SAND2020-6804C

United States
Department of Energy
National Nuclear Security Administration
International Nuclear Security

INS
International Nuclear Security
Reducing Risk of Nuclear Terrorism

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.

INS International Nuclear Security
Reducing Risk of Nuclear Terrorism

National Nuclear Security Administration

Preliminary Results From Invoking Artificial Neural Networks To Measure Insider Threat Mitigation

Shannon N. Abbott[1], Adam D. Williams[1], William S. Charlton[2]

[1]*Sandia National Laboratories*, Albuquerque, NM, USA, [sabbott; adwilli]@sandia.gov*
[2]*Nuclear Engineering Teaching Laboratory, University of Texas, Austin, TX, USA [wccharlton@utexas.edu]*

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. SAND2020-

Background

- Traditional approaches to Insider Threat Detection & Mitigation(ITDM)
  - Focus on individual characteristics
    - Difficult to identity, almost impossible to measure/quantify
  - Based on “prevention” and “protection” concepts
    - Best practices, for example
  - Struggle to anticipate growing “insider threat potential”
    - Underlying “reactionary” paradigm

- A new approach, based on several observations:
  - People working in nuclear facilities settle into “operational rhythms”
  - These can be described with data/signals already being collected at nuclear facilities
  - Recast “preventive” & “protective” approaches as boundaries on these rhythms

Developing a new ITDM Monitoring Method

- Assumption:
  - Insider threat ***attempts*** represent a deviation from these “operational rhythms”
- Conclusion:
  - Humans are ***creatures of habit*** & ***unpredictable*** – can deviation from normal rhythms ID insiders?
  - Anomaly detection ***may*** identify the ***potential*** for an insider opportunity to manifest into action
  - ***Artificial neural networks*** (ANNs) can be trained to ID patterns/deviations in operational rhythms
- Hypothesis: ANNs can evaluate facility data signals to support ITDM
  - Unusual access times as monitored by access control points like badge readers
  - Attempts to access physical areas beyond current access level as monitored by access control points
  - Increased or routine alarms from personnel radiation portal monitors

Equipment Installation

- SNL worked with the Nuclear Engineering teaching Laboratory at the University of Texas at Austin to install and test the ReconaSense software at the research Reacor
  - Included:
    - Duplicate NETL access control server + ReconaSense software
    - Small mods to access control system controllers, servers, and communication hardware
    - Performance testing
  - Completed: November 2019

INS
International Nuclear Security
Reducing Risk of Nuclear Terrorism

National Nuclear Security Administration

Preliminary Results

- 90 days of data
  - 13653 access control data points
  - 694 intrusion sensor data points
- Data Analysis = General Trends
  - Single access point
  - Time-sequenced, multiple access points
  - Personnel type access

