# A New Framework to Minimize Insider Threats in Nuclear Power Operations


**Young-A Suh, Man-Sung Yim**

Nuclear Environment & Nuclear Security Lab, Department of Nuclear and Quantum Engineering, Korea Advanced Institute of Science and Technology
291 Daehak-ro, Yuseong-gu, Daejeon 305-701
dreameryounga@kaist.ac.kr / msyim@kaist.ac.kr

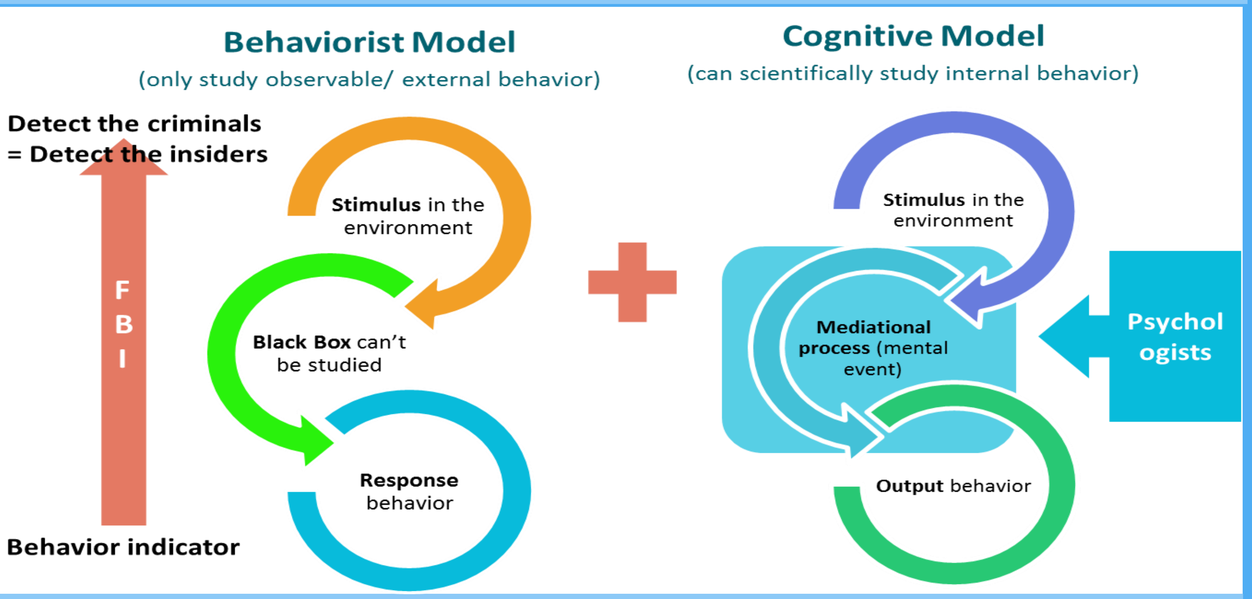

## Introduction

With the on-going global war on terror, the potential for a terrorist attack on a Nuclear Power Plant (NPP) is receiving a great deal of attention. The potential threat from an insider could lead to a grave outcome and deserves serious consideration.

### IAEA Preventive and Protective Measures for Insider Threats

- (1) Exclude access to potential insiders by identifying undesirable behavior or characteristics, which may indicate inappropriate motivation.
- (2) Remove from the premises individuals (potential insider) with undesirable behavior or characteristics after they have accessed the NPP.
- (3) Minimize opportunities for malicious acts by limiting access, authority and knowledge, by all available means.
- (4) Detect, delay and respond to malicious acts.
- (5) Mitigate or minimize the consequences resulting from malicious acts.

### Limitations: Existing Model for Insider Detection




### Objective of Research

- This study proposes a framework for detecting and predicting potential insiders.

