

# Session 11B: Information Assurance - Summary



Moderators: Joe Betser and Charlie Lavine, The Aerospace Corporation

- ◆ *Harmonizing the Certification and Accreditation Process With Modern Security Evaluation Standards*  
Stuart Schaeffer, The Aerospace Corporation
- ◆ *Hydra: Agents for Information Security*  
Morris Brill, TRW Systems
- ◆ *Ground Systems and the Challenge of Creating Collaborating I-A Communities via the Internet Research and Standards*  
Joe Betser, The Aerospace Corporation
- ◆ *Securing Ground Control Systems*  
Tracy Dorsey, Computer Sciences Corporation
- ◆ *Virtual Vulnerability Assessment for Spacecraft Ground Systems*  
Hoh Peter In and Steve Liu, Texas A&M University

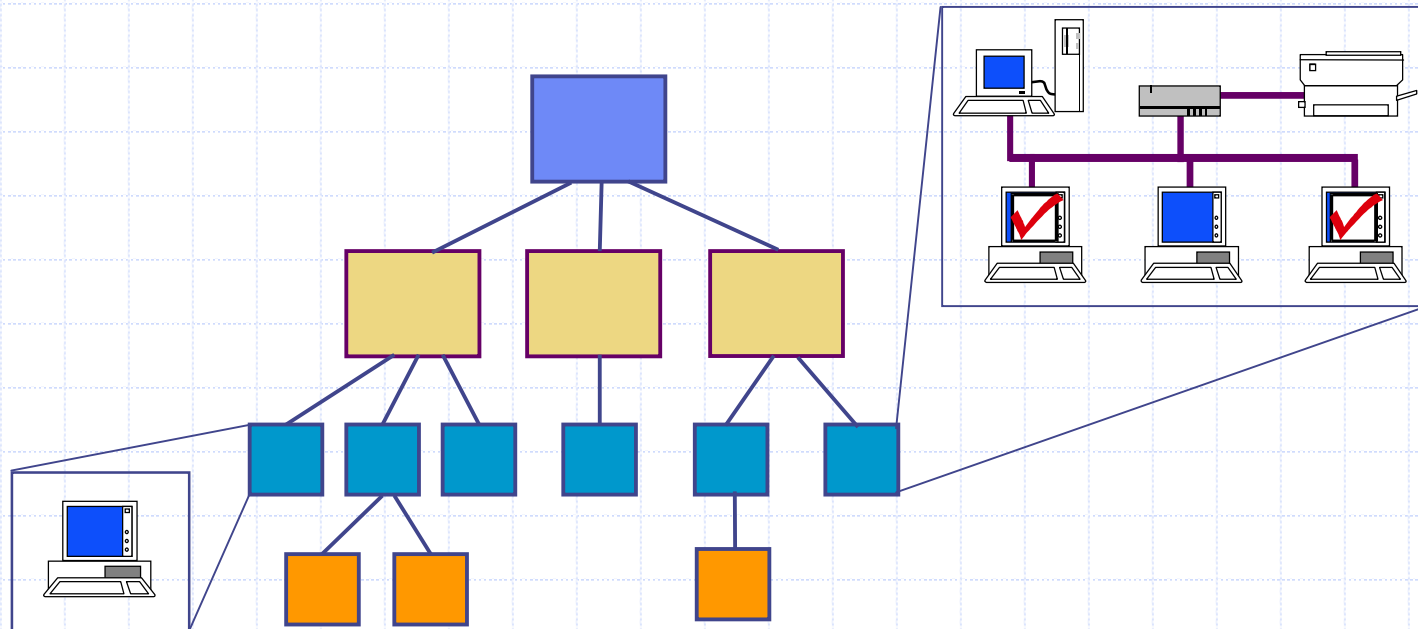
# Information Assurance

## –Challenges and Way Forward

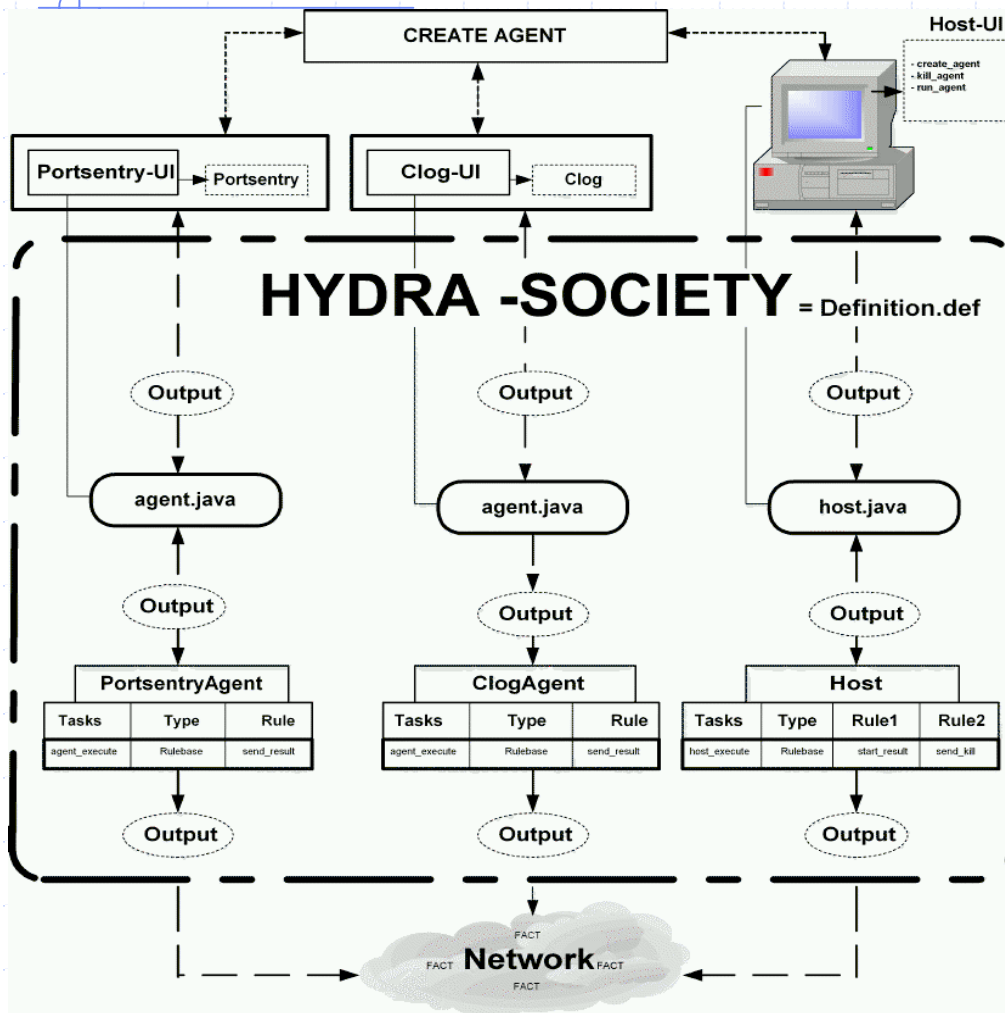
- ◆ *Multi-discipline, multi-community challenge*
- ◆ *Increased vulnerability due to increasing connectivity and COTS usage*
- ◆ *Intrusion Detection systems consisting of many sensors and correlators*
- ◆ *Difficult IETF standardization to decompose intrusion detection*
- ◆ *Tall order to get multiple communities to collaborate*
- ◆ *Common Criteria deployment difficult for complex systems*
  
- ◆ ***Collaborate among multi disciplines and multi communities***
- ◆ ***Employ software, system, and assurance engineering to reduce vulnerabilities***
- ◆ ***Research to gain understanding and to develop new approaches***
- ◆ ***Include human systems integration within information assurance***
- ◆ ***Develop standards and Interoperability – key to decomposition***
- ◆ ***Improve network protocols and crypto/key management***
- ◆ ***Design information assurance into systems upfront!***

