

***IEEE Industrial Electronics  
Society (IES)  
Resilience and Security for  
Industrial Applications (ReSia)***

**Formation Discussion  
Proposed Technical Committee**

August 2011

# Agenda

- **Define the unique problem space to holistically integrate resilience in next generation industrial computing and control designs**
  - A Problem Statement: Adaptation to Highly Nonlinear, Oft Ill-defined Disturbances in security, human integration, complex interdependency
  - Current techniques to respond to highly nonlinear, oft ill-defined disturbances are inadequate with respect to security, human integration, and complex interdependency. This committee provides a forum for technical discussions related to:
- **Define a strategy and business case for government and industry to invest in promising research**
  - A Mechanism to Measure: Real World Resilience Metrics
- **Plan for special sessions and publications, including industrial research, in IES and other conferences**
  - Establishing Technological Benefit: Research and report on areas of critical needs both in definition and technology results.
- **Define a path for coining standards that establish a framework for use by government and industry**
  - Codifying Demonstrable Results: Developing the nomenclature, definition and framework.
- **Define the membership list and committee operations**
  - Codifying Contributors and Committee Process: Confirm a charter, operations manual and membership representing government, academia and industry, including IES participation

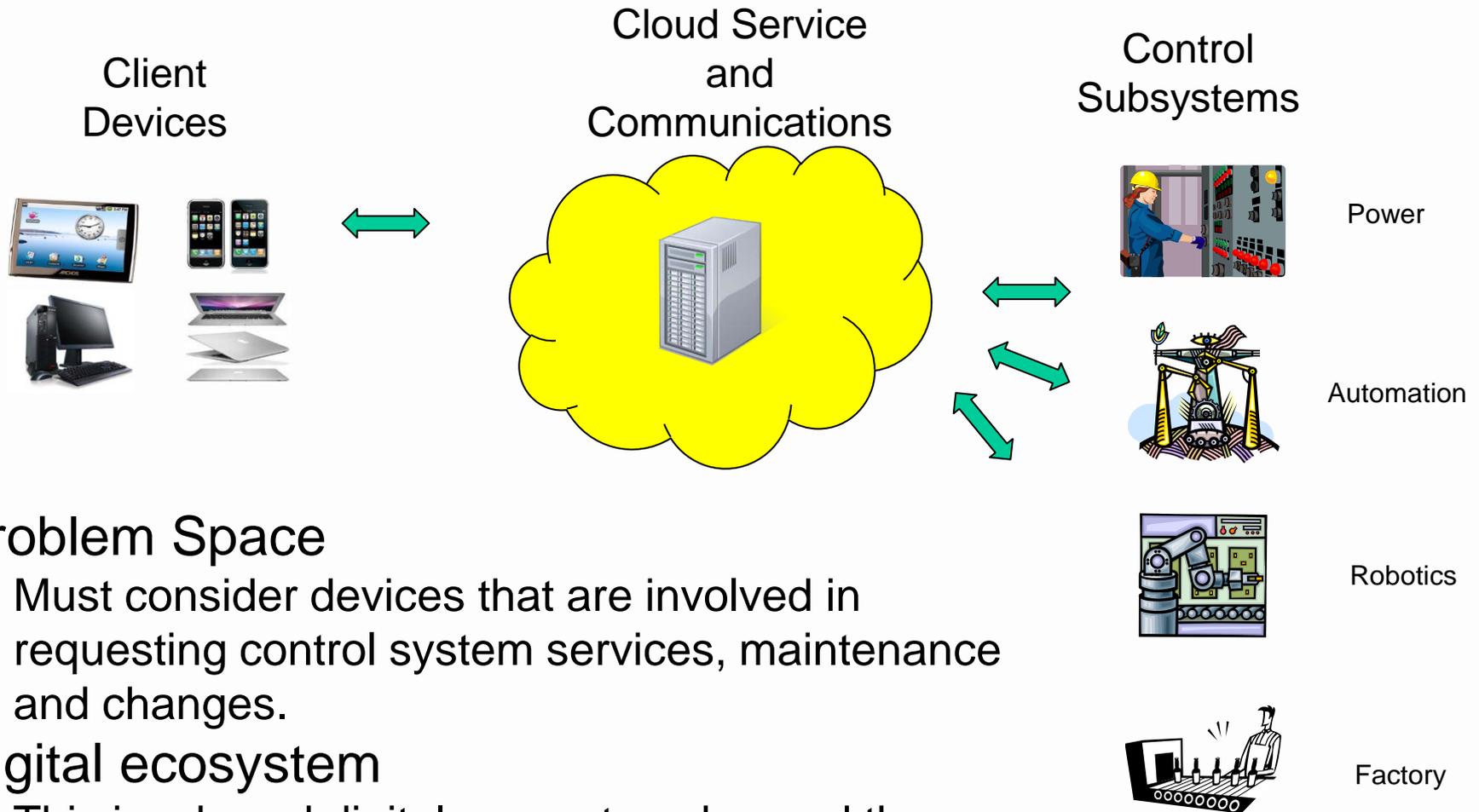
## ***Mission Statement***

- **Define the unique problem space and success criteria to holistically integrate resilience in next generation industrial computing and control design, implementation and operation throughout the lifecycle.**
- **Create a forum for discussion of ideas as they relate to resilience and security.**
- **Promote a strategy and business case to establish a structure and framework for investment by government and industry in promising research and the implementation of resilience into critical applications.**
- **Develop Resilience Metrics- including human systems, cyber security, and impacts of interdependencies on control systems.**
- **Foster a community of research scientists and engineers with the common goal of solving security and resilience problems.**
- **Identify a path for coining standards that establish a framework for use by government and industry**

## ***Introductions: ReSia Technical Committee***

- Name, Organization and Interests for those in attendance
  - Milos Manic, Professor, University of Idaho
  - Michael Condry, Senior Security Technologist, Intel
    - Milos and Michael co-chair the ReSia Technical Committee
  - Craig Rieger, Idaho National Laboratory, Secretary

## Define the unique problem space



### Problem Space

- Must consider devices that are involved in requesting control system services, maintenance and changes.

