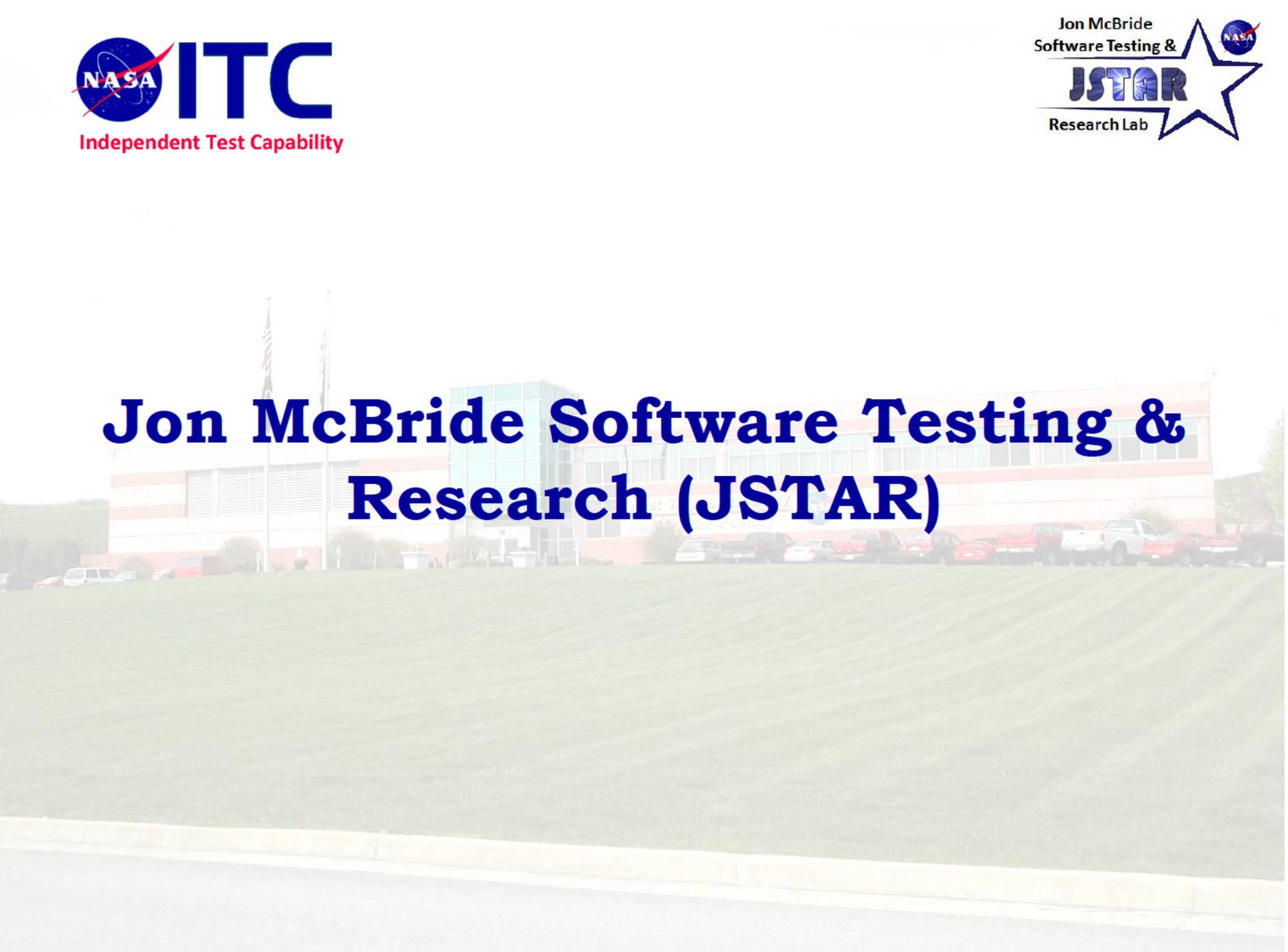




Jon McBride Software Testing & Research (JSTAR)

