Simulation Interoperability Standards Organization

"Simulation Interoperability & Reuse through Standards"

A Survey of Cross Domain Solutions for Distributed Mission Training

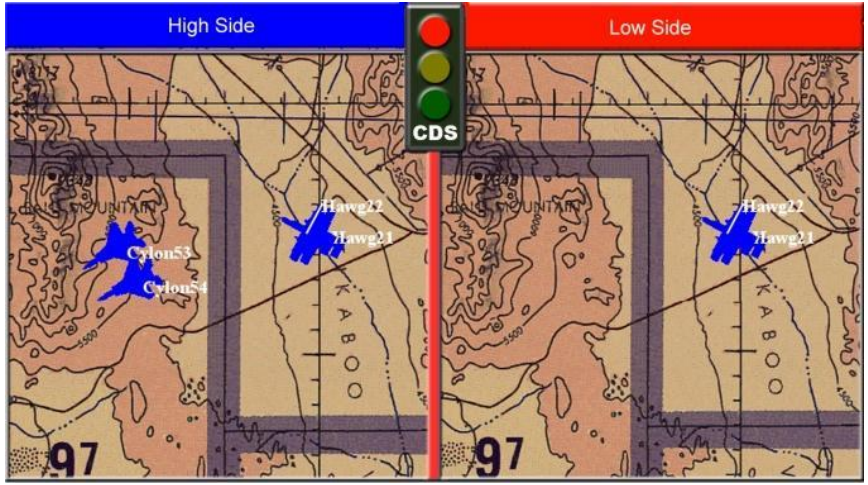
2020-SIW-Presentation-019

Peter Ross+, Will Oliver, and Peter Ryan,
Defence Science & Technology, Australia
+ presenter

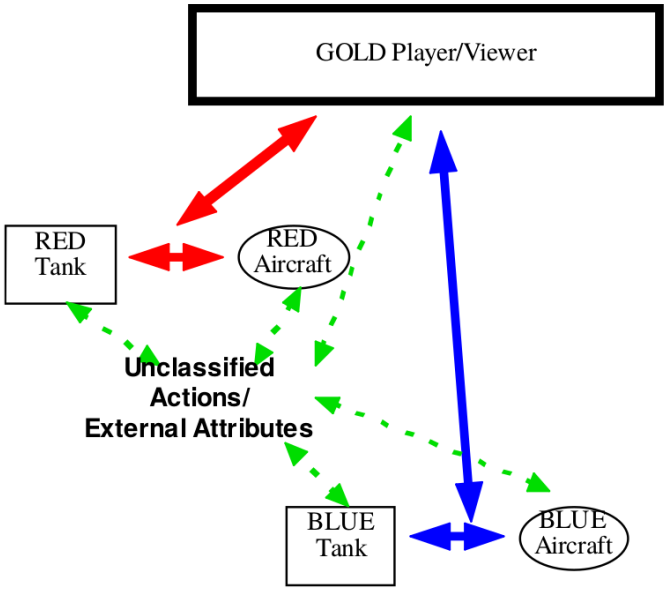
Outline of Presentation

- Cross Domain Solutions
- Distributed Mission Training
- Literature Survey
- Technology Readiness Levels of Cross Domain Solutions

Motivating Examples



McElveen et al. (2010) Cross Domain Rule Set Verification Tools and Process Improvements. I/ITSEC Paper 10042.

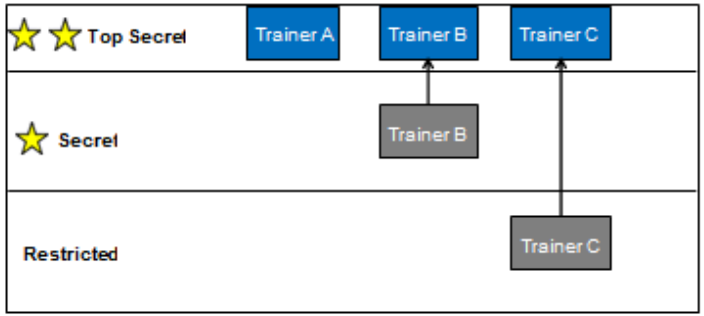


Luiijf et al. (1998) Fortezza-enabled Multi-level Sensitive Simulations. 98S-SIW-020.