## A New Framework to Minimize the Insider Threat

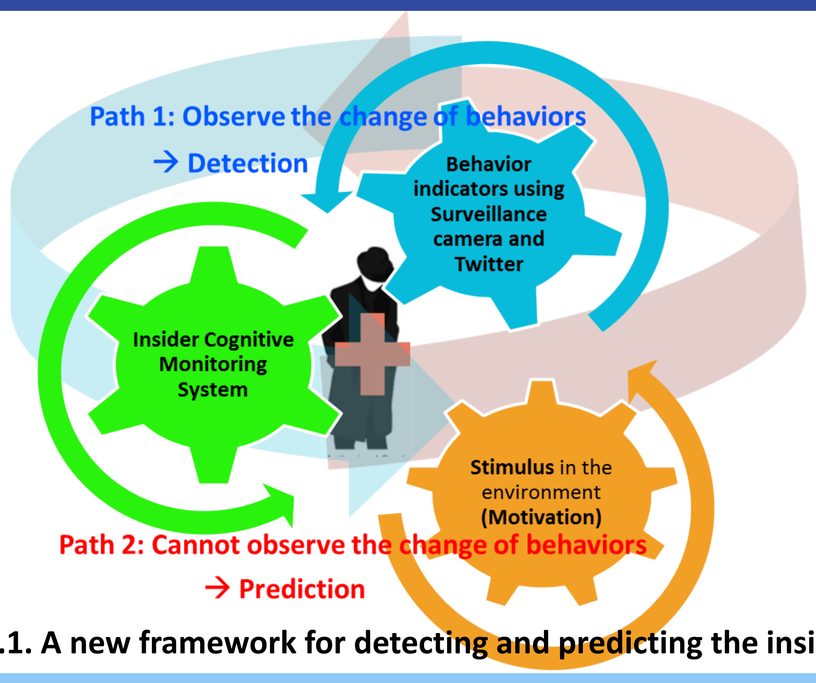
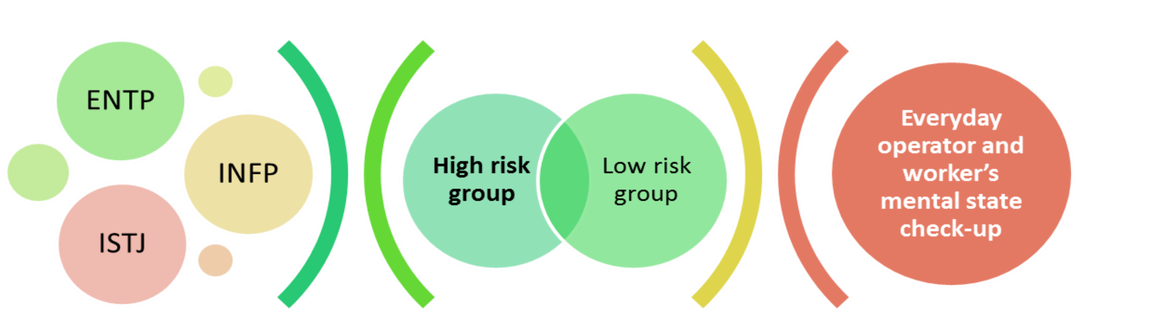



**Fig.1. A new framework for detecting and predicting the insider**

### Application of Framework to NPP Operators




**Introduction to Personality Screening System**

Using EEG test based on MBTI test for the purpose of hiring suitable employee

**Implement different style of training program**

Strengthen education for prevention of Insider threats

**Introduction to basic normal biodata collection system**

**Real-time worker's simple Biodata monitoring.**

Each day the operator's mental state should be checked to identify any abnormal bio-activity.