# Proposed Methodology

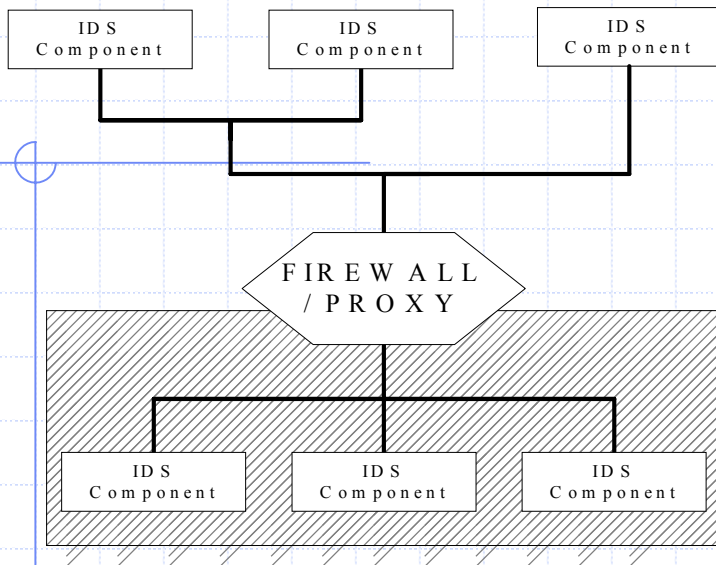
- ◆ Decompose System Requirements into Subsystem Requirements Recursively to Product Level
  - Provides path for recomposition of system from component products



# Hydra Architecture is Distributed and Extensible



- Agents act as wrappers for IDS tools
- Agents collect, format and forward data to host agent
- IDS data is evaluated for significant events using AI methods
- Agents respond intelligently by starting defensive or offensive agents
- ZEUS provides the infrastructure
- Each agent makes decisions about its environment and tasks



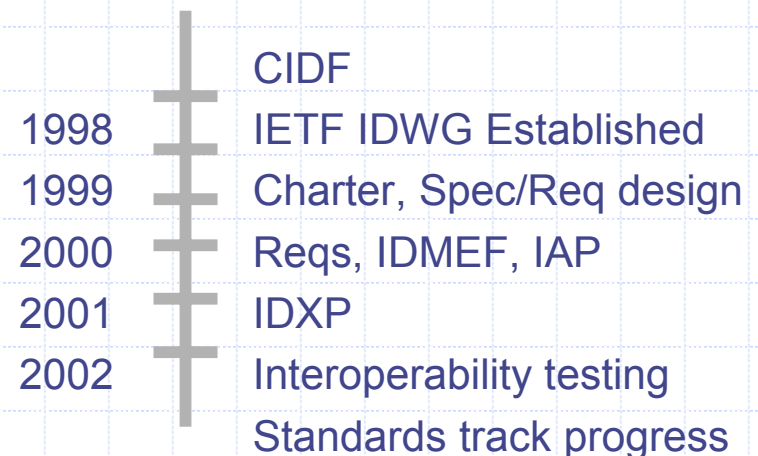
## Innovation

- The first attempt at globally interoperable IDS protocols
- Incorporation of input from numerous stakeholder communities including: Research, Commercial, Academic, Government, and International

