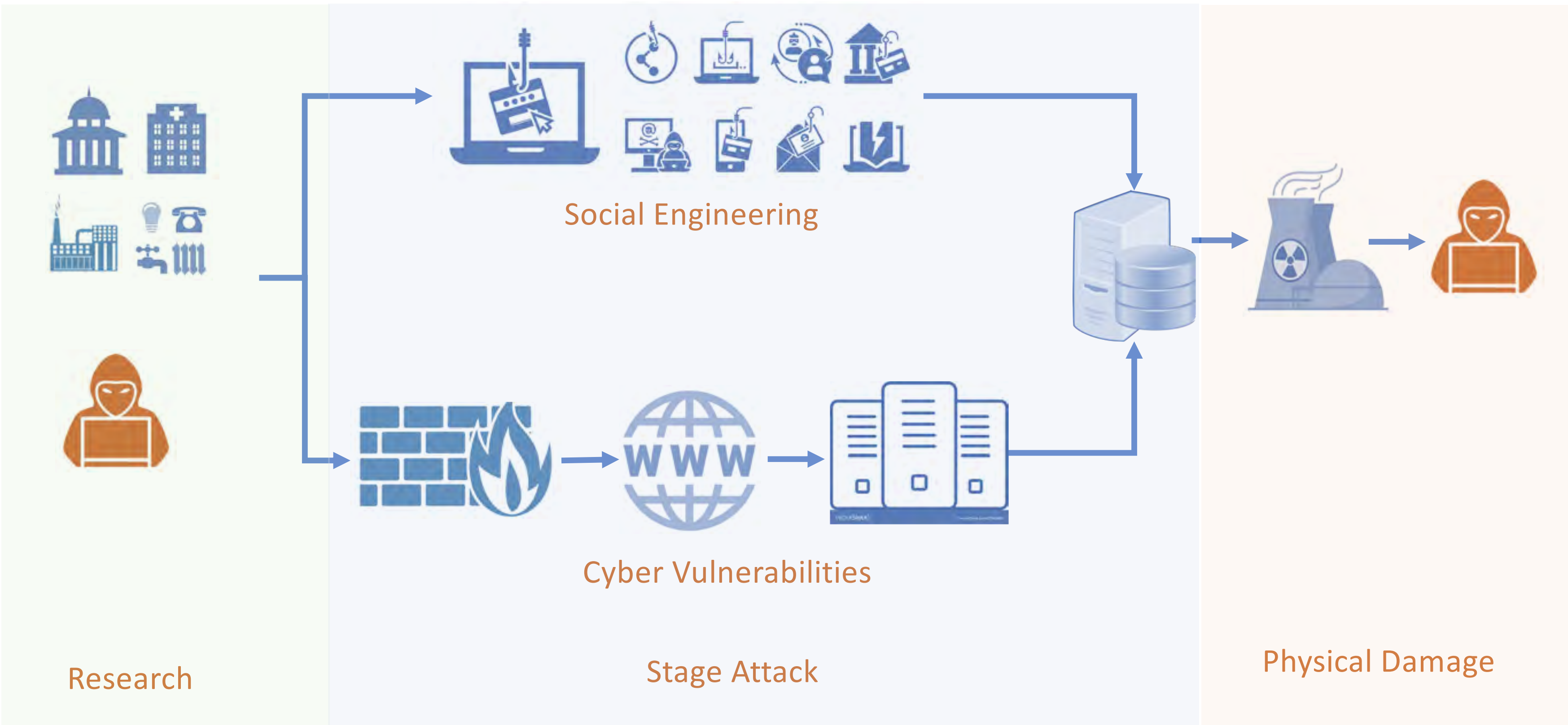
Physical Vulnerabilities: False data injection, cascading failures, etc.

