Automatic Test Committee Chair's Report

Patricia Griffin

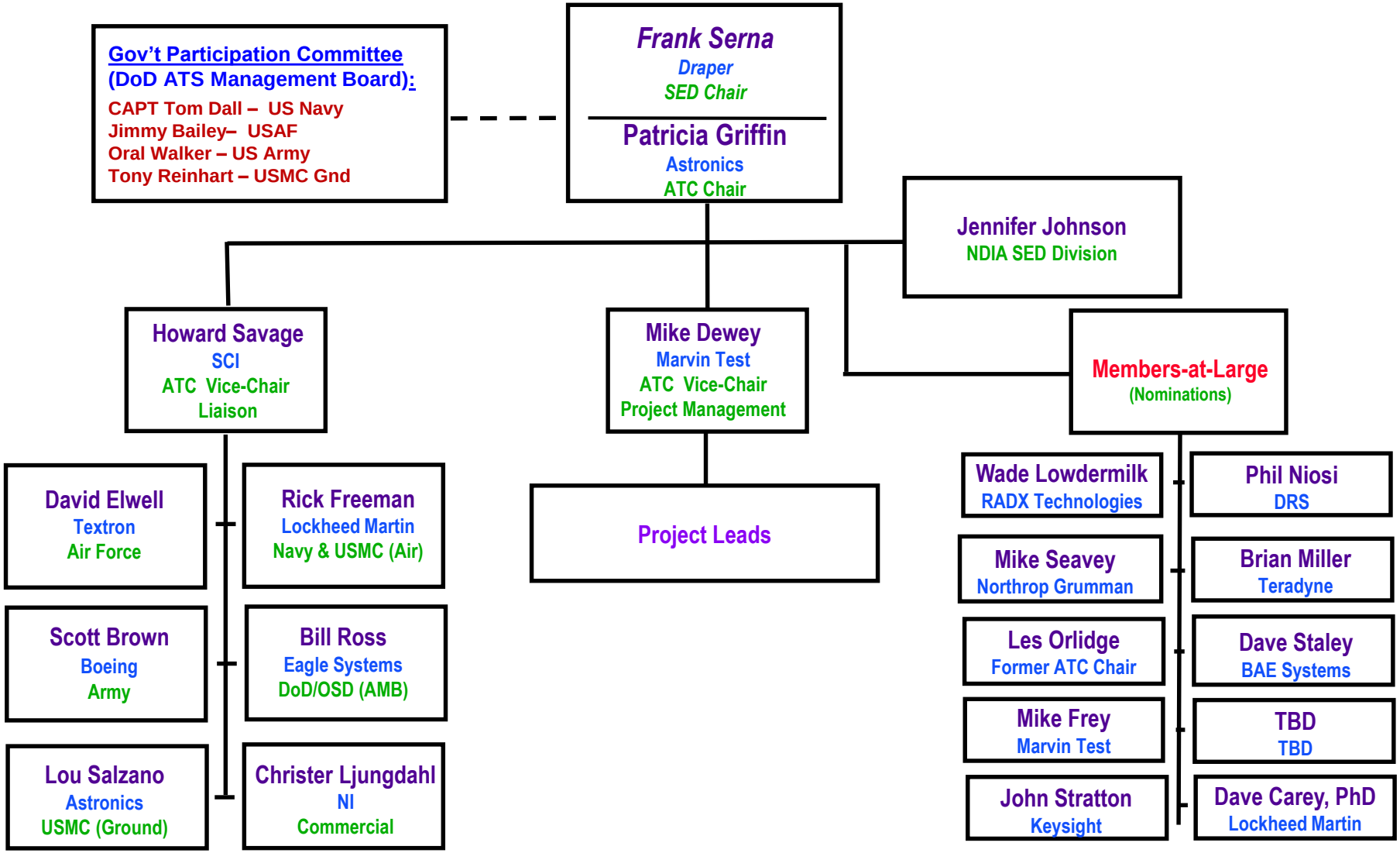
10 April 2019

678-315-5688
407-462-7898
Pat.Griffin@Astronics.com

National Defense Industrial Association - Systems Engineering Division

AUTOMATIC TEST COMMITTEE

2019 Steering Committee (April 10)



Automatic Test Committee - 2019 Task Plan

Proposed 2019 Tasks:

- **Government/Industry Liaison Reports**
- **John Slattery Award nominations**

- **ATC projects:**
  - Awaiting next project
  - Cyber Security discussions

Deliverables / Products:

- **Semi-annual Reports posted on ATC Web-site:**
  - **US Army ATS Liaison Report**
  - **USAF ATS Liaison Report**
  - **US Navy/USMC-Air ATS Liaison Report**
  - **USMC-Ground ATS Liaison Report**
  - **DoD AMB Liaison Report**
  - **Commercial ATS Liaison Report**
  - **ATC Project Updates**
- Survey industry for next project.

