The ITEA Journal

December 2013
Volume 34, Number 4

T&E in the Global Marketplace

Published quarterly
by the International
Test and Evaluation
Association

ITEA Journal 2013; 34: 399–405

Automating the NERC CIP Compliance-Test Lab to Meet CIP Standards

Chuck Reynolds
Technical Systems Integrators, Orlando, Florida
Alex Henthorn-Iwane
QualiSystems, Santa Clara, California

Electrical utilities and other industrial control entities must adhere to strict cyber security standards such as NERC CIP and many others. Compliance with these standards to ensure secure operation requires extensive and expensive, expertise, programming, control, and manipulation of many devices within the networks of these entities. Automation and management of these activities with tools designed to do so within the entity can ensure timely meeting of these standards with substantial cost savings as well as guaranteeing a more secure entity.

Key words: Test automation; lab management; cyber security; CIP; NERC.

For electrical utilities and other industrial control entities who are serious about maintaining strong cybersecurity and meeting strict North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) compliance standards, sound testing is a must. A successful CIP compliance testing regimen must deliver consistent and clearly documented test processes and results to ensure compliance and avoid significant fines. Due to the financial incentives that these fines provide to executive management, electrical utilities are making substantial ongoing investments in preproduction and compliance test-lab real estate, equipment, and personnel time. However, these investments and the testing processes they support risk failure due to manual processes that dominate test-lab infrastructure management and typical testing practices. The key to the success of CIP compliance testing is automation software and accompanying best practices in test-lab infrastructure management and test cycles. Implementing a tool set to create a regimen of standardized, rigorous, repeatable, and documented test processes and results reporting for CIP compliance testing ensures the protection of electric-utility infrastructures, as well as bottom lines.

The imperative of NERC CIP compliance

NERC is a nonprofit corporation chartered to ensure that the bulk electricity system (BES) in North America is reliable, adequate, and secure. As the federally designated Electric Reliability Organization in North America, NERC maintains comprehensive reliability standards that define requirements for planning and operating the collective bulk power system. Among these are the (CIP) Cyber Security Standards, commonly referred to as the NERC CIP Standards 002-011, which are designed to ensure the protection of the Critical Cyber Assets that control or affect the reliability of North America's BESs. These eight primary standards include 41 requirements and 164 sub requirements for mandatory compliance from all of the major electric companies that make up the North American power grid.

NERC CIP standards and guidelines apply to all Responsible Entities (REs) within the bulk power system, which are required to retain 12 months of auditable data, documents, and records on their information-security controls and specific logs for 90 days in order to be compliant with the new CIP standards.

Electric utilities are currently being audited based on CIP version 3 and are mandated to become fully compliant with version 4 by April of 2014, which has many entities struggling under the timeline pressure because of limited resources. In addition, CIP version 5 has already been drafted and is awaiting final approval. The financial significance of CIP compliance cannot be underestimated. Fines for compliance violations can be up to $1 million per day; since CIP compliance standards were published in 2008, more than $150 million in fines have been levied.

Many other government and regulatory agencies are looking to replicate the CIP standards to address the same cybersecurity issues within their respective industries. The NERC CIP compliance standards are leading the way in cybersecurity within networks across a broad range of industries.

What is involved in CIP compliance testing.

CIP compliance testing is challenging to accomplish due to the broad nature of the compliance standards and the need to maintain a high degree of auditability. The reality is that nearly 80% of preproduction test-lab equipment and personnel time can be dominated by CIP compliance testing. There are 11 standards, some of which have to do primarily with physical security, personnel and training issues, and incident response and reporting. However, a number of the standards require ongoing testing to validate compliance:

CIP-002: Critical Cyber Asset Identification. Requires the identification and documentation of a risk-based assessment methodology which, applied annually, will identify Critical Cyber Assets.

CIP-003: Security Management Controls. Specifies that security-management controls must be implemented—information associated with Critical Cyber Assets must be classified and protected, access control to this information must be maintained, and change control must be documented.

CIP-004: Personnel and Training. Requires that REs include a security awareness and training program for personnel having authorized cyber- or authorized unescorted physical access.

