

TERMS OF REFERENCE FOR THE NITRD WORKSHOP “BEYOND SCADA: Networked Embedded Control Systems” 2006

Helen Gill (NSF), Marija Ilic (CMU), Bruce Krogh (CMU), Brad Martin (NSA), and
Shankar Sastry (UC Berkeley)

The nation’s critical physical infrastructure depends crucially on SCADA (Supervisory Control and Data Acquisition) and DCS (Digital Control Systems). Power networks, oil, gas, and water networks, chemical process control, transportation networks, the heating, ventilation and air conditioning systems of buildings depend critically on the sensing, monitoring, gathering, and control of information from distributed sensing devices. It is clear that these devices have been deployed in ad-hoc fashion in our infrastructures and are widely used in a number of different kinds of applications including economic load dispatch, security monitoring, regulation of climate and other such functions. As our use of ubiquitous computing and communication devices has increased, we have gradually built greater functionality into our SCADA/DCS systems. The by-product of these technological advances has been a lack of planned deployment of what we may refer to as high confidence devices and software. These are Devices and Networked Systems that are:

1. **Correct by construction** and which can be reprogrammed on the fly based on the functionality that is expected of them.
2. **Fault tolerant**, such that they are able to resist catastrophic failure under certain kinds of faults and mis-configurations and are able to reconfigure themselves to degrade gracefully under faulty conditions.
3. **Resistant to information attack**, such that they have defense-in-depth features which allow them to resist attack by determined hackers, hacktivists, and possibly even nation-states.

One way of understanding the prevalence of SCADA/DCS/PCS systems is to consider Figure 1 below of interdependencies of infrastructures due to Dr. M. Heller of NSF. Two critical infrastructures – “Electricity” and “Telecom” – shown at the left and right columns of the figure, are responsible for provisioning and controlling the potable and waste water infrastructure, oil and natural gas infrastructure, transportation, emergency response, government operations, and banking and finance infrastructures. While SCADA is explicitly called out only in the linkages to the Telecom infrastructure, it is clear that DCS and PCS are prevalent in the connections between the electricity infrastructure and the other infrastructures as well as for the control of the power infrastructure itself. SCADA/DCS systems represent an opportunity for distributed monitoring and control of physical systems using a distributed, embedded computing and communications paradigm: that is the research program of real-time network embedded systems. Additionally, it is critical that security be built in from the start to not leave the physical infrastructures vulnerable to information attack. Furthermore, since the physical infrastructures being controlled are required to work through attacks, it is important that

the systems be designed to work, in perhaps, a degraded mode of operation even when information attacks have been successful.