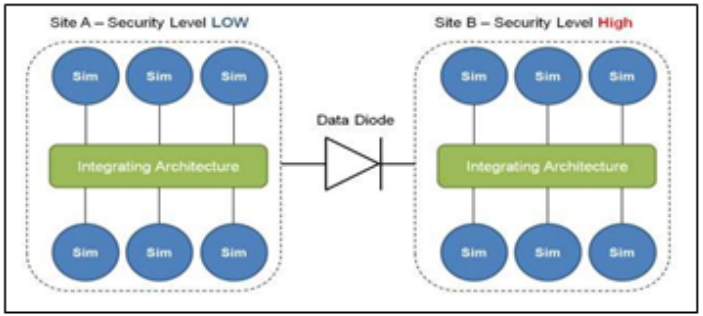
Cross Domain Solution

- Cross Domain Solutions are a type of security capability used to connect discrete systems within separate `security domains' in an assured manner
- CDS are implemented using a combination of human and machine actions, resulting in the transfer of information from one security domain to another.
- Rules govern when and how information is transferred from the higher domain to the lower domain

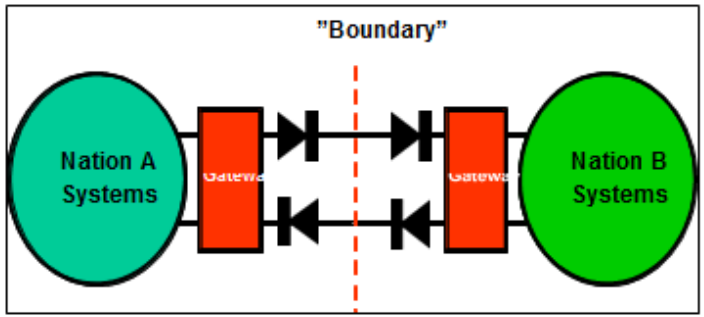
Integration Across Security Domains



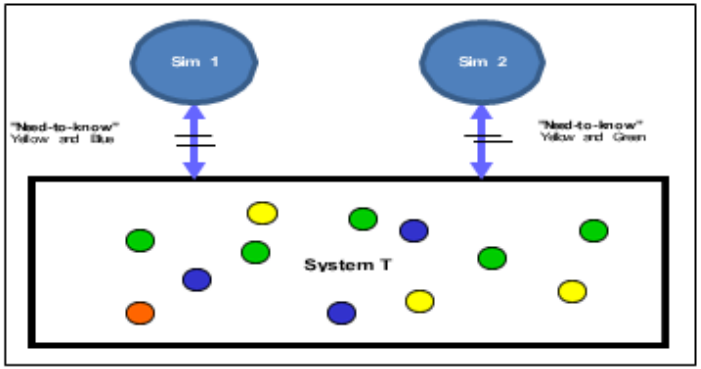
(a) System High



(b) Multiple Independent Levels of Security



c)Information Exchange Gateway



(d) Multi-level Security

Möller et al. (2011) Towards Multi-Level Security for NATO Collective Mission Training – a White Paper. 11S-SIW-069

Technical Protection Methods (Rule Sets)

- **Content Blocking**
  - blocks the passing of protocol information from the high side to the low side of the CDS
- **Content Guising**
  - substitutes one set of information for another in the protocol information as it passes from high to low
- **Interaction Guising**
  - seeks to represent a battlespace interaction as being of a different character than its simulated form on the high side

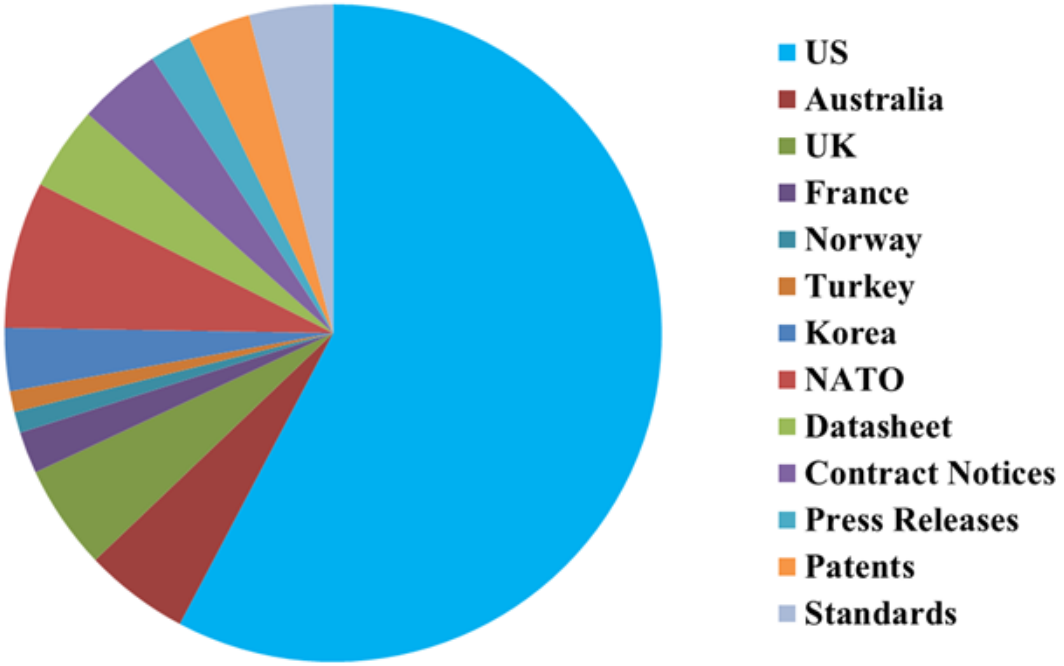
Non-Technical Protection Methods (Human Intervention)