CIP-005: Electronic Security Perimeters. Dictates that Electronic Security Perimeters (ESPs) and all access points to the perimeters be identified and that all Critical Cyber Assets reside within the ESP(s). REs must implement electronic access controls, continuously monitor access, and conduct annual vulnerability assessments at access points.

CIP-006: Physical Security of Critical Cyber Assets. Specifies that an RE must create and maintain an approved physical security plan and implement access controls as well as monitor the access points to Physical Security Perimeters.

CIP-007: Systems Security Management. Specifies a broad range of methods, processes, and procedures for securing Critical and noncritical Cyber Assets within the ESPs—such as patch management, malicious-software prevention, annual vulnerability assessment, and port and service lockdown—that should be implemented and documented for Cyber Assets within the ESPs.

CIP-008: Incident Reporting and Response Planning. Dictates that a Cyber Security Incident response plan be maintained and incident documentation retained for a period of 3 years.

CIP-009: Recovery Plans for Critical Cyber Assets. Specifies the creation and annual review of Critical Cyber Assets recovery plans, which include backup and storage of information to successfully restore Critical Cyber Assets.

CIP-010: Configuration Change Management and Vulnerability Assessments. Commands the prevention and detection of unauthorized changes to Cyber Systems by specifying requirements for configuration-change management and vulnerability assessment in support of protecting Cyber Systems from compromise that could lead to mis-operation or instability in the BES.

CIP-011: Information Protection. Dictates the preventions of unauthorized access to BES Cyber System information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to mis-operation or instability in the BES.

Practically speaking, CIP compliance testing can include:

Testing operational procedures. A simple example is ensuring the presence of secure log-in procedures with correct wrong-password responses and account locking after repeated failed log-in attempts.

- Checking operating-system (OS) and software product versions and patch-remediation levels.
- Implementing and configuring software security features—for example, testing to ensure that compliant antivirus products are installed and correctly configured or that only the correct ports are open on a device.
- Certifying new devices, OS versions, and Supervisory Control And Data Acquisition (SCADA) devices and deployment topologies, including full compliance regression testing.

The risk and waste of manual compliance-test processes

Given the financial importance of CIP compliance, it does not pay to make the significant capital and operational investments while neglecting process automation. The highly manual processes typically at play in test labs are the enemy of reliability, repeatability, and auditability. Manual processes are visible in a number of ways:

- Absence of live inventory visibility. In most test labs, equipment inventory is not tracked in a way that provides live visibility to engineers. While most IT organizations perform asset tracking for financial purposes, what passes for the inventory management used by engineers is a spreadsheet that is often ill maintained. As a result, it can be difficult to tell without exhaustive work what equipment exists, what is being used by whom, and what is truly available.

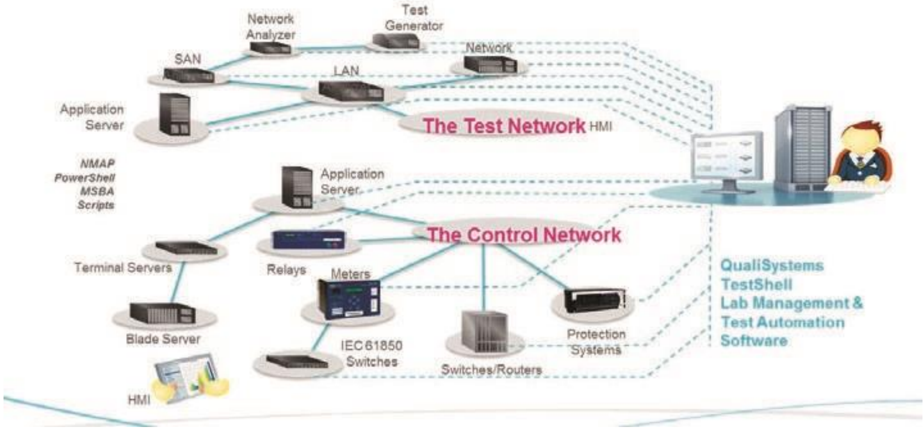
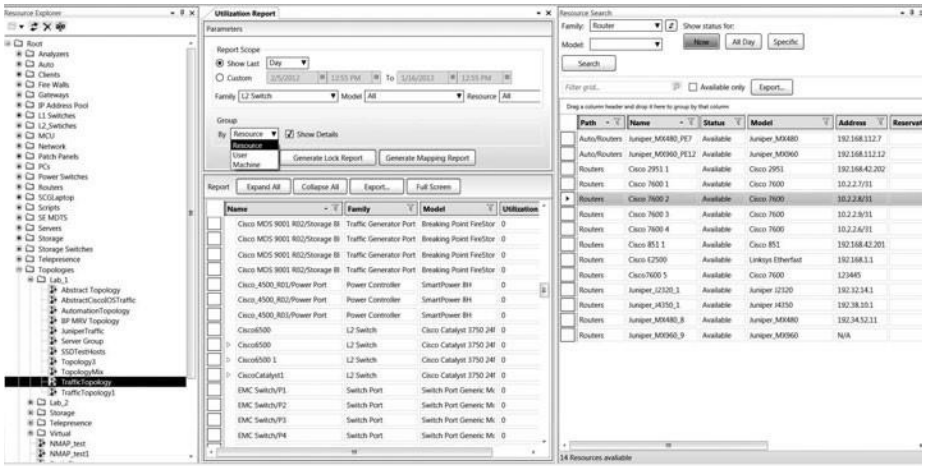


