NDIA

NATIONAL DEFENSE INDUSTRIAL ASSOCIATION

STRENGTH THROUGH INDUSTRY & TECHNOLOGY

NDIA ATC Project Updates

Recap: Synthetic Instrumentation & Cyber Security

Mike Dewey

March 26, 2019

Projects Recap from September 2018 Meeting

- Follow up to “Software Architecture for Synthetic Instrumentation Trade Study” undertaken in 2014
  - Created a questionaire & distributed to DoD individuals associated with Navair, Army and Air Force.
    - Does the DoD have a need for this effort? – i.e. a standardized method for communicating / controlling Synthetic Instrumentation. During the 4/17 meeting Dave Carey pointed out that IVI classes exist for many SI functions, so couldn’t IVI classes be used to “standardize” these interfaces?
    - What problems are we trying to solve by creating this standardization? Are there some examples that one can point to today that demonstrate how standardization would solve these problems?
  - No response from questionaire
- Recommendation: No need to pursue this effort, IVI classes can offer many of the standardized interfaces for SI functions

Projects Recap: Cyber Security Task

- 4/17/2018: Projects team asked to initiate a task to address cyber security for ATE systems
- Mike Dewey / Dave Carey as co-project leads initiated effort relating to ATE Cyber Security
- Questionnaire regarding Cyber sent to all NDIA members on 6/18/18 – limited response – 3 from DoD, 2 from industry
- Lack of response / participation indicates limited interest in this task
  - Reluctance on the part of industry to participate – addressing cyber is considered company IP
  - Projects committee recommended terminating any additional effort for this task
- Any future effort should be coordinated with other existing cyber project efforts that might be underway with other NDIA divisions, e.g. the Cybersecurity Division
- Framework for Cyber security of ATE systems will most likely employ methods / procedures detailed in the DoD's Application Security Technical Implementation Guide which is based on NIST documents and details how to manage and maintain a secure software – based system

Cyber Questionaire:
(Submitted to both DoD & Industry)

•Rank the outcomes associated with ATE cybersecurity for which you are most concerned. (0 (none) to 10 (high))

Outcome	Example	Rank
Confidentiality	Files or data theft	
Integrity	Corruption of data or system	
Availability	Server crash	
Non-Repudiation	Sending of misinformation or malicious messages	
Authentication	Login credentials theft	

•Rank the listed “entry” source or method for an ATE cybersecurity attack that concerns you the most and the perceived probability of that entry point for an attack. Rank 0 (none), 10 (high), Probability 0 to 100%)

ATE Entry Method / Source	Rank	Probability
Network		
Memory devices (USB Drive, CD/DVD, Disk)		
Equipment Vendor		
Test Program		
Instrument Driver		
User/operator		
Calibration Facility		
Repair Facility		
Test Instrument		
Weapon system or unit under test		

•Have you experienced a cybersecurity breach with a test system or instrument? If yes, explain if authorized or possible.

Cyber Questionaire: Compiled Responses

Outcome	Example	Rank	Rank	Rank	Rank	Rank	
	Responses	**1**	**2**	**3**	**4**	**5**	**AVE**
Integrity	Corruption of data or system	8	10	6	0	5	5.8
Availability	Server crash	5	10	4	0	8	5.4
Confidentiality	Files or data theft	7	7	6	`0	2	4.4
Non-Repudiation	Sending of misinformation or malicious messages	1	5	10	0	3	3.8
Authentication	Login credentials theft	2	1	8	0	2	2.6

ATE Cyber Security Entry Method / Source of Most Concern	Rank	Rank	Rank	Rank	Rank	
Responses	1	2	3	4	5	**AVG**
Equipment Vendor	7	10	7	10	2	7.2
Memory devices (USB Drive, CD/DVD, Disk)	8	10	10	0	5	6.6
User/operator	5	5	9	5	5	5.8
Repair Facility	3	10	5	10	1	5.8
Instrument Driver	7	10	7	0	1	5
Weapon system or unit under test	4	10	7	0	0	4.2
Test Program	6	7	6	0	1	4
Network	0	1	7	0	9	3.4
Test Instrument	4	7	5	0	1	3.4
Calibration Facility	2	7	5	0	2	3.2