Support for Reactor Operators in Case of Cyber-Security Threats

PI: C. Smidts, The Ohio State University

Program: Nuclear Energy

Collaborators: Q. Zhu- New York University; I. Ray – Colorado State University; T. McJunkin- Idaho National Laboratories; J. Hollern- Areva

ABSTRACT:

Our objective is to develop methods and a prototype tool to characterize abnormal nuclear power plant (NPP) events as "cyber" or "safety" incidents, and to further develop this tool as a real-time operator aid to assist in response to the incident. Increasing use of digital technology in NPPs poses cyber-security as a crucial threat to public safety and to continuous energy production. Cyber-security risks are comprised of complex known and unknown interactions between various entities, system vulnerabilities, network protocols, human users and malicious attacks. There is little understanding or research geared towards plant operators' response under cyber-security threats and operation procedures to cope with such threats. This is particularly critical when a cyber-security event masquerades as a safety incident or an evolving accident. Instead of leading operators to the remediation of the accident, the masked cyber event may lead them to circumvent the safety mechanisms of the plant. We will pursue three major milestones to address this threat: 1) **Event Classifier Prototype**: we will review available data and work with industry experts to develop indicators to help operators distinguish between cyber-security related events and safety related events, which will be integrated in a prototype tool the "Event Classifier"; 2) **Cyber Detection and Response Tool:** we will use the event classifier during the operation of the plant to suggest a cyber response based on attack classification and game theoretic principles. The cyber response will modify the operator and plant personnel procedural steps according to the threats perceived. The event classifier and cyber response algorithms will be integrated into the "Cyber Detection and Response" module; 3) **Experimental Validation:** we will validate the approaches and tools developed using a full scope NPP simulator environment. The state-of-the-art shows that no other methods or tools exist to achieve the stated objectives of this research. The research is critical, given the progressive and unchallengeable increase of digital technologies within current and future generations of power plants, the un-mistakable threat posed by cyber-security events and the misgivings, confusion and possibly erroneous actions operators can take endangering the safety goals. The methods and prototype tool developed will demonstrate the feasibility of this approach and provide a platform for adapting the tool for plant-specific cyber networks and digital control systems; be useable both as an on-line support and for training operators; and be easily adaptable to other plants and training simulators. Outside NPPs, the approach can support secure operations of other critical infrastructures (air traffic control, water systems, etc.). Our diverse team brings complementary strengths to this research: NYU, game theory; CSU, cyber security; INL, data fusion and displays; Areva, industry perspective; and OSU, risk assessment, human behavior and digital systems.