- **Behaviour Prohibition**
  - These methods explicitly prohibit warfighters from performing specific actions, techniques, or procedures.
- **Information Control**
  - This type of rule is often a technical rule that restricts access to specific, protected information to the high side participants.
- **Certification**
  - This requires simulation vendors to assert that their modeling implementations follow conditions defined by the rules plan.

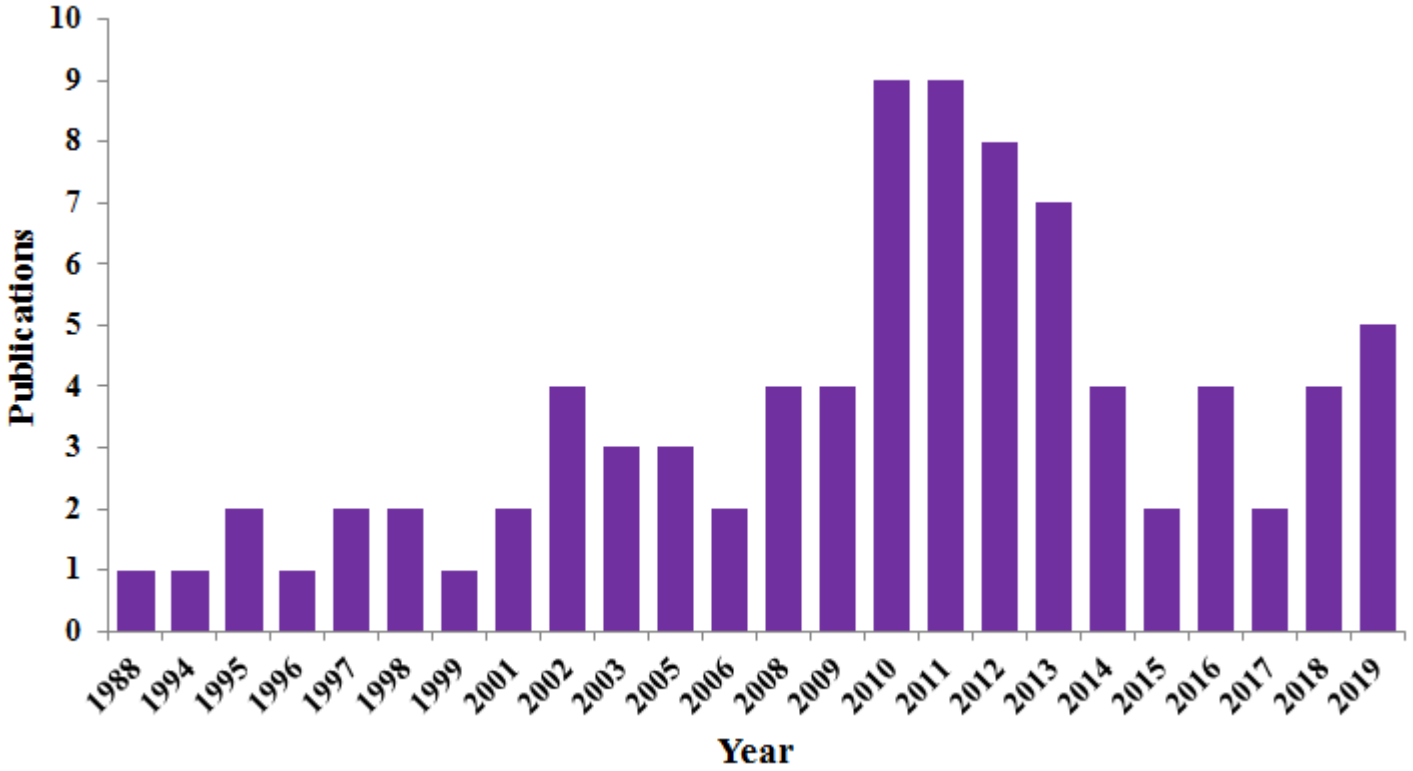
Sample Rule Set for DIS Domain

- ES PDU – hard to filter since would compromise exercise fidelity
- Fire / Detonation PDUs – can filter some fields
- EE and Designator PDUs – can filter some fields

Distribution of CDS Information Sources



Papers Reported by Year: 1998 - 2019



Permanent CDS Solutions

- Navy Continuous Training Environment
- Distributed Mission Operations Network
- Nevada Test and Training Range
- Joint Pacific Alaska Range Complex
- US/Korea Battle Simulation Center

Temporary / Experimental CDS

- Broad Area Maritime Surveillance (BAMS)
- US Army Vengeance
- Fleet Battle Experiments
- LVC Bold Quest
- Cyber Operational Architecture Training System (COATS)
- UK Niteworks
- NextGen Experimentation Hub

Technology Readiness Levels (NASA)

- **TRL 1-3**
  - TRL 1 basic principles identified
  - TRL 2 technology concepts
  - TRL 3 proof of concept
- **TRL 4-5**
  - TRL 4 laboratory validation
  - TRL 5 validation in a relevant environment
  - TRL 6 prototype demonstration
- **TRL 6-7**
  - TRL 6 prototype demonstration in a relevant environment
  - TRL 7 prototype demonstration in an operational environment
- **TRL 8-9**
  - TRL 8 system qualified and tested
  - TRL 9 system proven in operations

Technology Readiness Level:
https://www.nasa.gov/directorates/heo/scan/engineering/technology/txt_accordion1.html

TRL 1 - 3

- **Laboratory experimental systems or even theoretical designs**
  - TRL 1 specifies basic principles identified
  - TRL 2 technology concepts
  - TRL 3 proof of concept
- **Examples**