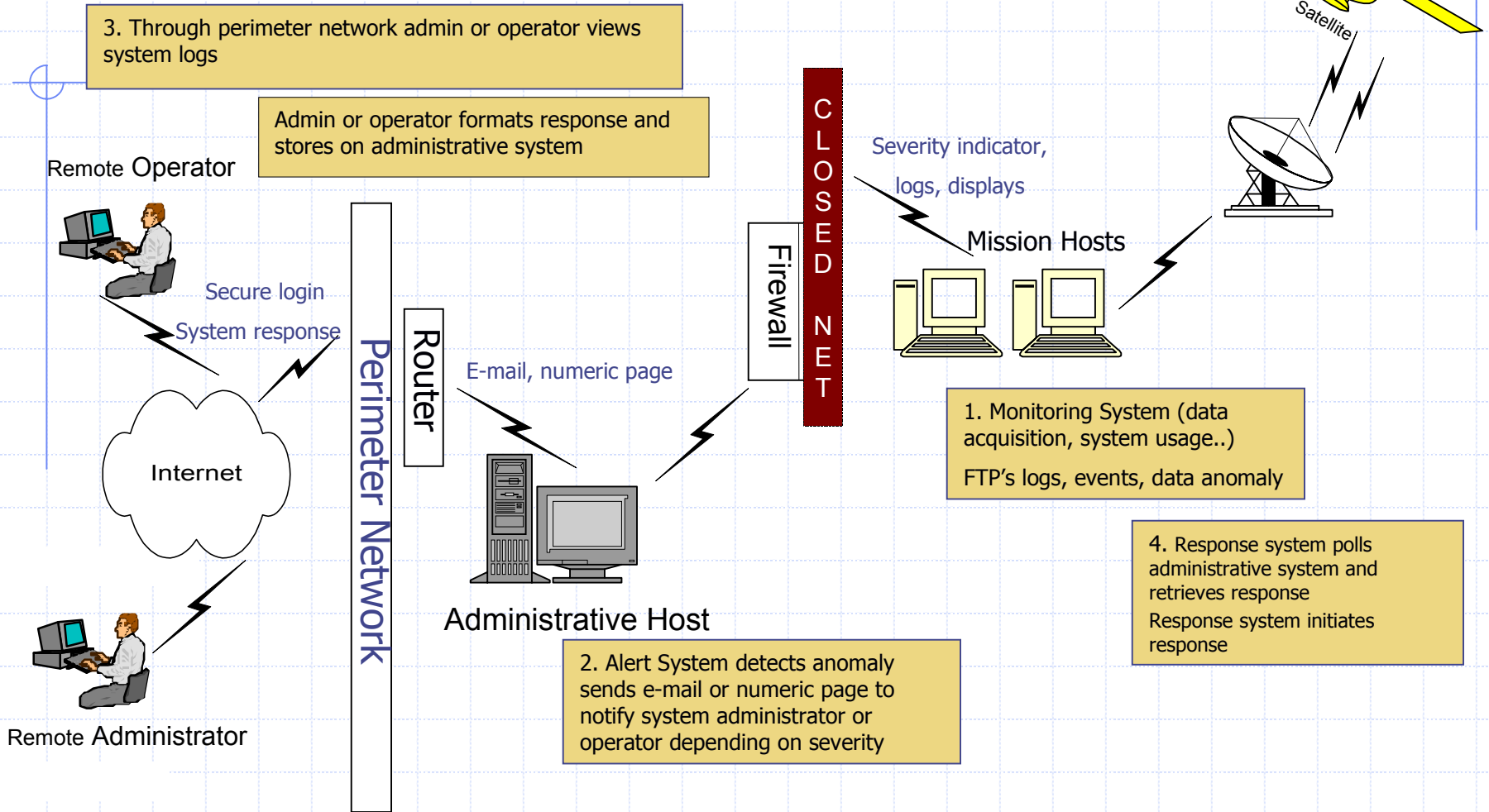
## Impact

- Create **global** Internet IDS protocols and data structures to enable IDS component communication in **global** enterprises
- IETF: Ubiquitous **global** dissemination of usage & interoperability -- a condition for advancement in standards track
- “Rough Consensus and Running Code”