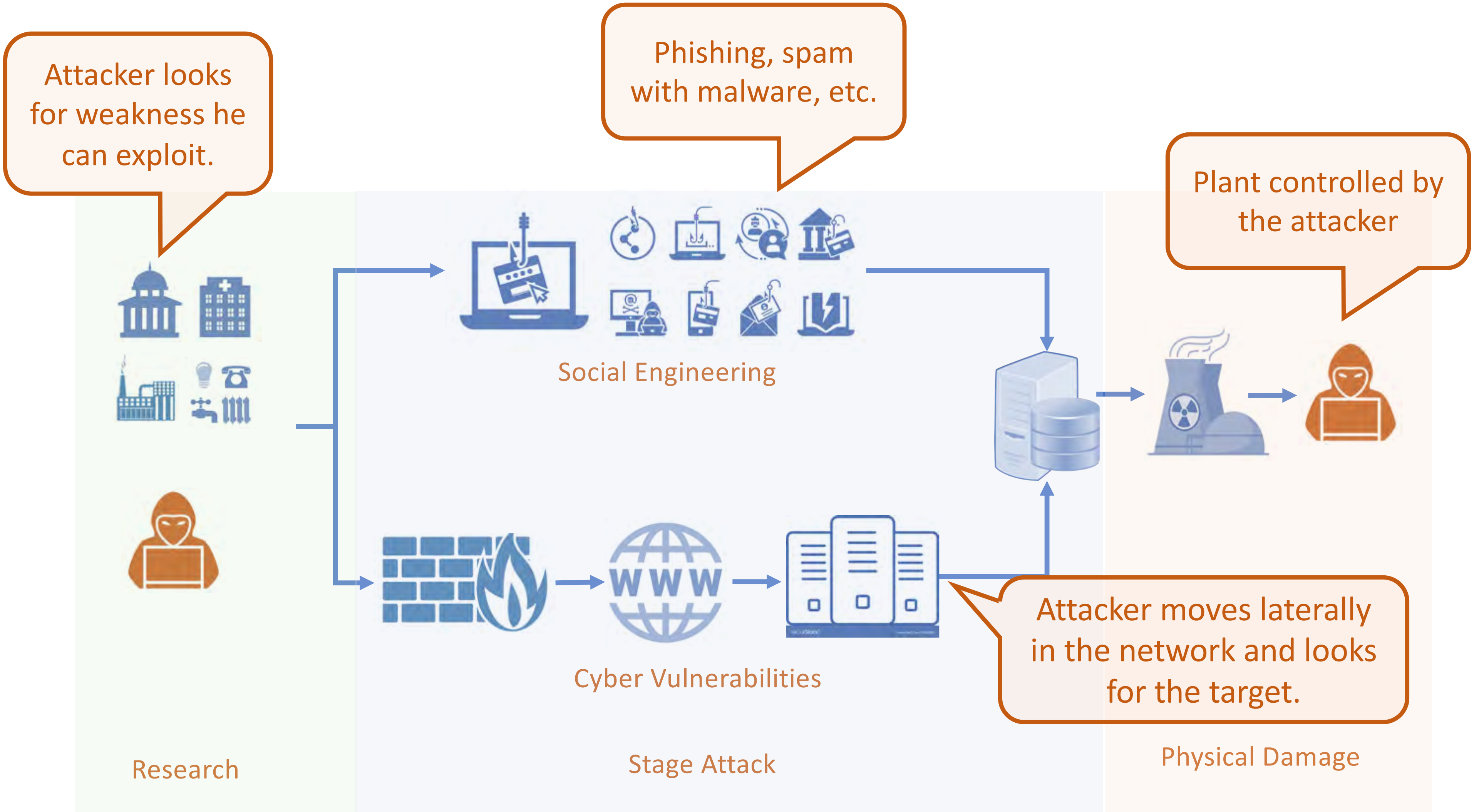
Cross-Layer Protections



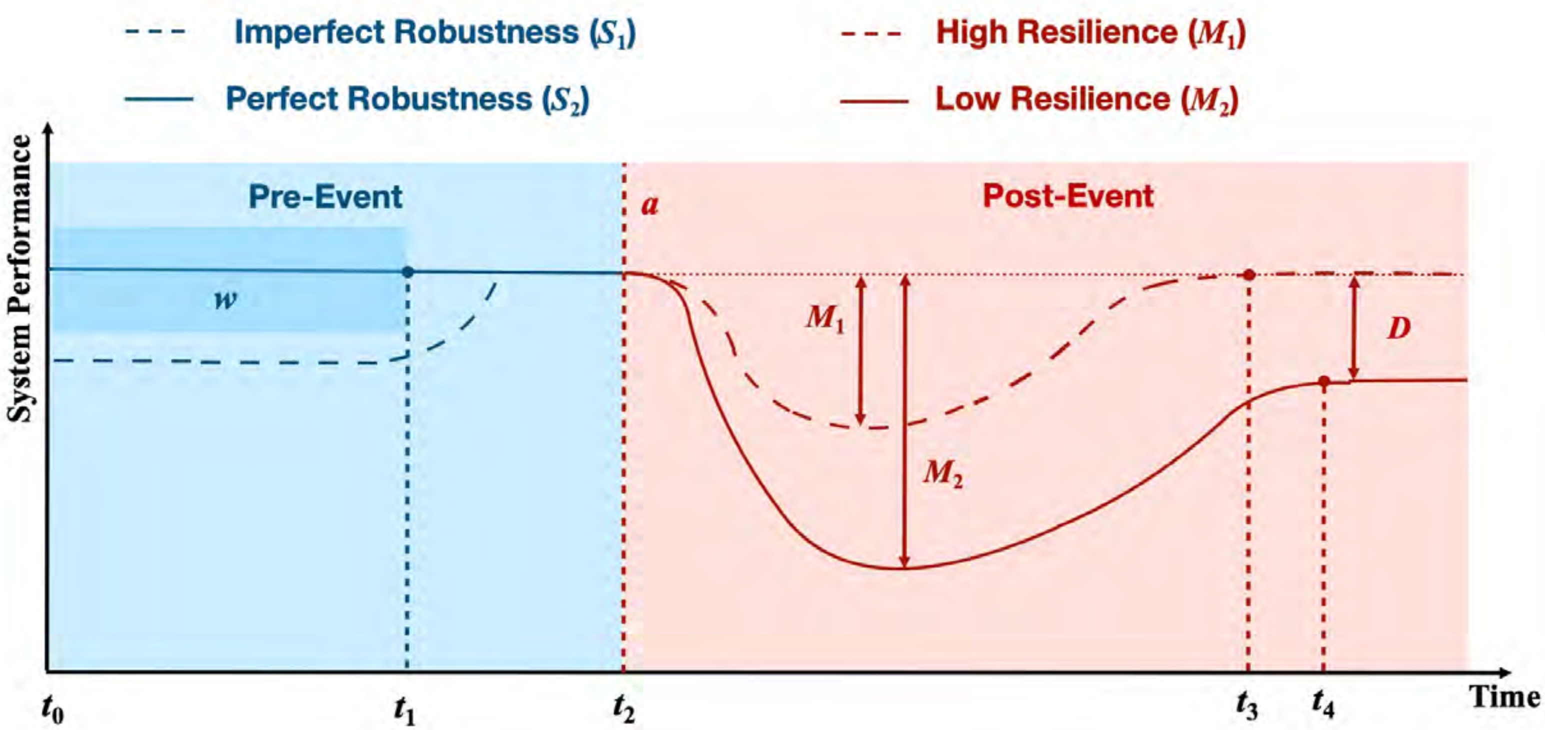
- ***a***: cyber attack
- ***l***: defense
- ***u***: control
- ***w***: physical attack

