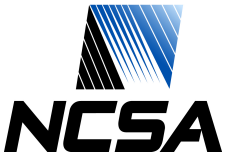
Big Control in the Industrial Internet

GE Global Research
Contact: Benjamin Beckmann
beckmann@ge.com

GE Global Research

Internet2
Contact: Christian Todorov
ctodorov@internet2.edu

National Center for Supercomputing Applications
Contact: Merle Giles
mgiles@illinois.edu



University of Virginia
Contact: Barry Horowitz
bh8e@virginia.edu

The Industrial Internet (II) connects equipment to advanced analytics through system platforms that support business process and value creation.

General Objective

One major category of II applications is wide-area control, or Big Control. Big Control applications monitor, predict, and decide how fleets of distributed assets are orchestrated to deliver reliable, resilient, and optimized performance. However, the needs and risks associated with of Big Control applications are broader than in traditional commercial applications.

Big Control applications need access to computational resources at varying scales and predictable network performance. Specifically, there is a pressing need to drive down costs and increase speed and capability by interconnecting data in three locations: edge, cloud, and high performance computing (HPC). Bridging these resources is key to allowing for optimal use of the best characteristics of each: 1) edge is fast and readily available, 2) cloud has scale and cost advantages, and 3) HPC addresses scale, complexity, and speed.

The II will usher in Big Control applications within and across industries that require high-levels of assurance. Assurance related to time, security, composablity and trust are required in each of the building blocks of Big Control. Additionally, continual operation (even under degraded conditions) will be hallmarks of Big Control applications. A significant requirement for achieving system cyber security will be resilience to cyber attacks, requiring the detection, isolation and characterization of attacks, as well as control capabilities to restore corrupted software controlled system functions. Attaining such capabilities will require sufficient system monitoring to enable derivation of responses to overcome disruptive cyber attacks.

Domain Specific Testbed – Transportation

Merging physical transportation with the power of the II will enable a revolution in the movement of people and assets. Based on a set of distributed assets (e.g. trains, trucks, ships, packages, machines), an II transportation testbed can connect nodes to enable complex transportation network experimentation for developing novel transportation systems. An II transportation testbed can provide the basis for a crash-to-care, emergency evacuation, or logistic optimization scenario. Benefits of such a demonstration testbed are 1) feasibility of high speed remote monitoring, diagnostic, and control, 2) enabling of efficient cost reduction and scalability of II transportation solutions, 3) system uptime reliability near 99.9% when required, and 4) resilience of real-time control, including responses to cyber attacks.

A focus on the II, and accompanying technologies and standards, will have broad industrial sector benefits and will drive wide ranging economic gains. The II will change how people work and how systems are controlled.