Figure 1. Lab monitor.

- Off-line test-topology design. Since there is no usable inventory visibility, it follows that test topology design is done completely off-line without regard for resource availability. Visio or other diagramming tools are most common, and basically produce the electronic version of a paper drawing, which is usually then printed to aid in a time consuming manual hunt for relevant equipment.
- Chaotic connectivity management and costly errors. Once inventory is found that is at least apparently available, engineers must manually re-cable connections between the equipment. With multiple engineers making additions, moves, and changes, typically without up-to-date documentation, errors such as disconnecting someone else’s test inevitably occur. Test breaks are a sadly common reality in most test labs today.
- Lack of device-configuration baselining. Engineers performing tests must often change OS images, apply patches, and create new configurations on devices. Unfortunately, it is all too easy to forget to set devices back to a baseline state, which means that when the next engineer uses the device, he or she may wrongly assume that it is configured at a known baseline state and execute a series of test protocols on an incorrect configuration.

The result of these manual processes is inaccuracy, inefficiency, and waste, evident through a number of indicators:

- Lack of test integrity and repeatability. Manual processes tend to experience operator errors that compromise test integrity. The lack of repeatability that results means that it is very hard to offer sufficient proof of compliance when offering test results to auditors.



Resource Explorer

- Root
  - Analyzers
  - Auto
  - Clients
  - Fire Walls
  - Gateways
  - IP Address Pool
  - L1 Switches
  - L2_Switches
  - MCU
  - Network
  - Patch Panels
  - PCs
  - Power Switches
  - Routers
  - SCGLaptop
  - Scripts
  - SE MDTS
  - Servers
  - Storage
  - Storage Switches
  - Telepresence
  - Topologies
    - Lab_1
      - Abstract Topology
      - AbstractCiscoIOSTraffic
      - AutomationTopology
      - BP MRV Topology
      - JuniperTraffic
      - Server Group
      - SSDTestHosts
      - Topology3
      - TopologyMix
      - TrafficTopology
      - TrafficTopology1
    - Lab_2
    - Storage
    - Telepresence
    - Virtual
    - NMAP_test
    - NMAP_test1