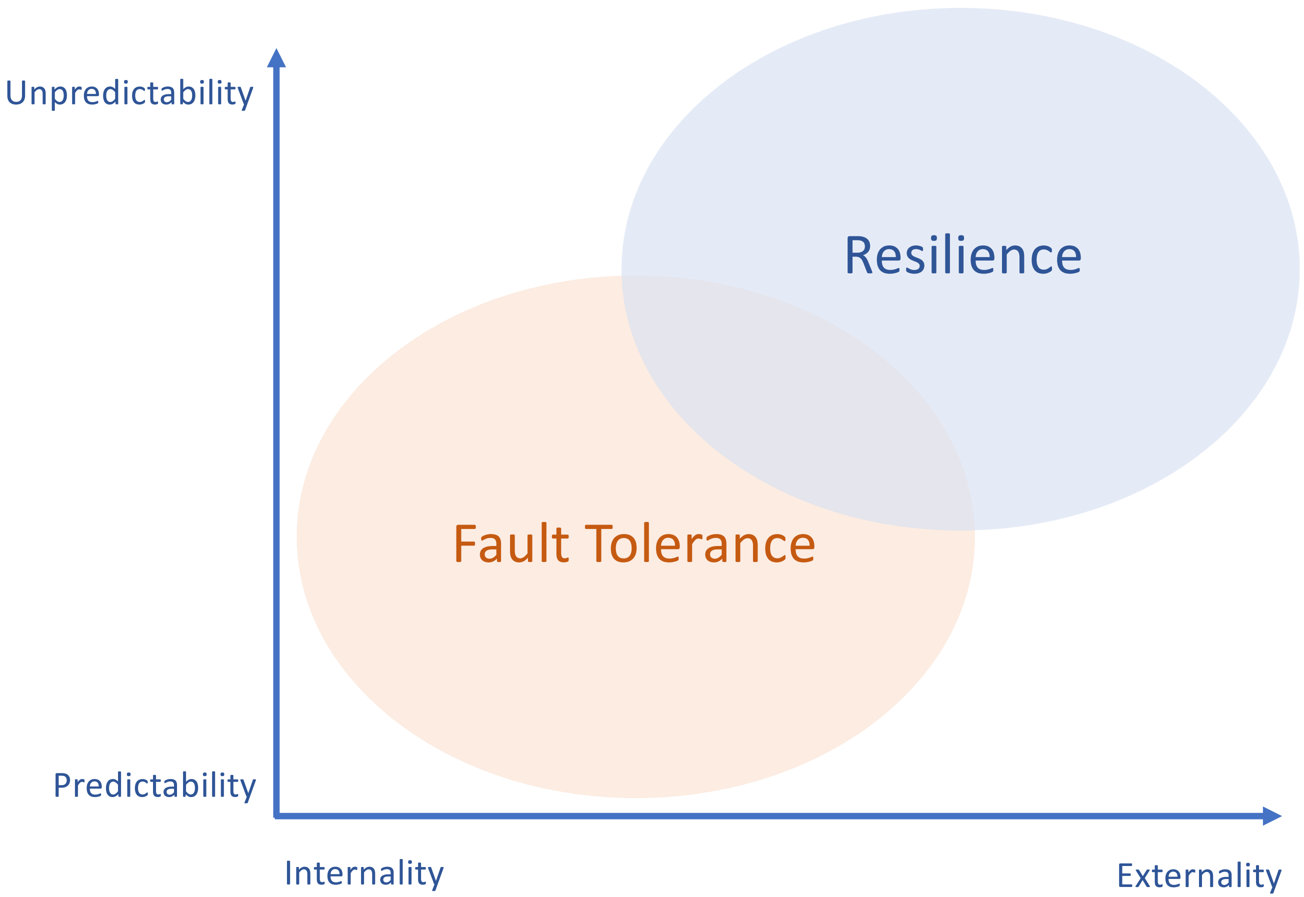

Primitive Attacks
Spray-and-pray
Smash-and-grab
One-shot
Rule-following
Advanced Persistent Threats (APTs)
Targeted and persistent
Stealthy and deceptive
Multi-stages and multi-phases
Adaptive learning