Schedule / Resources

Status/Review/Present at regular ATC meetings:

- **March 26th at NDIA HQ - Completed**
- **August 26-29 adjacent AUTOTESTCON in National Harbor, MD**
- **Every other month with SED (DC area)**

No resource issues or support anticipated

Issues / Concerns:

Limited Budget/resources:

- **ATC is focusing on high value projects, deferring lower priority projects primarily due to limited resources.**
- **Several committee member changes noted on new org chart**

Automatic Test Committee – 2019 Status

2019 Tasks Planned	Status	Accomplishments (deliverables, etc.) - Comments
No new tasks assigned from March 26th Meeting	Awaiting new task	-Two invited presentations at Spring meeting -LXI TWG (Security Working Group) -Cyber security vulnerability with LabVIEW -LXI security white paper posted to website
Chair challenged the Steering Committee to identify tasks that would be beneficial	Awaiting input	
John Slattery Nominations	In Process	Two nominations being drafted

Note to SED members: This presentation and white paper are available for review. If interested, contact Pat.Griffin@Astronics.com

Securing LAN-based Instrumentation Communication

LXI Working Group Status Review

Tom Sarfi
Business Development/NPI
Pickering Interfaces
tom.sarfi@pickeringtest.com

Rev NDIA_ATC_0319

www.lxistandard.org

Use the connection you already know!

Topics to be covered

- Introduction & Overview Security Standards
- LXI Communication Channels
  - Remote Control Web Browser Interface
  - Encryption
- PKI – Public Key Infrastructure
  - Certificates / Public & Private Keys / Encryption
  - Certificate Authorities (CAs)
  - Public Trust / Private Trust
- LXI Security WG Proposals for Secure Communication

Note to SED members: This presentation and white paper are available for review. If interested, contact Pat.Griffin@Astronics.com

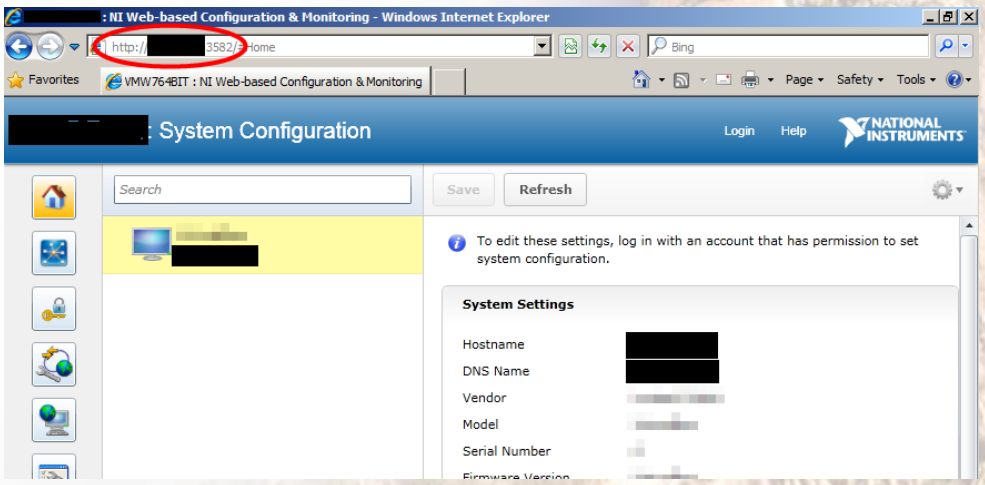
Cyber Security Vulnerability

LabVIEW Web-Based Configuration & Monitor

- NI System Web Server (default port 3582) –
- The system web server is used to configure the web server(s), manage HTTPS certificates, and manage other web service permissions.
- NI Application Web Server (default port 8080) –
- This web server hosts user created web services developed in LabVIEW
- Both ports remain open with critical computer information visible to anyone on the network.
- http://localhost:3582

This was presented by a member from a large defense company with approval from management and security team

- This has been around for about 10 years.
- Can Login as "admin" with a blank password
- Can create simulated devices, view even more information.
- By default this is enabled on all NI targets
- Any computer with the development suite installed



Cyber Security Vulnerability

LabVIEW Web-Based Configuration & Monitor
SOLUTIONS

- **Note: this requires Admin privileges on the computer.**
- **For a computer with LabVIEW installed**
- **Open the local services**
- **Open the properties for following services**
- **NI Application Web Server**
- **NI System Web Server**
- **Disable, Close, and STOP each service**
- **Reboot the system**
- **Verify that the services are still disabled**
- **Verify both local system cannot reach the ports**

New LabVIEW Installation

•For new installations of LabVIEW 2017 and newer:

•Install LabVIEW via command line using this command:

•setup.exe /props NIAPPWEBSERVERNOINSTALL=1.

•Note: this will not correct this issue if you have earlier versions of LabVIEW already installed.

Alternative Solution

•Disable incoming connections on these ports via firewall settings.

•Might require an IT policy change.