Utilization Report

Parameters

Report Scope

● Show Last: Day
○ Custom: 1/5/2012 12:55 PM To 1/16/2013 12:55 PM

Family: L2 Switch Model: All Resource: All

Group
By: Resource (Resource / User / Machine) ☑ Show Details

Name	Family	Model	Utilization
Cisco MDS 9001 R02/Storage BI	Traffic Generator Port	Breaking Point FireStor	0
Cisco MDS 9001 R02/Storage BI	Traffic Generator Port	Breaking Point FireStor	0
Cisco MDS 9001 R02/Storage BI	Traffic Generator Port	Breaking Point FireStor	0
Cisco MDS 9001 R02/Storage BI	Traffic Generator Port	Breaking Point FireStor	0
Cisco_4500_R01/Power Port	Power Controller	SmartPower BH	0
Cisco_4500_R02/Power Port	Power Controller	SmartPower BH	0
Cisco_4500_R03/Power Port	Power Controller	SmartPower BH	0
Cisco6500	L2 Switch	Cisco Catalyst 3750 24I	0
Cisco6500	L2 Switch	Cisco Catalyst 3750 24I	0
Cisco6500 1	L2 Switch	Cisco Catalyst 3750 24I	0
CiscoCatalyst1	L2 Switch	Cisco Catalyst 3750 24I	0
EMC Switch/P1	Switch Port	Switch Port Generic Mc	0
EMC Switch/P2	Switch Port	Switch Port Generic Mc	0
EMC Switch/P3	Switch Port	Switch Port Generic Mc	0
EMC Switch/P4	Switch Port	Switch Port Generic Mc	0

Resource Search

Family: Router Model:

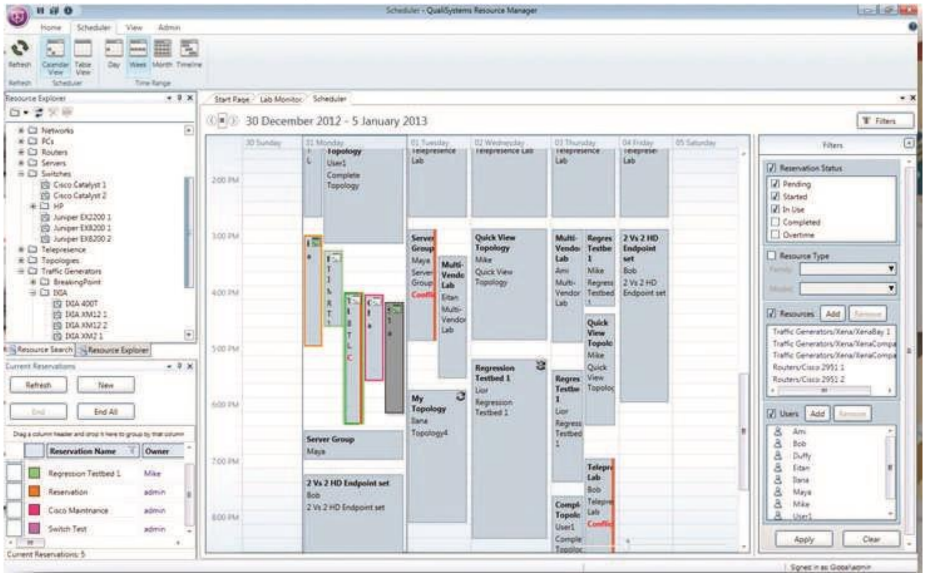
Show status for: Now All Day Specific

Search
Filter grid...
☐ Available only
Export...
Drag a column header and drop it here to group by that column

Path	Name	Status	Model	Address	Reservat
Auto/Routers	Juniper_MX480_PE7	Available	Juniper_MX480	192.168.112.7	
Auto/Routers	Juniper_MX960_PE12	Available	Juniper_MX960	192.168.112.12	
Routers	Cisco 2951 1	Available	Cisco 2951	192.168.42.202	
Routers	Cisco 7600 1	Available	Cisco 7600	10.2.2.7/31	
Routers	Cisco 7600 2	Available	Cisco 7600	10.2.2.8/31	
Routers	Cisco 7600 3	Available	Cisco 7600	10.2.2.9/31	
Routers	Cisco 7600 4	Available	Cisco 7600	10.2.2.6/31	
Routers	Cisco 851 1	Available	Cisco 851	192.168.42.201	
Routers	Cisco E2500	Available	Linksys Etherfast	192.168.1.1	
Routers	Cisco7600 5	Available	Cisco 7600	123445	
Routers	Juniper_J2320_1	Available	Juniper J2320	192.32.14.1	
Routers	Juniper_J4350_1	Available	Juniper J4350	192.38.10.1	
Routers	Juniper_MX480_8	Available	Juniper_MX480	192.34.52.11	
Routers	Juniper_MX960_9	Available	Juniper_MX960	N/A	

14 Resources available

Figure 2. Lab utilization and search.