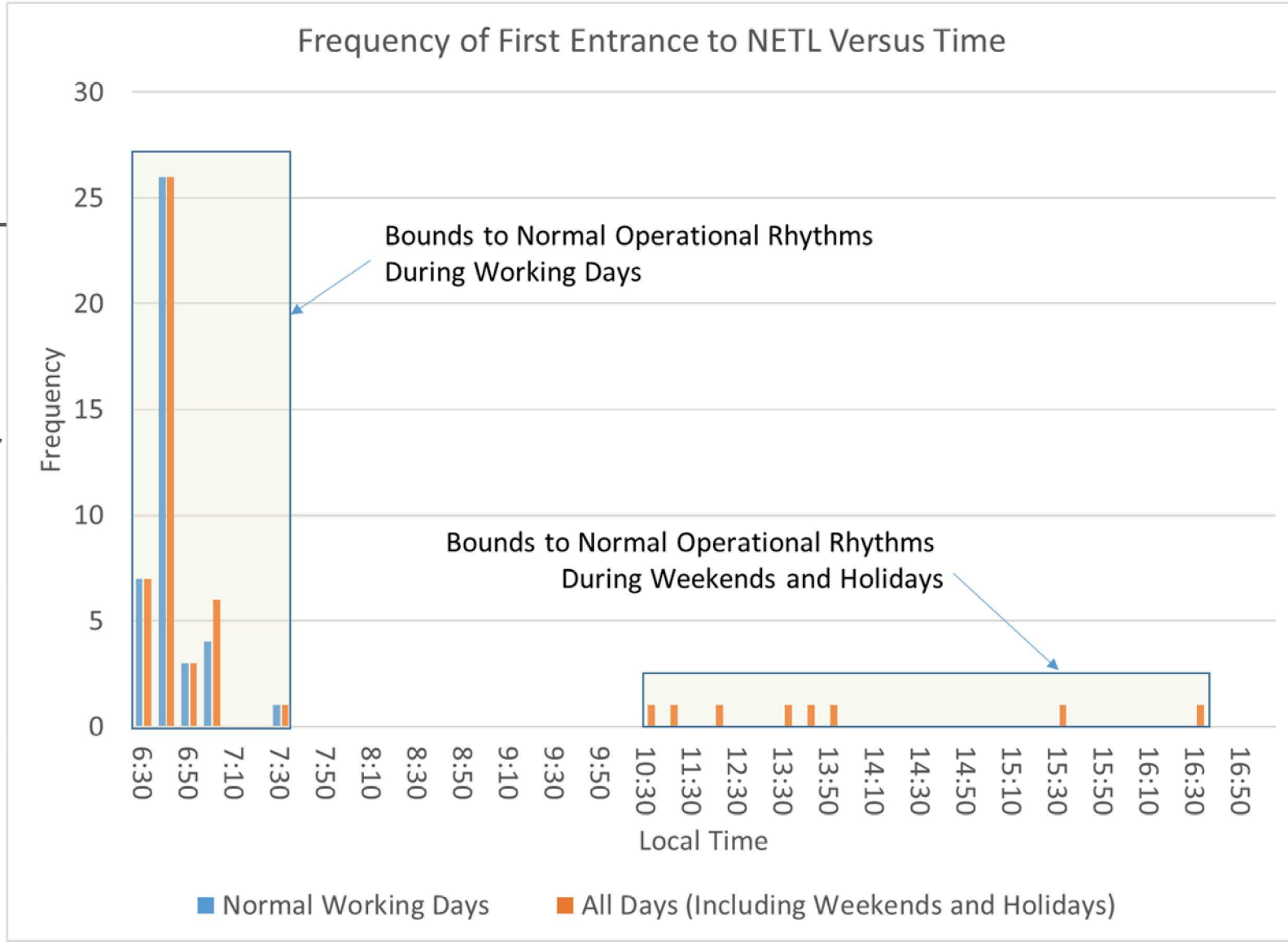
INS International Nuclear Security
Reducing Risk of Nuclear Terrorism

National Nuclear Security Administration

Preliminary Results

Single Access Point Analysis

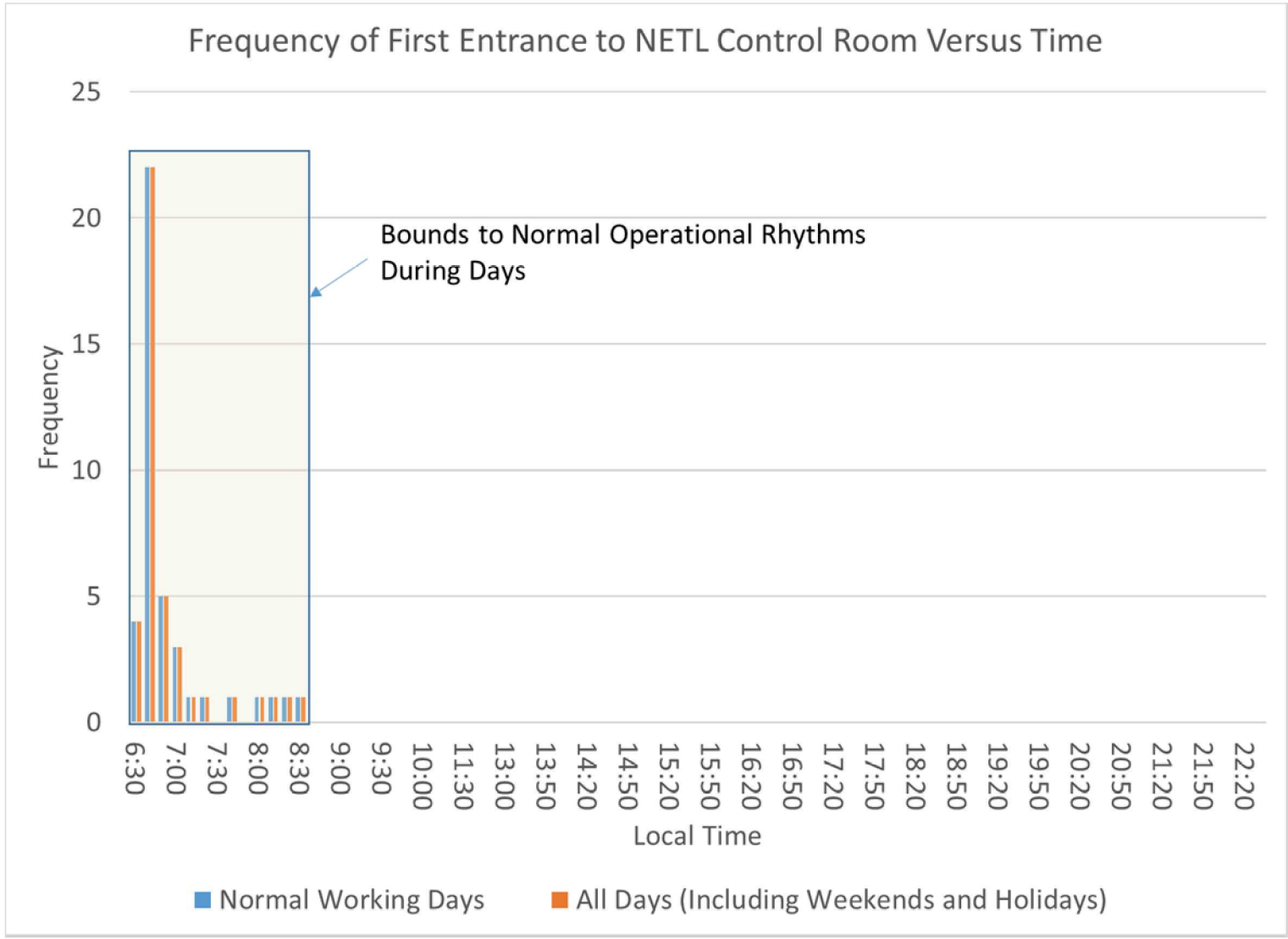
- Frequency distribution of the first allowed access to the NETL facility versus the time of access is
- Clear bounds on the normal time of first entry are evident for both weekdays & weekends
- ANN is capable of analyzing for deviations outside of these bounds
  - Example: First access to the NETL during normal working days is performed by the same two individuals in all but one instance