Social Engineering
Cyber Vulnerabilities
Research
Stage Attack
Physical Damage

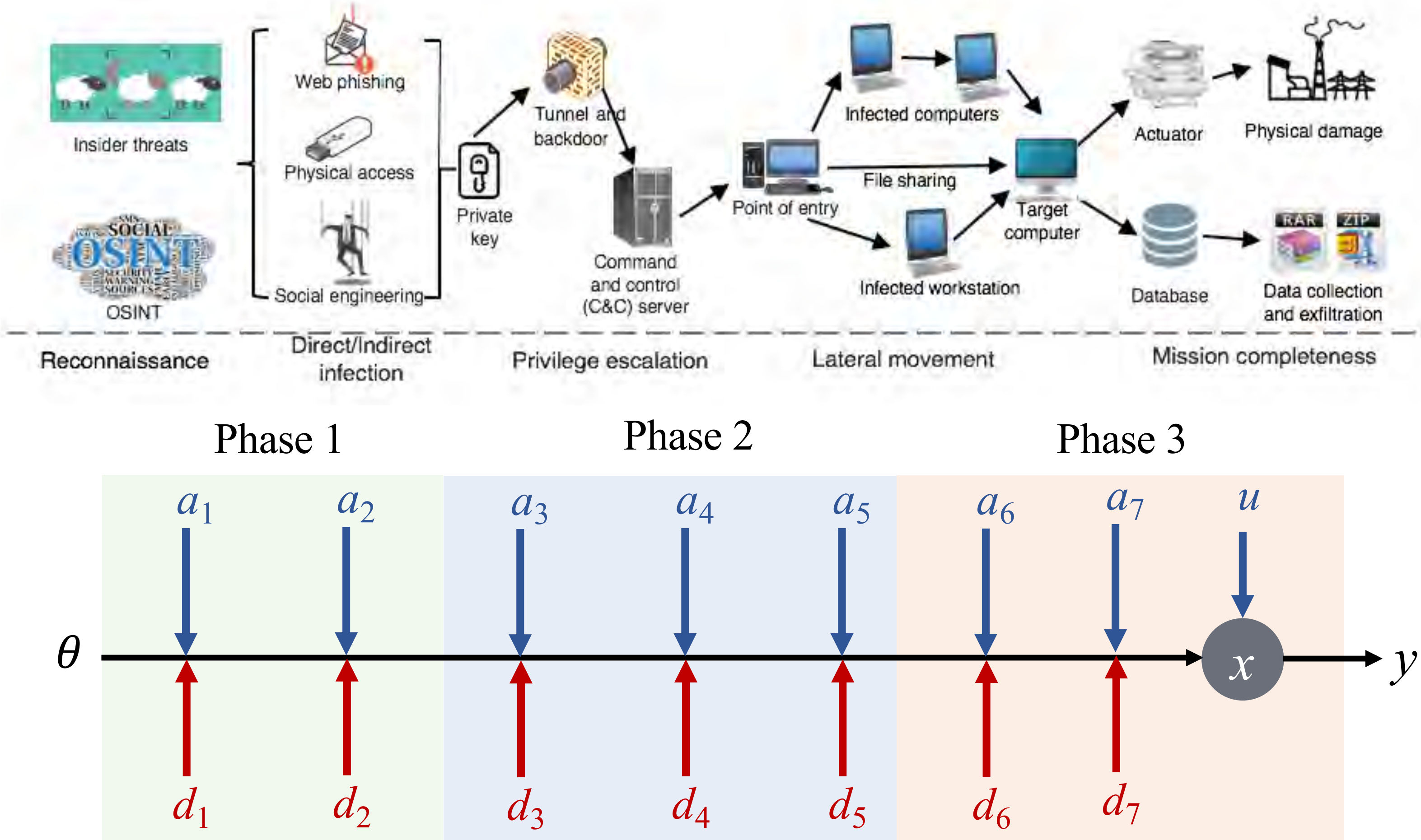

Attacker looks for weakness he can exploit.
Phishing, spam with malware, etc.
Plant controlled by the attacker
Social Engineering
Cyber Vulnerabilities
Attacker moves laterally in the network and looks for the target.
Research
Stage Attack
Physical Damage

Two aspects of Protection: Prevention and Resilience





Unpredictability
Resilience
Fault Tolerance
Predictability
Internality
Externality



Insider threats
OSINT
Web phishing
Physical access
Social engineering
Private key
Tunnel and backdoor
Command and control (C&C) server
Point of entry
Infected computers
File sharing
Infected workstation
Target computer
Actuator
Physical damage
Database
Data collection and exfiltration
Reconnaissance
Direct/Indirect infection
Privilege escalation
Lateral movement
Mission completeness
Phase 1
Phase 2
Phase 3
a_1 a_2 a_3 a_4 a_5 a_6 a_7 u
θ
x
y
d_1 d_2 d_3 d_4 d_5 d_6 d_7