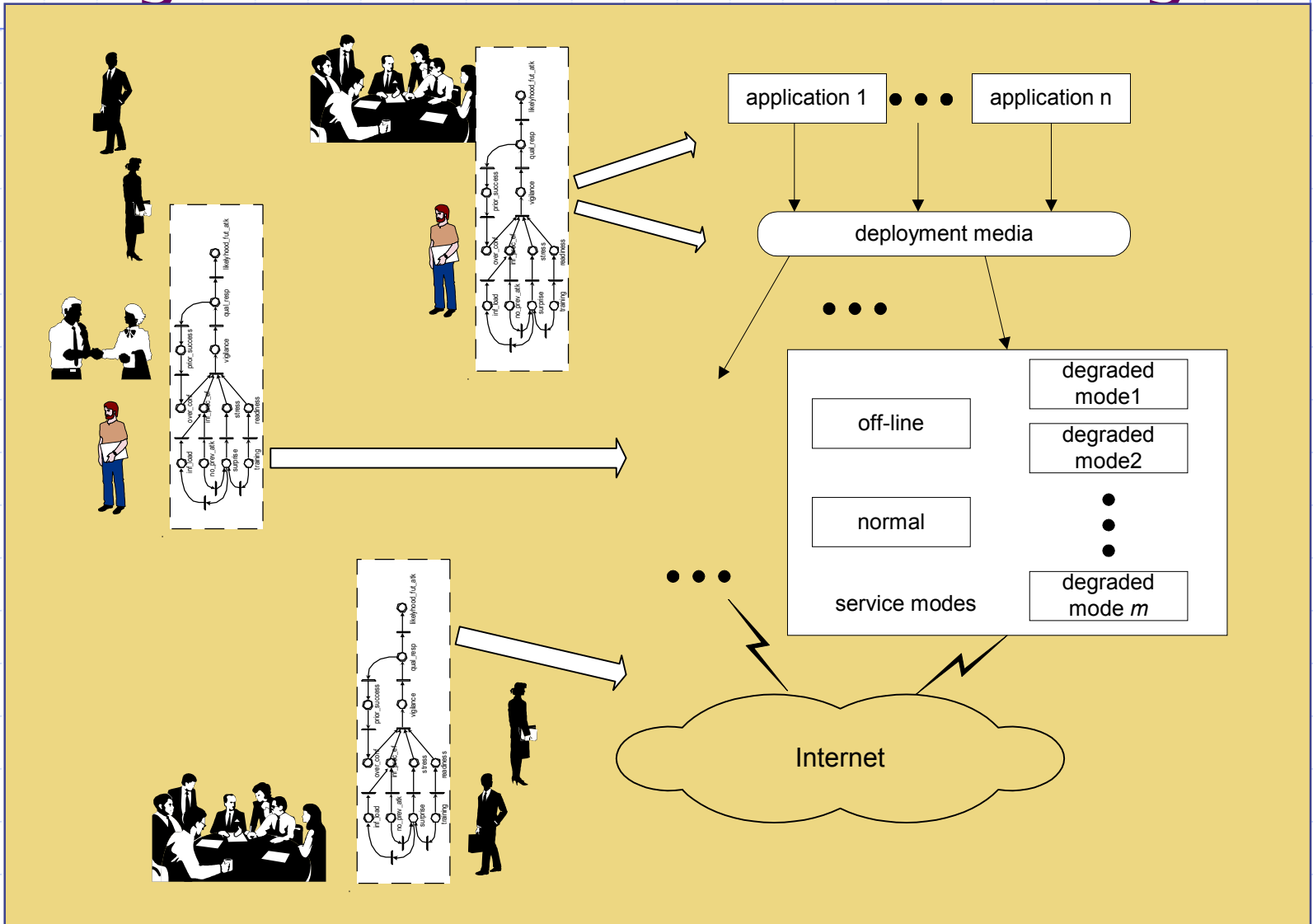
## Schedule



# How it works



# Integrated Man-Machine Modeling



# Information Assurance

## –Challenges and Way Forward

- ◆ *Multi-discipline, multi-community challenge*
- ◆ *Increased vulnerability due to increasing connectivity and COTS usage*
- ◆ *Intrusion Detection systems consisting of many sensors and correlators*
- ◆ *Difficult IETF standardization to decompose intrusion detection*
- ◆ *Tall order to get multiple communities to collaborate*
- ◆ *Common Criteria deployment difficult for complex systems*
  
- ◆ ***Collaborate among multi disciplines and multi communities***
- ◆ ***Employ software, system, and assurance engineering to reduce vulnerabilities***
- ◆ ***Research to gain understanding and to develop new approaches***
- ◆ ***Include human systems integration within information assurance***
- ◆ ***Develop standards and Interoperability – key to decomposition***
- ◆ ***Improve network protocols and crypto/key management***
- ◆ ***Design information assurance into systems upfront!***