Scheduler - QualiSystems Resource Manager

Resource Explorer

- Networks
- PCs
- Routers
- Servers
- Switches
  - Cisco Catalyst 1
  - Cisco Catalyst 2
  - HP
  - Juniper EX2200 1
  - Juniper EX8200 1
  - Juniper EX8200 2
- Telepresence
- Topologies
- Traffic Generators
  - BreakingPoint
  - IXIA
    - IXIA 400T
    - IXIA XM12 1
    - IXIA XM12 2
    - IXIA XM2 1

Current Reservations

Refresh
New
End
End All
Drag a column header and drop it here to group by that column

	Reservation Name	Owner
🟩	Regression Testbed 1	Mike
🟧	Reservation	admin
🟥	Cisco Maintnance	admin
🟪	Switch Test	admin

Current Reservations: 5

30 December 2012 - 5 January 2013

Filters

☑ Reservation Status
☑ Pending
☑ Started
☑ In Use
☐ Completed
☐ Overtime

☐ Resource Type
Family:
Model:

☑ Resources Add Remove
Traffic Generators/Xena/XenaBay 1
Traffic Generators/Xena/XenaCompa
Traffic Generators/Xena/XenaCompa
Routers/Cisco 2951 1
Routers/Cisco 2951 2

☑ Users Add Remove
Ami
Bob
Duffy
Eitan
Ilana
Maya
Mike
User1

Signed in as Globaladmin

Figure 3. Scheduling.

Poor test-process documentation. Manual processes are by nature difficult and time consuming to capture in documentation for auditing purposes. When changes occur in testing processes, it is too easy to miss documentation steps, which can bedevil the audit trail.

Incomplete test reporting. Thorough testing can generate voluminous result data. Manual analysis processes struggle to digest these data and provide sufficient reporting for auditing purposes.

Large ratio of test setup to actual testing. Test engineers can easily spend days in the setup process for a test that takes less than a day to run.

Very low asset utilization. Millions of dollars in capital equipment are typically only 15% to 20% utilized. This represents a huge waste of annual capital-depreciation costs.

There are significant implications of the inaccuracy and waste created by manual operating processes in CIP compliance-test labs:

Risk of noncompliance due to issues with test integrity, repeatability, and documentation. Even if testing processes are painstakingly performed in an accurate fashion most of the time, the inefficiency and slow pace of manual processes may make it nearly impossible for allocated personnel to achieve sufficient testing coverage and reporting, which creates further compliance risk.

Significant waste of capital-depreciation costs. Test-lab asset utilization under 20% also means that as demands for compliance testing grow, the pace of investment in test-lab capacity will rise at a rapid rate. With data centers costing anywhere from $1,000 to $3,000 per square foot, inclusive of equipment costs, this can lead to huge, unnecessary capital expenditures (CAPEX) outlays over time.

Implement a test and lab automation solution

Using a test- and lab-automation solution can help test labs achieve dramatically higher accuracy, efficiency, and productivity, leading to significant CAPEX and operational expenditures (OPEX) savings, faster test-cycle completion, and sustainably documented processes and reporting for CIP compliance auditing. A sound test-lab automation solution delivers a fully integrated, object-oriented software framework for automating preproduction and CIP compliance test labs and includes:

Centralized, live infrastructure and resource inventory;