  - CERTI (French Aerospace)
  - SecProxy
  - HLA Security Guard
  - SENSIM (US Army/ Netherlands Army)
  - HLA RTI Ipsec
  - Generic HLA CDS

TRL 4 - 5

- **Generally prototypes**
  - TRL 4 specifies laboratory validation
  - TRL 5 validation in a relevant environment
- **Examples**
  - DIS Deep Packet Inspection (FPGA approach)
  - Patented System from L3 (hardware approach)

TRL 6 - 7

- **TRL 6-7 systems can be considered as mature prototypes**
  - TRL 6 specifies a prototype demonstration in a relevant environment
  - TRL 7 specifies a prototype demonstration in an operational environment
- **Examples**
  - AIME Secure (UK Dstl / Qinetiq)
  - NAWCTSD Distributed Training Network Guard and Enterprise Network Guard
  - AFRL Distributed Training Network Guard

TRL 8 - 9

- **TRL 8-9 refers to systems that have been deployed and are operational**
  - TRL 8 describes a system that has been qualified and tested
  - TRL 9 describes a system that has been proven in operations
- **Examples**
  - Radiant Mercury Guard (RADMERC)
    - *Support DIS. HLA support achieved through additional products*
    - *USN system; Lockheed Martin contractor; >800 instances world wide*
  - SimShield
    - *Supports DIS, HLA, TENA etc*
    - *Forcepoint/Raytheon*

Summary and Conclusion

- **CDS for DMT using only open-literature sources**
- **US was the major source of literature on CDS with only a few papers cited from Europe and other areas**
- **Radiant Mercury Guard and SimShield main commercial products from Lockheed Martin and Forcepoint/Raytheon respectively**
  - RADMERC appears to be the more widely adopted system with applications dating back to mid 1990s and over 800 installations globally. RADMERC is protected by US patents.
  - SimShield is a newer, seemingly more capable system with support for more simulation protocol types but there is little information on its performance reported in the literature.

Simulation Interoperability Standards Organization

"Simulation Interoperability & Reuse through Standards"

QUESTIONS