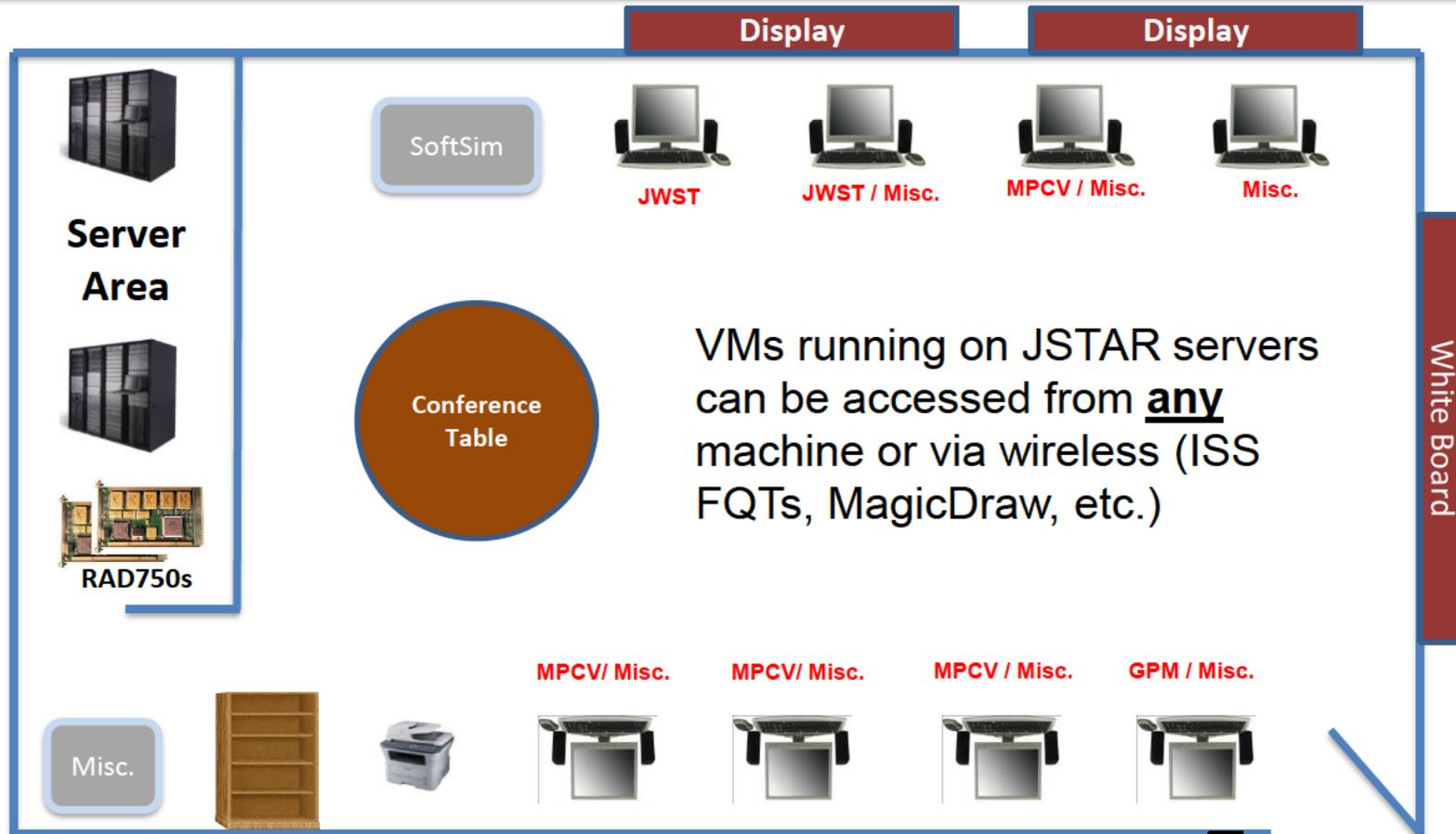


Independent Test Capability (ITC)

- Develop, maintain, and operate test environments and supporting tools for the IV&V Program that enables the dynamic analysis of software behaviors for multiple NASA missions
 - ITC Team = experts in test systems (simulations & test beds)
 - IV&V Project Team = experts in systems (Projects)