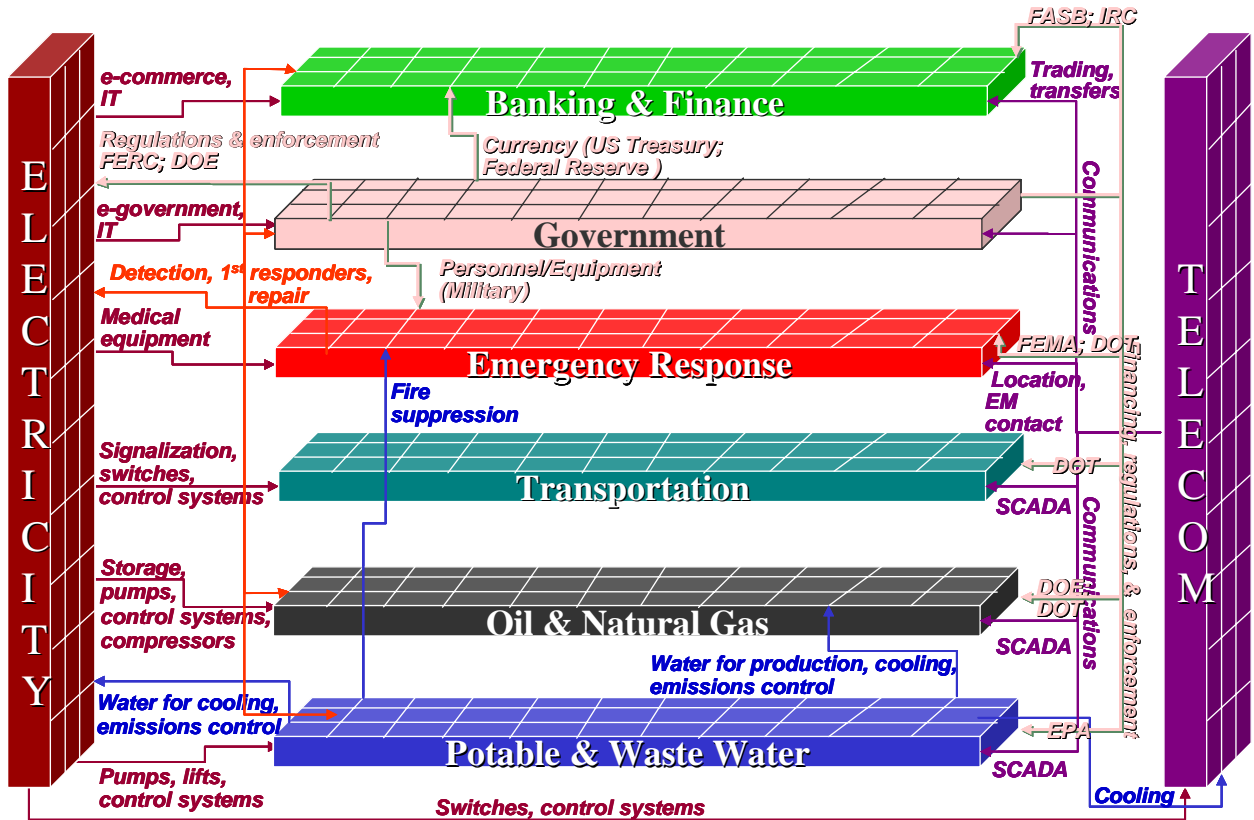


Figure 1: Showing the special role of the Electricity and Telecom Infrastructures in the control of other critical infrastructures. A key feature of this figure is the number of different feedback loops and interdependencies of distributed networked embedded systems.

The goals of the NITRD Workshop “Beyond SCADA/DCS Systems” is to begin with a survey of existing state of the art in SCADA/DCS systems along with a technology assessment of new technology directions in networked embedded systems, especially wireless networked embedded systems, develop a research agenda, and make recommendations for a research and development roadmap in industry (with stake holder input) in the following areas:

1. Evolution of SCADA/DCS into distributed, networked embedded control systems (i.e., integration of the new technologies of sensor webs, smart dust, MEMS actuators and sensors)
2. Meta Modeling and integration of domain specific models of physical infrastructures with SCADA/DCS systems

3. Closing the loop (i.e., distributed control over time varying wired and wireless networks of networked embedded systems)
4. High Confidence Co-design (i.e., building in correctness, fault tolerance and security into deployments of new generation SCADA/DCS systems)

Since the needs of different infrastructures are likely to be somewhat different, we will, for the sake of specificity, also work through the details of the evolution of SCADA/DCS systems for three infrastructure systems including:

1. Electric Power Generation and Distribution Systems
2. Chemical Process Control Systems
3. Building Management Systems

Workshop Format

We expect the workshop to have the following components:

1. First Day (Morning) – 3-5 plenary talks from industry, government, academia surveying the state of the art in SCADA systems, vulnerabilities, future directions of growth.
2. First Day (Afternoon) – Breakouts by the following areas:
 - a. Power and Energy Systems
 - b. Process Control
 - c. Building Management Systems

Charge to the breakout areas is to:

- a. Develop status reports about the state of SCADA in each sector
- d. Devise a road map for research
- b. Identify new technologies, show stoppers, hard problems, technological breakthroughs that are needed

The day ends with 20-minute outbriefs per area.