### Digital ecosystem

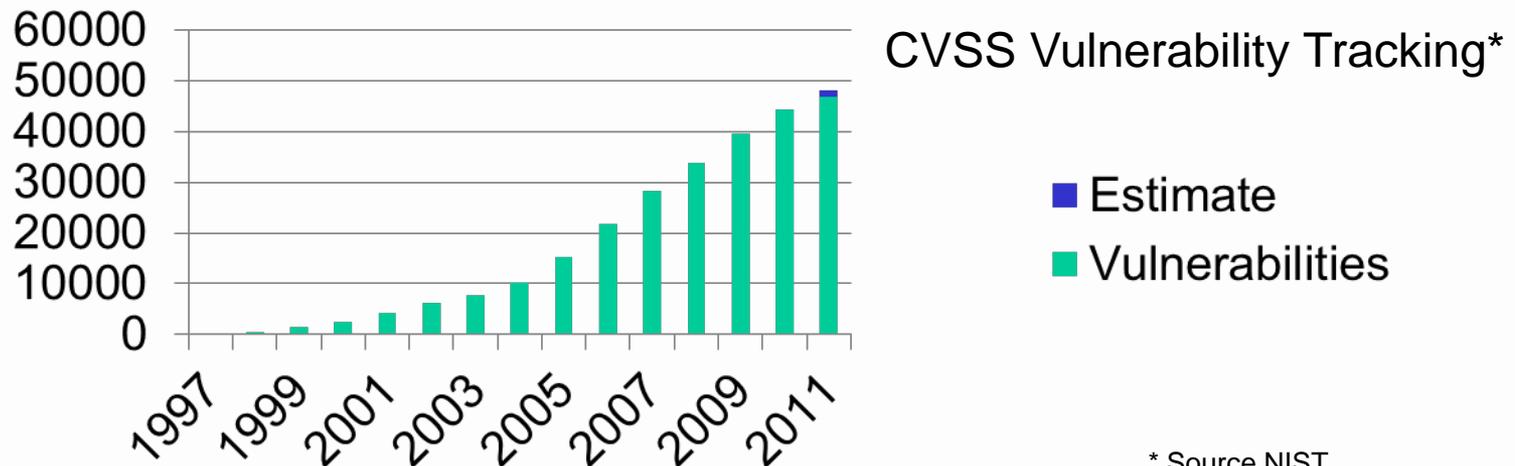
- This is a broad digital ecosystem, beyond the scope of control PLCs.

## *Scope of Resilience and Security Issues*

- Elements of the digital ecosystem that can impact resilience and security
  - It is assumed that solutions will need to be customized based on context in diverse environments/industries.
- Known generic methods for addressing resilience and security areas, including
  - Self-healing, dynamic reactive response to failures and attacks
  - Adapting to highly non-linear disturbances, often in presence of uncertainties, systems thinking, behavior (un)learning
  - Demand-response and predictive optimization
  - Detection & prevention of malware, recovery, patching and upgrading
  - Securing media, data, assets, identity protection, fraud deterrence
- Coverage of BKM in these areas needs to be evaluated
- Evaluation of implementations
  - Many solutions for a problem area (some w/ lower vulnerabilities, less exposures...)
- Tracking
  - CVSS is not enough for Control systems

## Define a strategy and business case

- Resiliency across the computational ecosystem is a major issue with many elements “out of control”
- Recent McAfee study showed multiple attacks to American sites and our allies, only one of many
- Verizon study shows cloud exposures growing
- CVSS only tracks software and it grows 5K/year.



\* Source NIST

## *Plan for special sessions and publications*

- Special Sessions
  - ISIE 2012 and IECON 2012
  - Scope Problem and Solution Techniques
  - Research Oriented
- Industry Forum
  - A “form” of special session for Industry Speakers
  - Focus on problem space and product directions
- Publications
  - Transactions on Industrial Electronics
  - Transactions on Industrial Informatics
  - Industrial Electronics Magazine
  - Conference Proceedings

## ***Define a path for coining standards***

- Consider all elements of the security profile and all devices that can be used to access control systems
- SCADA has multiple recent exposures
- Separate generic solution strategies and find a measurement system the allows this to scope coverage
- Define a criteria for evaluation of vulnerabilities, implementations must be graded by their exposures
- Define security metrics that narrow the issue to what affects resilience.
- Provide metrics that add value

## ***Define membership list & committee operations***

- Meet at least one, sometimes twice a year. Once at ISRCS and one meeting at a major conference.
- Conference call as needed.
- Split tasks that chairs and secretary will follow up with committee members.
- We need to define problem space and grow with strategic members that will be involved.
- Provide special session to major conference such as IECON.
- Understand what can be submitted to IES as recordable committee activities.

***Path Forward and Final Comments***