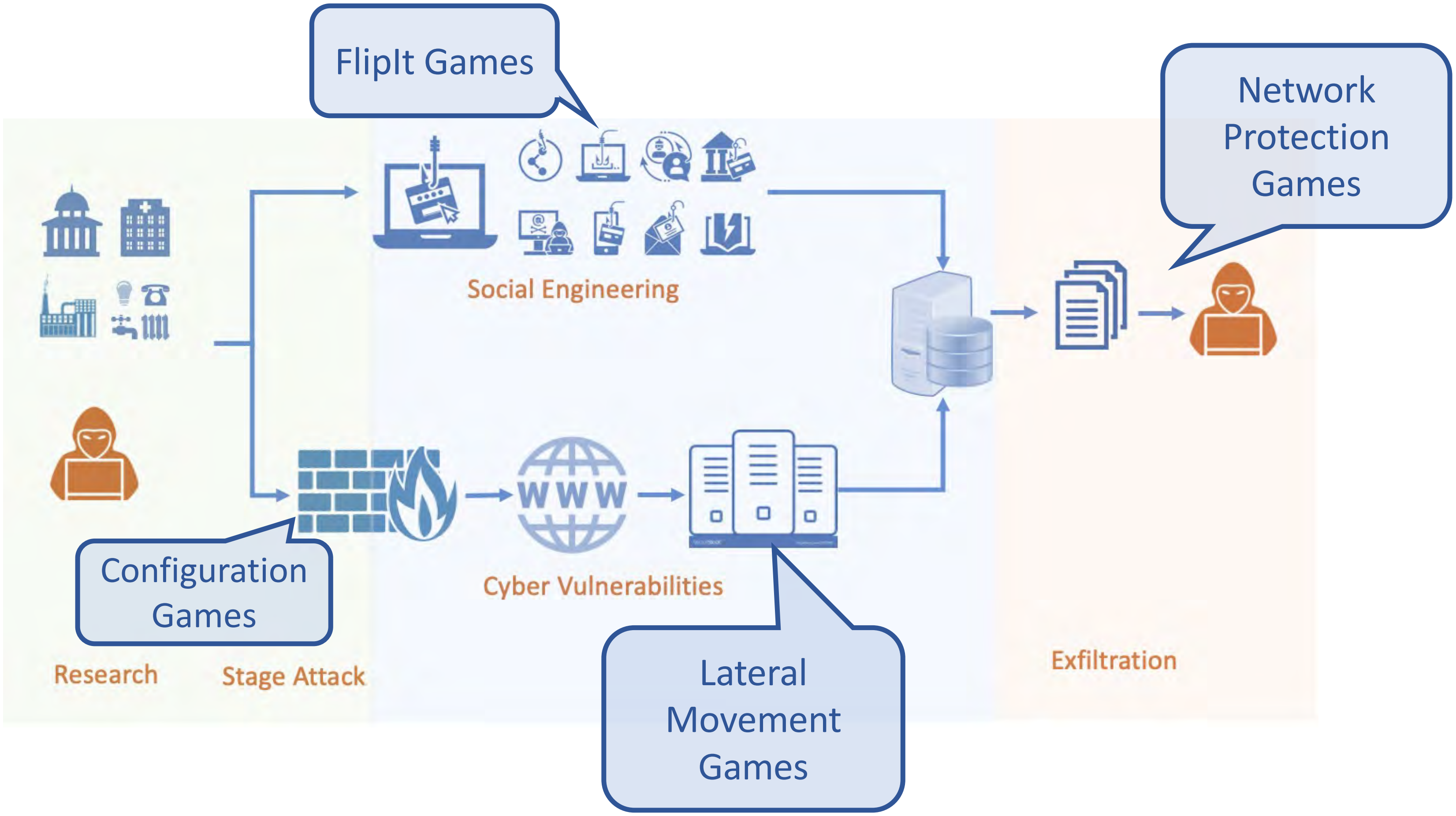
Security and Resilience by Design

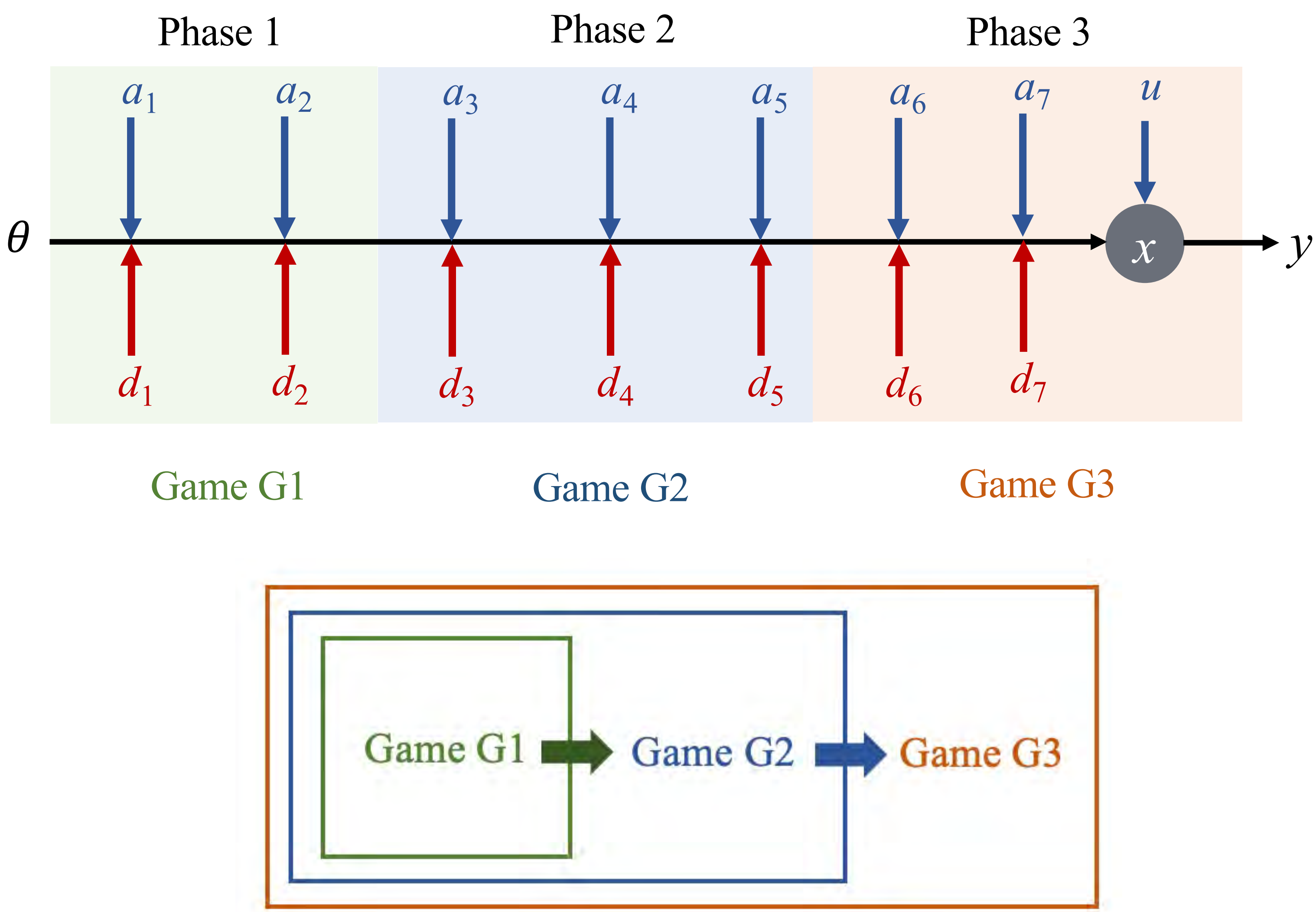
- Design under human, cyber, and physical constraints.
- Game models can be used for risk analysis and strategic design of defense mechanisms.
- Game models provide ways to design new defense mechanisms
  - Moving target defense
  - Deception
  - Automated defense

Game-Theoretic Risk Assessment

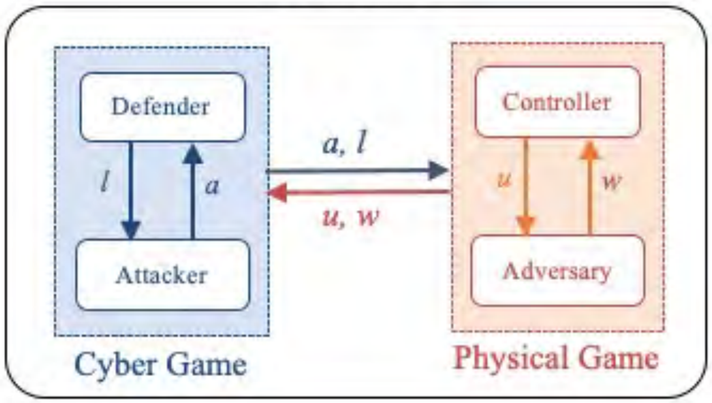
- Evaluate risks under a prescribed attack model.
- Game-theoretic models can specify
  - Attacker capability and resources
  - Attacker information
  - Attacker objectives
  - Attacker rationality
- Equilibrium solutions:
  - Predict the outcome in the long run.
  - Evaluate the cyber risk
  - Design the defense
- Baseline models guide the way to learn and assess risks online.