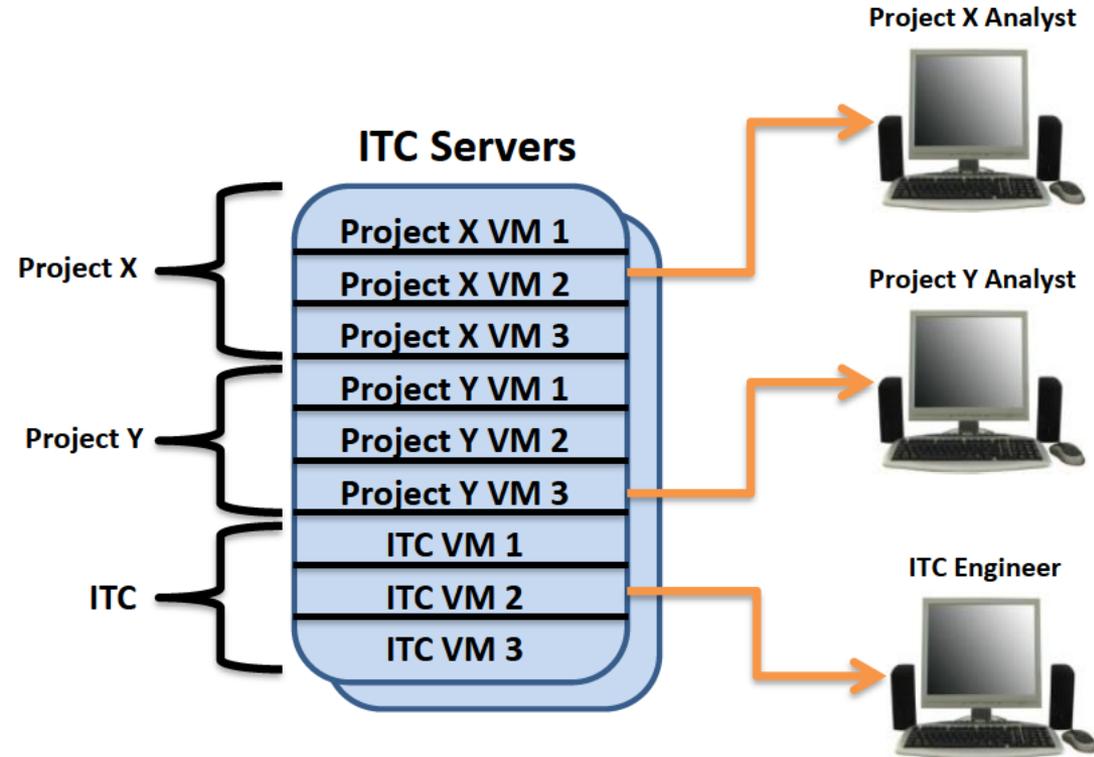
Jon McBride Software Testing & Research (JSTAR) Laboratory

- JSTAR Lab is a **shared resource** within NASA's IV&V Program and is available for use by anyone supporting the IV&V Program
- Provide advanced testing and evaluation capabilities in support of verifying and validating NASA's critical software systems
- Explores and rapidly matures capabilities needed to meet the future challenges of NASA including
 - Modeling and Simulations
 - Robotics Applications
 - Mission Flight Software
 - Spacecraft Development
 - Cutting-edge Tool Evaluations



Single Location – Multiple Preconfigured Tools and Test Environments

The lab utilizes server (VmWare) and desktop virtualization (VirtualBox) to improve the efficiency and availability of resources and tools. This provides the ability to run multiple virtual machines on each physical machine. Virtualization removes the physical server constraints and enables sharing of resources within the lab.



Creating virtual machines of test environments will allow for quick setup of test environments. This will increase efficiency of analysts because they will not have to spend many hours configuring their workstations. Also this will foster smooth transitions when team members transition to other projects.

- JSTAR vCloud provides functionality similar to remote desktop for virtual machines running on the segregated JSTAR network
- Access via <https://jstarvcloud.faircon.net/cloud/org/jstar>
 - Login credentials are managed by JSTAR Lab Manager and are different from IV&V Network credentials
- JSTAR Wiki contains detail on how to access
 - <http://itcjira.ivv.nasa.gov:8090/display/JSTAR/JSTAR+vCloud>
- Any tool installed in the JSTAR Lab can be exposed through the JSTAR vCloud
 - Currently only the highly requested/used tools are available

- List maintained on JSTAR Wiki (<http://itcjira.ivv.nasa.gov:8090/display/JSTAR/Lab+Resources>)
 - BAE RAD750 6U (contains onboard spacwire and 1553)
 - BAE RAD750 3U (is in Chassis with 1553 and Spacewire cards)
BK Precision Power Supply
 - Compact PCI (cPCI) Chassis
 - cPCI Bus Analyzer
 - Gespac 3750 (PowerPC 750)
 - FPGA Development Kits
 - One GR-CPCI-XC4V - http://www.pender.ch/products_cpci_xc4v.shtml
 - Six GR-XC6S - http://www.pender.ch/products_xc6s.shtml
 - Logic Analyzer (TLA6402 - <http://www.tek.com/logic-analyzer/tla6400>)
 - MIL-STD-1553 Cards (ExpressCard and cPCI)
 - Oscilloscope (MSO4104B - <http://www.tek.com/oscilloscope/mso4000-dpo4000>)
 - PMC Carrier Card
 - Spacewire Test Set (SWTS)



