



**Strategic vision in certifiable software:  
Cross-domain commonalities**

Sushil Birla

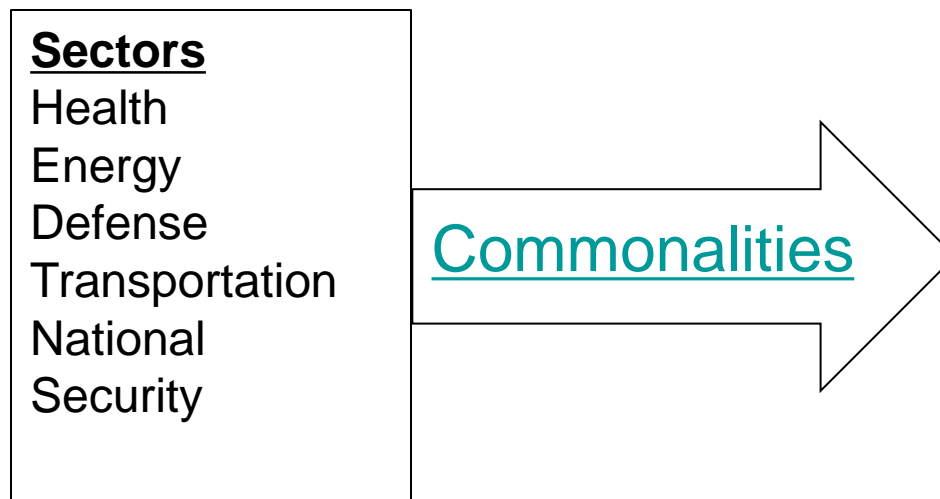
Software Certification Consortium - 7<sup>th</sup> Meeting – May 1-2, 2011

## Background & source of vision


Context: U.S. Govt. Inter-agency coordination activities

- NITRD (Networking & IT R&D)
  - HCSS (High Confidence Software & Systems)
    - Cyber-physical systems
      - » Today's focus: Safety critical systems

Initiators: NITRD/HCSS co-chairs Helen Gill, Brad Martin, Al Wavering



## Current state – some commonalities

- Safety-critical CPSs are typically too **complex** to be completely verified and validated. Remaining uncertainties are significant, but not well understood. 
- Safety analysis and evaluation require high competence and judgment, but these capabilities are very scarce.
- Cyber adversaries' ability to develop and launch new attack tools and techniques outpaces the ability to develop and deploy countermeasures.
- The competence ↔ complexity gap is widening rapidly.
- Similar problems exist in most safety-critical, mission-critical application domains, but there is little synergy to find a common core set of underlying solution capabilities.
- The requisite knowledge is not well-systematized
- Commercially available tools, driven by non-critical consumer applications, are being used in critical applications, but their commensurate verification is not feasible economically.

## **Current state: Some complexity issues**

- A single defect can make logic wrong, potentially leading to serious consequences, but the capability to engineer defect-free systems does not exist.
- Networking (wired or wireless) introduces new vulnerabilities that are not well understood
  - Hidden dependencies and couplings
- Latent defects could combine in many scenarios
- Latent defects could cause a high consequence failure
- The more complex a system the more exposure to defects
- Verification of a high-integrity system or component, e.g. operating system, takes more effort and time than its initial development.



## **Vision state: Some commonalities**

- Systems can be routinely developed with built-in assurance of safety and security
  - “Do it right the first time” becomes the cheapest and fastest way to realize a system
- Accredited third party services are commercially available for verification & validation (V&V)
- Accredited third party services are commercially available for review, attestation, and certification
- Requisite tools are certified
- Requisite competence (knowledge, skills) is certified
- Requisite competence becomes readily available
- Requisite body of knowledge is mature and readily accessible
- Educational and training institutions have mature curricula to produce and certify the requisite competence

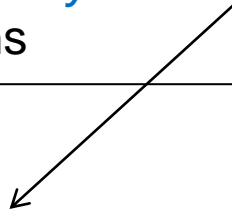


# Some definitions

# ISO 17000 definitions - 1

## 5.5 certification

*Third-party attestation* related to products, processes, systems or persons



## 5.2 attestation

Issue of a statement, based on a decision following *review*, that fulfillment of *specified requirements* has been demonstrated

## 5.1 review



Verification of the suitability, adequacy and effectiveness of selection and determination activities, and the results of these activities, with regard to fulfillment of *specified requirements* by an object of *conformity assessment*



# ISO 17000 definitions - 2

## 3.1 *specified requirement*

Need or expectation that is stated. NOTE: Specified requirements may be stated in normative documents such as regulations....

## 2.1 *conformity assessment*

Demonstration that specified requirements relating to a product, process, system, person or body are fulfilled

## 2.4 *third party*

A person or body that is independent of the person or organization that **provides** the object, and of **user interests** in that object



# ISO 17000 definitions - 3

## *2.5 conformity assessment body*

Body that performs conformity assessment services

## *5.6 accreditation*

Third-party attestation related to a *conformity assessment body* conveying formal demonstration of its competence to carry out specific conformity assessment tasks

## *2.6 accreditation body*

Authoritative body that performs accreditation  
NOTE ... authority ... generally derived from government

# Some **expectations** & **gaps**