3. Second Day (Morning) – 3-5 plenary talks on the state of research, technology, and start ups
4. Second Day (Afternoon) – Breakouts by technology challenges including:
 - a. Networked Embedded Systems: hardware, real-time OS, real-time networking
 - b. Model Based Design of Networked Embedded Systems and Closing the loop on networked embedded systems
 - c. Privacy and Security

Charge to the breakout areas is to develop a research road map to address customer challenges of previous day followed by new directions of expansion. There are 20-minute outbriefs per area.

5. The workshop ends with a panel discussion by the six outbrief leaders.

Draft List of Invitees

Academia

Marissa Crow (Univ of Missouri Rolla) crow@umr.edu
Mladen Kezunovic (Texas A&M)
Vijay Vittal (ASU)
Felix Wu (UCB and HKU) ffwu@eecs.berkeley.edu
Kris Pister (UCB) pister@eecs.berkeley.edu
Jeannette Wing (CMU) wing@cs.cmu.edu
William H Sanders whs@crhc.uiuc.edu
Pete Sauer sauer@ece.uiuc.edu
Ken Birman (Cornell) birman@cs.cornell.edu
Robert Thomas (Cornell) rjt1@cornell.edu
Janos Sztipanovits (Vanderbilt) janos.sztipanovits@vanderbilt.edu
Jack Stankovic stankovic@cs.virginia.edu
George Cybenko (Dartmouth) gvc@dartmouth.edu
Massoud Amin mamin@minnesota.edu
Anthony Joseph (UC Berkeley) adj@eecs.berkeley.edu
Panos Antsaklis antsaklis1@nd.edu

Non profits and FFRDCs

Patrick Lincoln (SRI) lincoln@csl.sri.com
Ulf Lindqvist (SRI) ulf@csl.sri.com
Terry Benzel (ISI) tebnzel@isi.usc.edu
The I3P (David Kotz?)
Mitre (who?)
Sami Saydjari (Cyber Defense Agency) Ssaydjari@CyberDefenseAgency.com
Sandia Labs (Sam Varnado?)

Industry

Tariq Samad (Honeywell) tariq.samad@honeywell.com
Clas Jacobsen (United Technologies) JacobsCA@utrc.utc.com
Kyle Nelson (Adventium Labs) Kyle.nelson@adventiumlabs.org
Bonnie Bennet (Adventium Labs) Bonnie.Bennet@adventiumlabs.org
Feng Zhao (Microsoft) zhao@microsoft.com
Don Paul (Chevron) dlpaul@chevron.com (zeeg@chevron.com)
Victoria Stavridou (Intel) victoria.stavridou-coleman@intel.com
Rick Mc Geer (HP) rick.mcgeer@hp.com
Teresa Lunt (PARC) teresa.lunt@parc.com
Tim Johnson (GE)
David Corman (Boeing, St. Louis) david.e.corman@boeing.com

Don Wilson (Raytheon)
Prasanta Bose (Lockheed Martin Co) (prasanta.bose@lmco.com)

Government

Helen Gill (NSF) hgill@nsf.gov
Douglas Maughan (DHS) dmaughan@dhs.gov
Brad Martin(NSA) wbmart@tarius.tycho.ncsc.mil
Sally Howe (NCO/ NITRD) howe@nitrd.gov
Frankie King (NCO/ NITRD) king@nitrd.gov
Henry Kenchington (DOE) henry.kenchington@hq.doe.gov
William Parks (DOE) William.parks@hq.doe.gov
Paul Domich (NIST/DHS) paul.domich@nist.gov and paul.domich@dhs.gov
Kevin Tomsovic (NSF) kevin.tomosovic@nsf.gov
Al Wavering (NIST) albert.wavering@nist.gov
Peter Miller (DHS) peter.miller@dhs.gov
William Spees (FDA) wss@cdrh.fda.gov
Robert Gold (OSD) robert.gold@osd.mil
Paul E. Black (NIST) paul.black@nist.gov