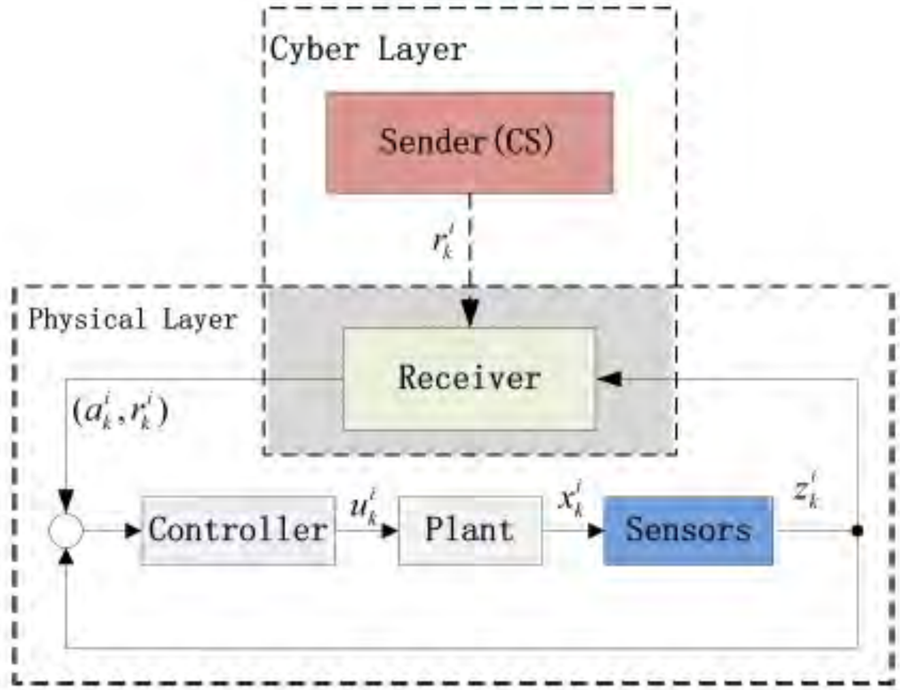
Games as Building Blocks




Phase 1
Phase 2
Phase 3
a_1 a_2 a_3 a_4 a_5 a_6 a_7 u
θ
x
y
d_1 d_2 d_3 d_4 d_5 d_6 d_7
Game G1
Game G2
Game G3
Game G1
Game G2
Game G3