Independent Test Capability

JSTAR Current Body of Work



- **Current Project Overview**
 - JWST Integrated Simulation and Test (JIST)
 - Multipurpose Crew Vehicle (MPCV)
 - Space Launch Systems (SLS)
 - Ground Systems and Data Operations (GSDO)
 - OSIRIS-Rex (SoftSim)
 - International Space Station (ISS)
- **NASA Operational Simulator (NOS)**
 - Reusable Hardware Models and Utilities
 - Simulation Middleware
- **Test Automation**
- **Hardware Modeling**
- **Cyber Security**
- **STF-1 CubeSat**

- Enables IV&V Program project teams to IV&V complex system and software behaviors
 - Independent Testing
 - Fault Injection
 - Flexible Time
 - Source Level Debugging

*NASA's IV&V Program
Safety and Mission Assurance (SMA) Office
Information Assurance/Cybersecurity Support*

Cybersecurity



Cybersecurity – A Mission Assurance Function

Reducing Risk



NASA Missions are at RISK for Cyber Attacks -
Multiple vulnerabilities could adversely impact
Mission Operations (Architecture, SW, IT, etc.)

- Not only an “infrastructure” problem
- Flight and Ground Software Risks
 - Open Source Code
 - Commercial Operating Systems
 - General coding rules
- Ground System Networks for Missions
 - Unsecured data flows
 - Unknown network configurations/usage
 - Commercial transport (internet)

Reducing Risk



- The IV&V Program Cyber Team was formed to Assess, Understand, Communicate, Reduce and Mitigate the risk of cyber threats and attacks to NASA Missions.
 - Joint funded OSMA, IV&V and OCIO
- Joint Civil Servant and Contractor Team
 - DoD and FBI experience
- Working with OCIO as they establish a Cyber Security Council/Program

Identifying & Preventing Risks



- Perform Security Analyses throughout the development life-cycle on NASA Missions (part of IV&V approach)
- IV&V created a Vulnerability Assessment Capability - Performing VAP assessments for Agency CIO
 - Tool assessments and integration
 - Cyber Attack Survivability Assessment
 - JPL completed June 2015 (MSL, MER, DSN)
 - GSFC Underway (IONet, HST)
 - GSFC Planned (MAVEN, Near Earth Network, Space Network, Earth Orbiting Network)
- Assisting Headquarters in Cyber Road map development – It's more than infrastructure!
- Participant in NPRs, Standards, Handbooks

Identifying & Preventing Risks



- Established IV&V's Secure Coding Web Portal (SCP)
 - Providing tools and best practices to NASA community
 - Newsletter for latest information/threats
- Created Cyber Lab
 - Training Facility
 - Virtual Environment for Penetration Testing
 - Concept Verification (CCSDS Green book on Space Threats)
 - Tool integration and checkout
- Provided support to AMES SOC medium-to-high FIPS-199 A&A transition
- Performed Interoperability testing on the CCSDS Space Data Link Layer Security protocol – enabled them to publish CCSDS Green Book

Identifying & Preventing Risks



- Performing independent assessment of DOE's insider threat program
- Partnering with WV National Guard
 - Cyber guard teammate; Knowledge exchange for performing vulnerability assessments; provide training to WVNG on penetration testing and network defense
- Establishing partnerships throughout cybersecurity domain
 - NASA: Space Asset Protection, SWG, SAWG, Mission Assurance Security WG, ITSMB, HEO Security WG
 - External: DoD SwA CoP, DHS SW Supply Chain, AIAA Cybersecurity WG, Cyber Threat Modeling WG, Mitre, CMU-SEI, MIT-LL, WVANG, Dept of Energy

IV&V's Contributions to Discovering Vulnerabilities



Blue Team Vulnerability Assessment Program (BT-VAP)

- Comprehensive evaluation to ascertain the operational security posture of NASA's critical mission systems/networks that enable the mission to operate
- Methodically evaluate multiple factors using diverse Subject Matter Expertise

Five Key Role Specialists on the BT-VAP Team:

*Security Analyst/
Threat Protection*

*Network Security/
Information Assurance*

ICS/SCADA /Computer Network Defense

*Space Systems/
Program Protection*

*Software Security/
Cybersecurity Operations*



completed

in progress

Evaluate the security risks to mission critical systems without disrupting mission operations.