## Insider Prediction Monitoring Model

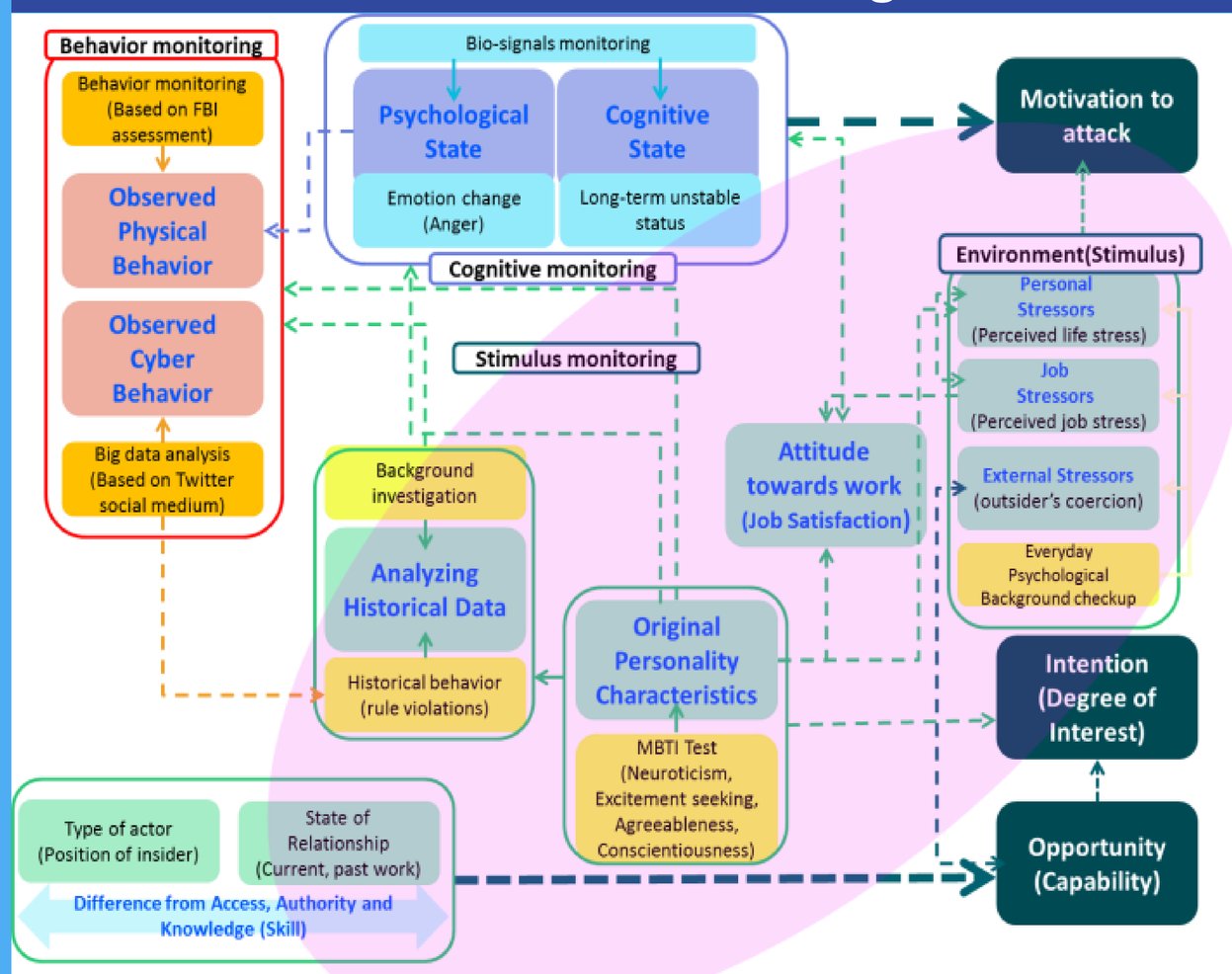



**Fig.2. Insider prediction monitoring model**

## Feasibility of the New Framework

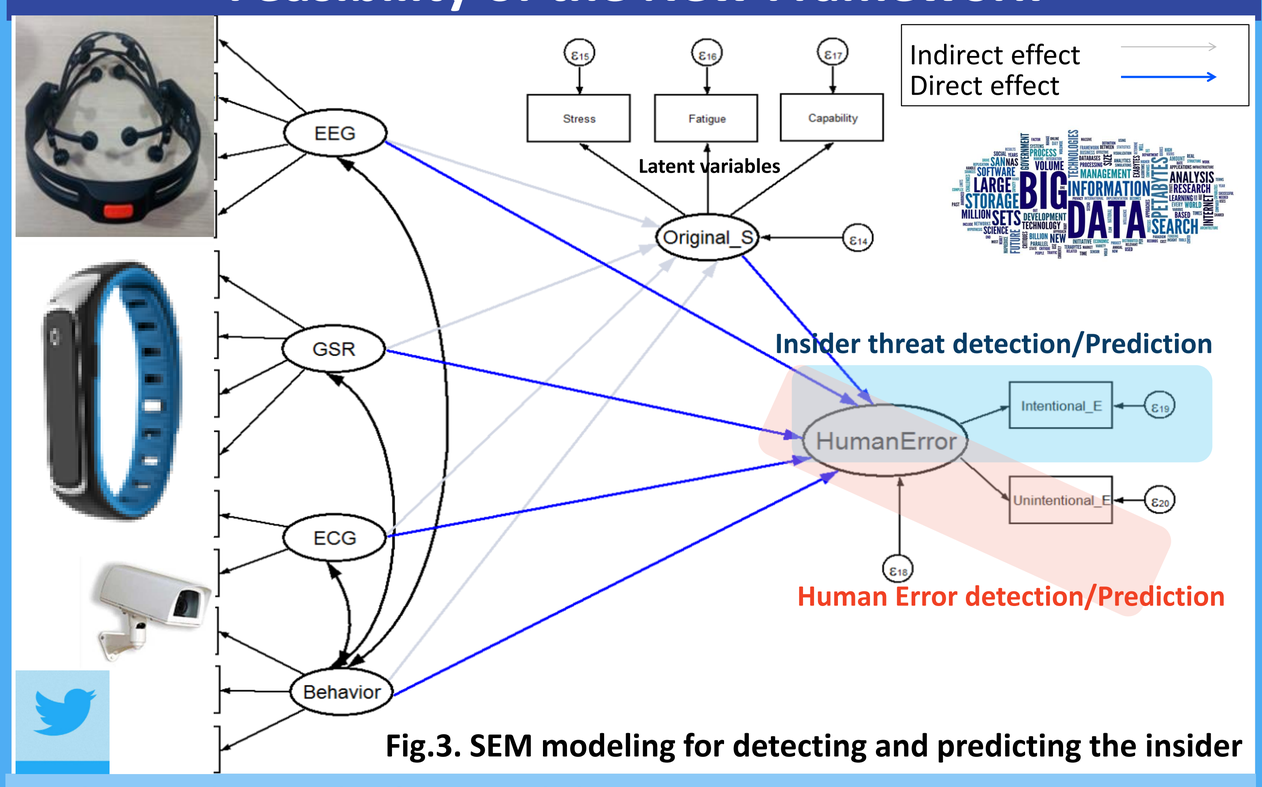
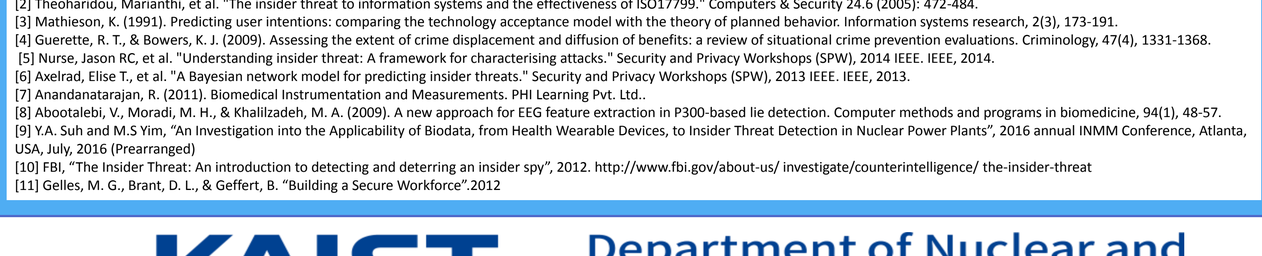