Example: Strategic Trust

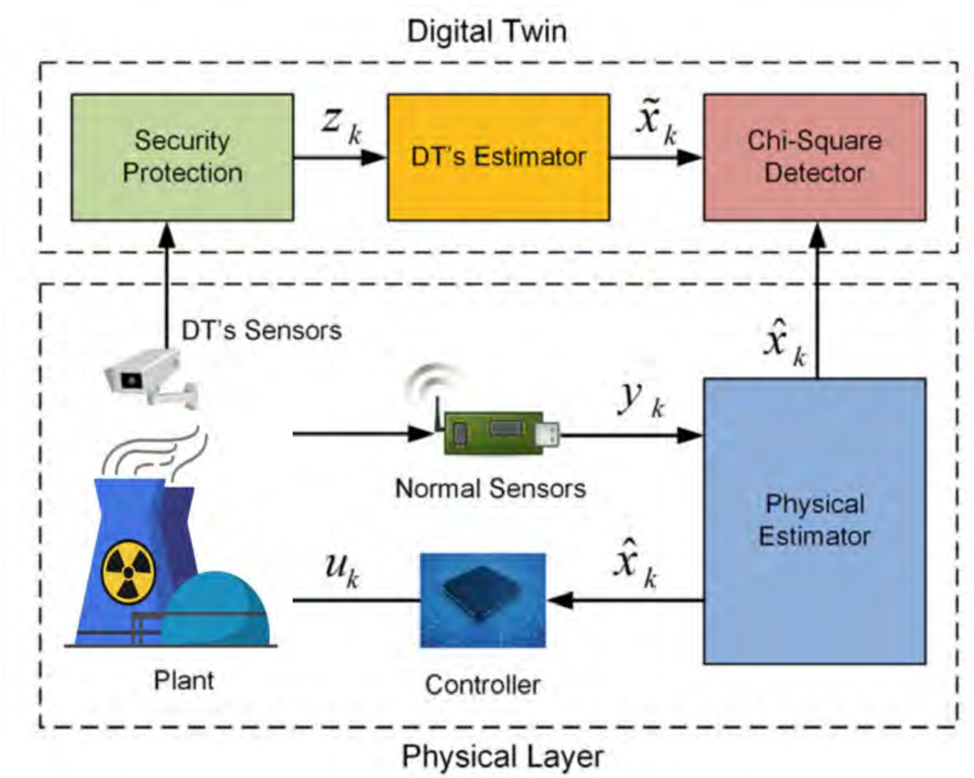




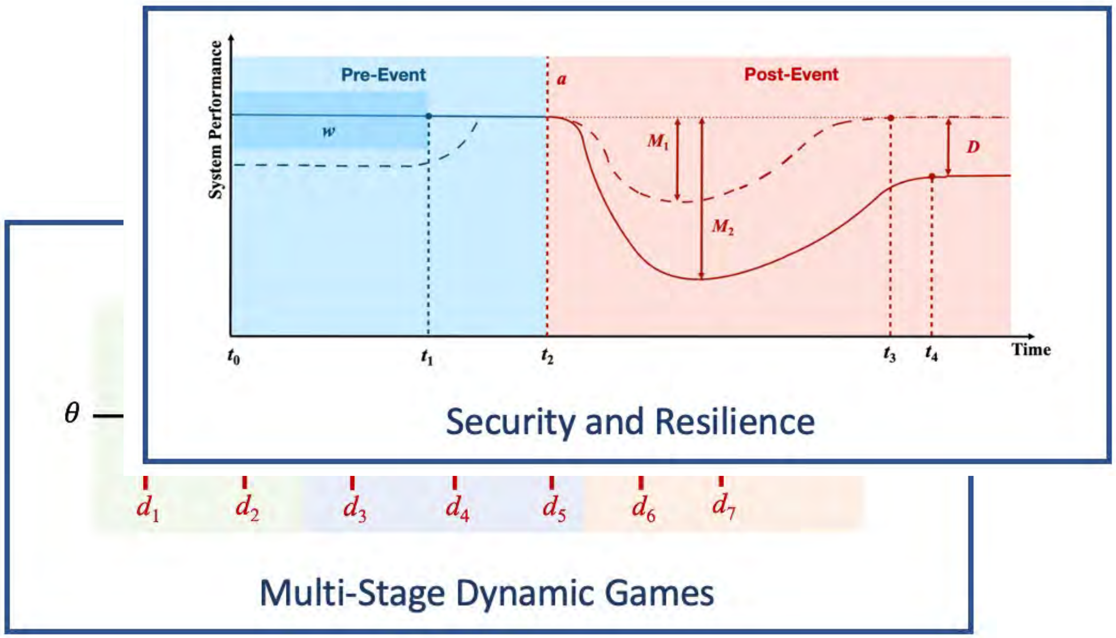
- a: cyber attack
- l: defense
- u: control
- w: physical attack

- r: command and control message
- a: actuation
- u: control
- x: physical state
- z: sensor output

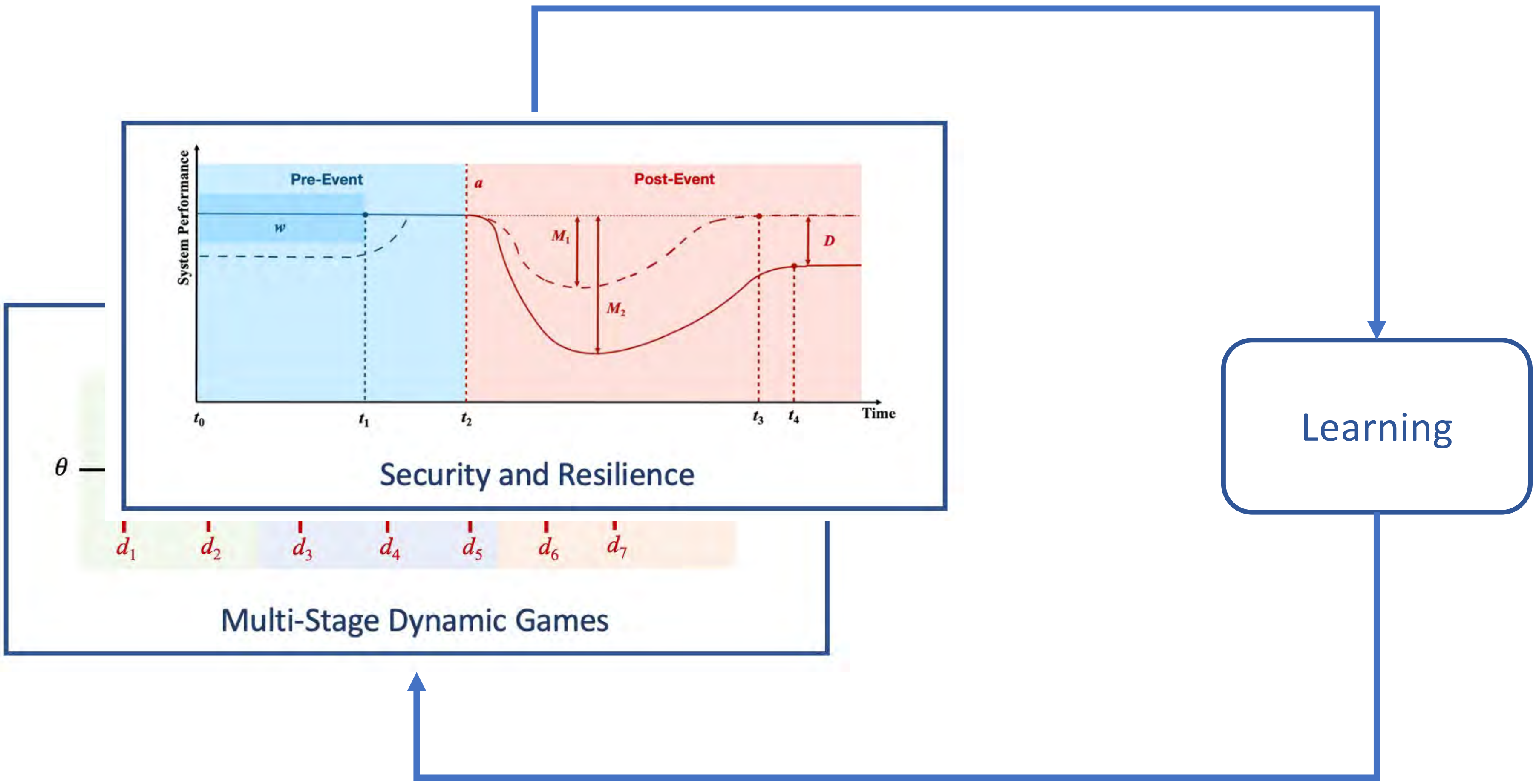
Digital Twin



The physical estimator sends the estimation to the DT, which uses its secure evidence to verify the identity of the estimator.