Preliminary Results

Time-sequenced, multiple access points Analysis

- Frequency distribution of the first allowed access to the NETL reactor control room versus the time of access
- Clear bounds on the normal time of first entry to the facility exist for working days & weekends
  - Same result! → NETL labs operate on weekends and holidays
- ANN is capable of analyzing for deviations in behavior outside of these bounds
  - Example: The first access to the NETL reactor control room during normal working days is performed by the same three individuals



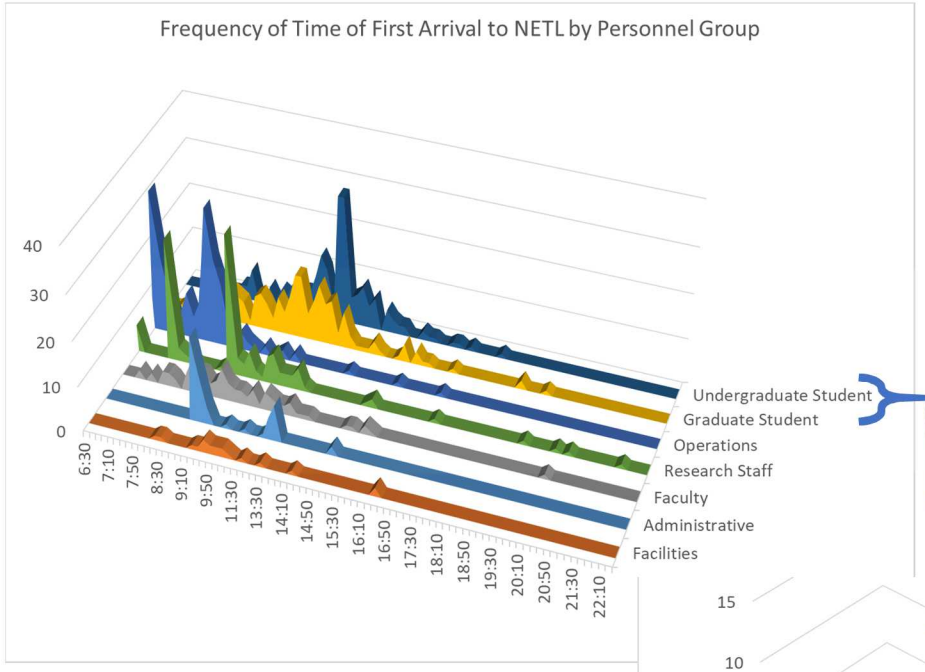
INS
International Nuclear Security
Reducing Risk of Nuclear Terrorism