**Fig.3. SEM modeling for detecting and predicting the insider**

### Pilot Study Results for Feasibility on Cognitive Monitoring System




## Conclusion

- This paper suggests a new framework for predicting and detecting insider threats. This framework integrates not only behavioral indicators, but also stimulus monitoring and cognitive monitoring.
- This is particularly significant since recent developments and analysis in cognitive monitoring, based on human biodata, are shown to be quite reliable.
- The framework presented here opens the possibility of detecting and predicting an insider before a crime is actually committed. This model can be directly applied to reduce NPP security risks.

## References


[1] Guide, Implementing. "Preventive and Protective Measures against Insider Threats."
[2] Theoharidou, Marianthi, et al. "The insider threat to information systems and the effectiveness of ISO17799." Computers & Security 24.6 (2005): 472-484.
[3] Mathieson, K. (1991). Predicting user intentions: comparing the technology acceptance model with the theory of planned behavior. Information systems research, 2(3), 173-191.
[4] Guerette, R. T., & Bowers, K. J. (2009). Assessing the extent of crime displacement and diffusion of benefits: a review of situational crime prevention evaluations. Criminology, 47(4), 1331-1368.
[5] Nurse, Jason RC, et al. "Understanding insider threat: A framework for characterising attacks." Security and Privacy Workshops (SPW), 2014 IEEE. IEEE, 2014.
[6] Axelrad, Elise T., et al. "A Bayesian network model for predicting insider threats." Security and Privacy Workshops (SPW), 2013 IEEE. IEEE, 2013.
[7] Anandanatarajan, R. (2011). Biomedical Instrumentation and Measurements. PHI Learning Pvt. Ltd..
[8] Abootalebi, V., Moradi, M. H., & Khalilzadeh, M. A. (2009). A new approach for EEG feature extraction in P300-based lie detection. Computer methods and programs in biomedicine, 94(1), 48-57.
[9] Y.A. Suh and M.S Yim, "An Investigation into the Applicability of Biodata, from Health Wearable Devices, to Insider Threat Detection in Nuclear Power Plants", 2016 annual INMM Conference, Atlanta, USA, July, 2016 (Prearranged)
[10] FBI, "The Insider Threat: An introduction to detecting and deterring an insider spy", 2012. http://www.fbi.gov/about-us/ investigate/counterintelligence/ the-insider-threat
[11] Gelles, M. G., Brant, D. L., & Geffert, B. "Building a Secure Workforce".2012



NENS Nuclear Energy Environment and Nuclear Security Laboratory

KAIST Department of Nuclear and Quantum Engineering