Human and
Uncertainties



Pre-Event
Post-Event
System Performance
w
a
M_1
M_2
D
t_0
t_1
t_2
t_3
t_4
Time
Security and Resilience
θ
d_1 d_2 d_3 d_4 d_5 d_6 d_7
Multi-Stage Dynamic Games
Learning

April 2, 2021

Robert England
I&C Research Engineer

Experimental Testbeds and Cyber Hardening of Fission Batteries

Nuclear Science and Technology

Idaho National Laboratory

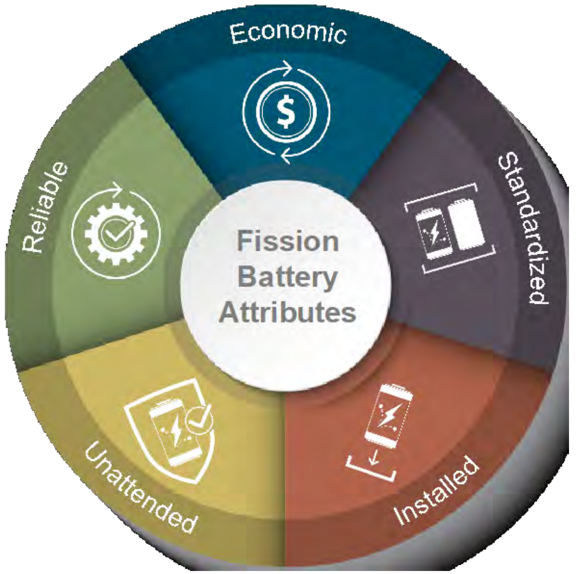
Experimental Testbeds

Provide a safe environment for testing and checkout of proposed fission battery hardware

- Must be hosted in a secure environment
- Good cyber hygiene must be maintained
- Components to be utilized for control of fission batteries must be thoroughly tested to ensure compliance to cybersecurity standards
- Vendor equipment must be scanned and sanitized before interfacing with control hardware
- Capable of leveraging sandbox environments to ensure that sensor data is secure and that no reverse communication can affect battery operation

Fission Battery Attributes

- **Economic** – Cost competitive with other distributed energy sources (electricity and heat) used for a particular application in a particular domain. This will enable flexible deployment across many applications, integration with other energy sources, and use as distributed energy resources.
- **Standardized** – Developed in standardized sizes, power outputs, and manufacturing processes that enable universal use and factory production, thereby enabling low-cost and reliable systems with faster qualification and lower uncertainty for deployment.
- **Installed** – Readily and easily installed for application-specific use and removal after use. After use, fission batteries can be recycled by recharging with fresh fuel or responsibly dispositioned.
- **Unattended** – Operated securely and safely in an unattended manner to provide demand-driven power.
- **Reliable** – Equipped with systems and technologies that have a high level of reliability to support the mission life and enable deployment for all required applications. They must be robust, resilient, fault tolerant, and durable to achieve fail-safe operation.



Fission Battery Assumptions

Independent Operation:

- No External Control Interface
- No Remote Operation Capabilities
- Power Output is Variable Based Only on Natural Means
- Closed and Secured Container

Remote Monitoring:

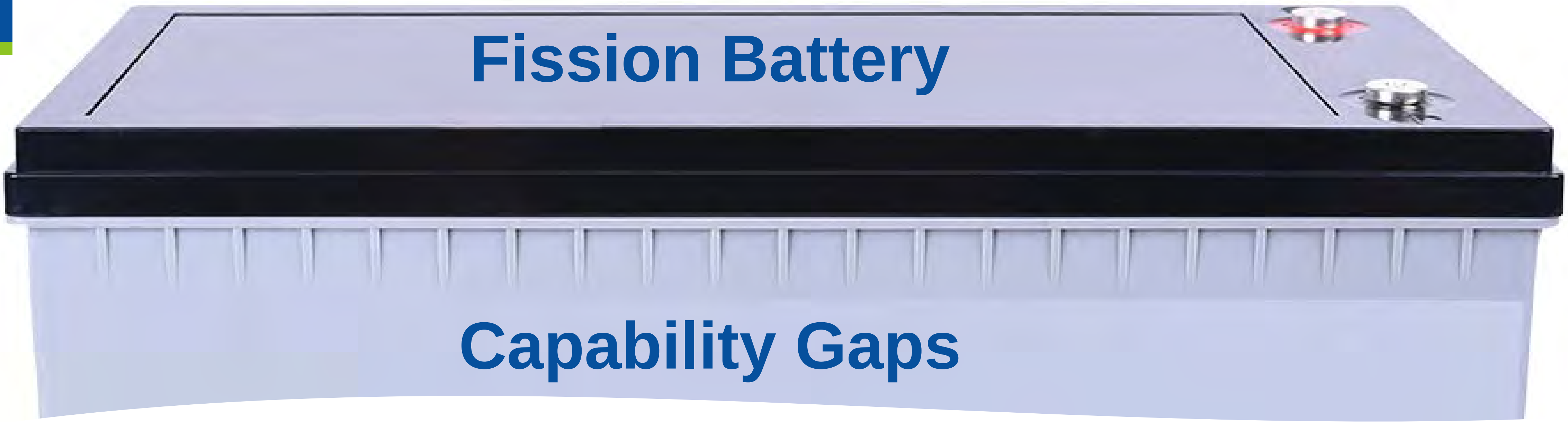
- Output Sensors
- Diagnostic Sensors
- Hazard Sensors

Fission Battery Cyber Considerations

- Internal Control Interface is Adequately Secured
- Remote Manipulation, Tuning is Disabled
- Refurbishment, Manipulation and Tuning are Factory-Only Functions
- Supply Chain is Cybersecured

Remote Monitoring and Diagnostics

- Must not include any remote-control ability
- Systems must be hardened against cyberattacks
- Monitoring of the logs of the one-way cyber appliance for awareness and response to any attempted intrusions
- All monitoring sensors must flow through a data diode or similar cybersecurity device to ensure no return traffic to the device could affect the battery operation in any way



Fission Battery

Capability Gaps

Battery System:

- More research needed to ensure a closed-loop control system can maintain required operational output
- Design of battery will determine if the level of control system complexity creates a further need for cybercontrols

Remote Monitoring and Diagnostics:

- More research is needed to ensure sensor data is a secure, one-way feed to allow for remote monitoring and diagnostics while preventing any operational impacts
- Data stream integrity research is needed to ensure false positives at the monitoring and diagnostics center do not hinder ongoing operations

INL
Idaho National Laboratory

Questions?