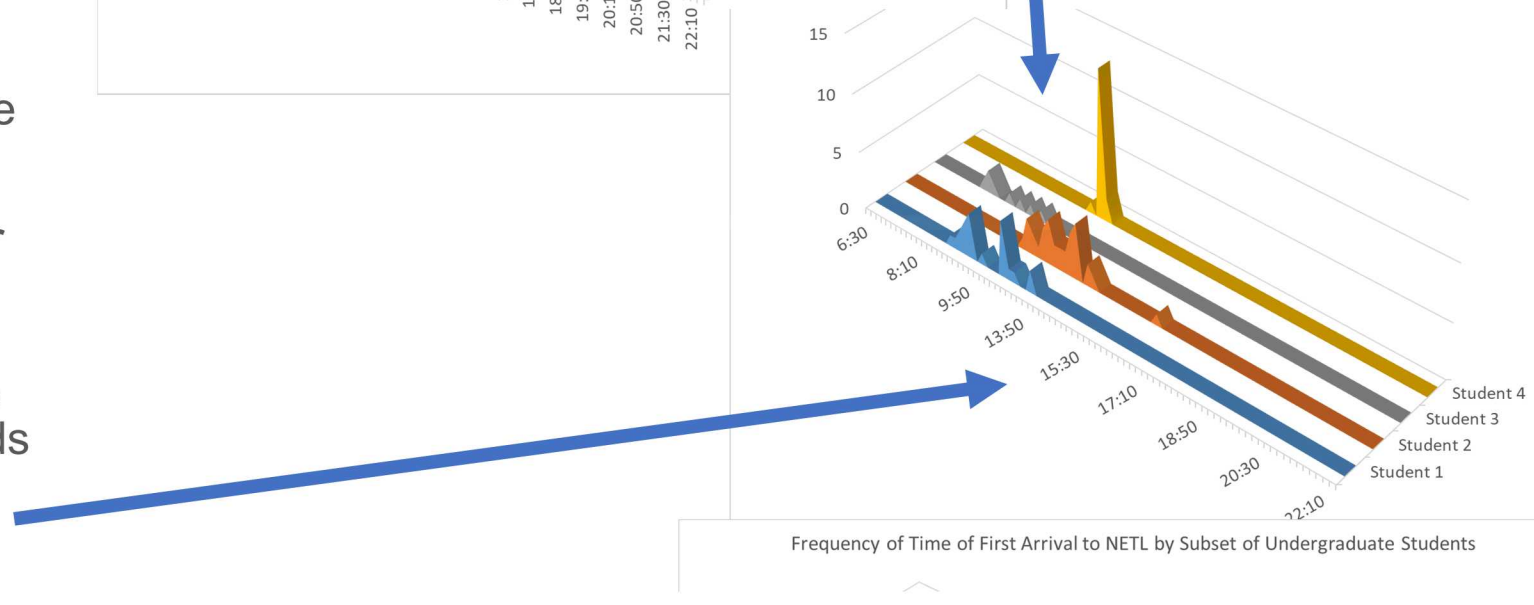
National Nuclear Security Administration

Preliminary Results

Personnel-Type Access Analysis

- Frequency distribution of the first allowed access to the NETL facility by ***personnel type*** versus the time of access is
- Clear bounds on the normal time of first entry → profiles per personnel type
  - Still large variation within each type
- ANN is capable of analyzing for deviations within each type
  - Despite a wide bound for undergraduate students (dark blue above) → ANN shots tighter bounds for individual students





Phase I Activities: Preliminary Results

#	Scenario Name	Test Description	Preliminary Results
1	Security Closet Access	Unauthorized Access Attempt	Detected and Access Denied In All Cases
		Authorized Access Credentials Used by Unauthorized Individual Who Entered Building Using Their Own Credentials	Detected and Access Denied In Most Cases
		Authorized Access Credentials Used by Unauthorized Individual Who Entered Building Using Authorized Individual's Credentials	Not Detected and Access Granted in All Cases
2	Reactor Bay Access	Unauthorized Access to Reactor Bay	Detected and Access Denied In All Cases
		Early Detection by Motion Sensor	Not Tested
3	Fuel Storage Surveillance	Insider Surveillance	Difficult to Detect Without Additional Sensing Input
		Insider Alarm Testing	Not Tested

- Conclusions:
  - Obvious patterns of life for most personnel
  - Established bounds for the facility operation rhythms
  - ***Even from the limited baseline data

- Therefore, ***potential detection*** of insider attempts through deviations from these bounds is ***feasible***

Phase I Activities: Implications

- Implications
  - Successful ReconaSense demo → Capability to define “operational rhythms”
  - ANNs identified patterns → Capability for patterns to help ITM
  - Successful Pilot Study → Capability for ANN-based, data-analytic ITM

- Recommended Next Analytical Steps
  - Training of ANNs for higher fidelity patterns (e.g., weekday vs. weekend)
  - Expand depth/randomness of evaluated scenarios
  - Incorporate additional data signals (e.g., camera data, radiation monitors)