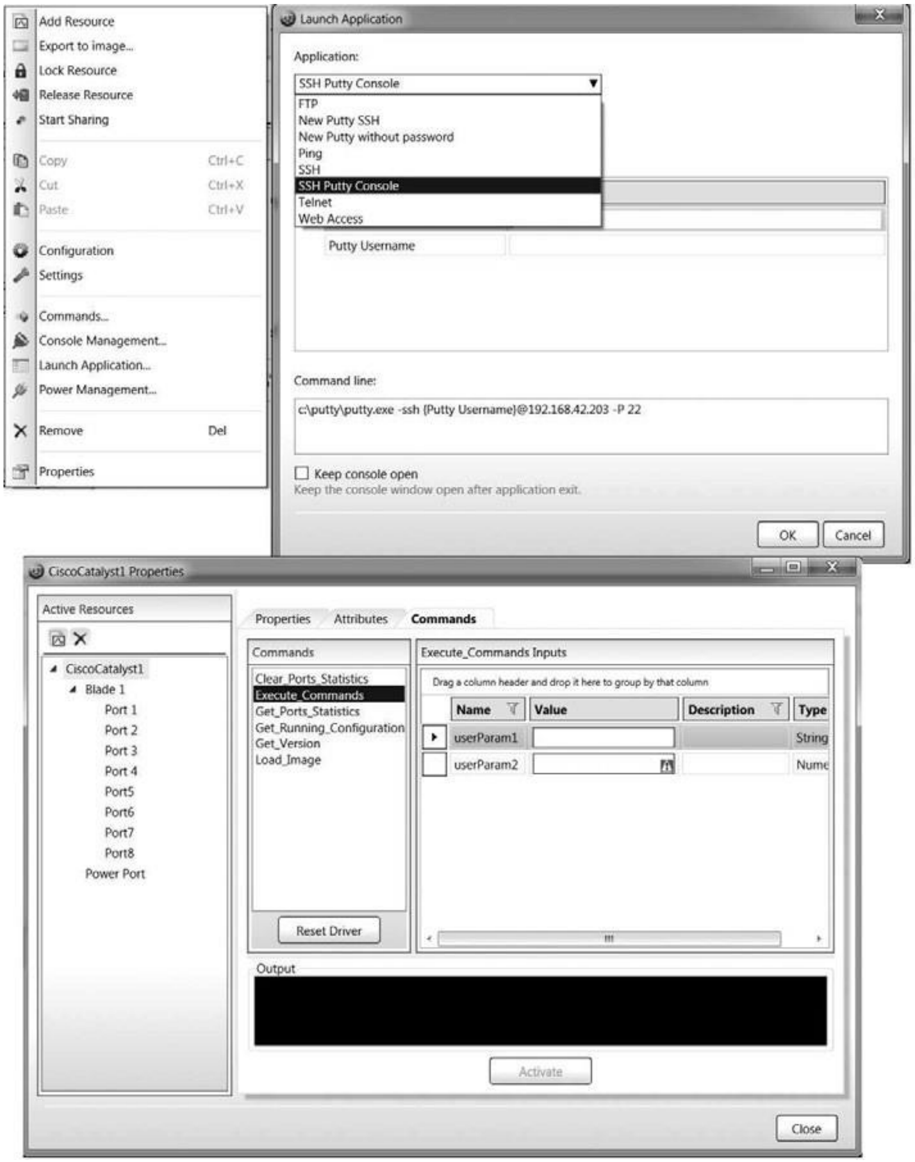
Inventory-aware test-topology design;

Shared, calendar-based resourceand topology reservation;

Connectivity mapping and automated connectivity control;

Easy-to-create automated provisioning tasks;

Creation of automation workflows that are friendly to nonprogrammers, based on a library of highly reusable, template test objects that can be created from a wide variety of sources and leveraged to create



Application: SSH Putty Console

Command line:

```
c:\putty\putty.exe -ssh {Putty Username}@192.168.42.203 -P 22
```

□ Keep console open
Keep the console window open after application exit.

Name	Value	Description	Type
userParam1			String
userParam2			Nume

Figure 4. Commands.

- Auto-discovery, auto-baselining, and other automated maintenance routines, and
- Full test-automation workflows; and

Powerful automated reporting that provides a rock-solid audit trail.

If designed properly, the automation architecture avoids the pitfalls of script-based approaches to automation, which cannot scale due to their high maintenance costs. Best-of-breed commercial solutions deployed by industry leading organizations worldwide provide them with the fastest path to a successfully and sustainably automated testing system. Leading power utilities, enterprises, government and military agencies, telecommunication service providers, and technology manufacturers transform chaotic manually-driven environments to highly efficient test operations. These organizations can:

Manage test-lab inventory, including physical device under test (DUT) and testing equipment, L1 switches, and virtual resources such as virtual machines and virtual switches, in a live, searchable database of resource objects tagged with searchable attributes, eliminating manual searching for equipment in racks and allowing engineers to interface with the data-center infrastructure efficiently via software. An inventory and resource management tool allows

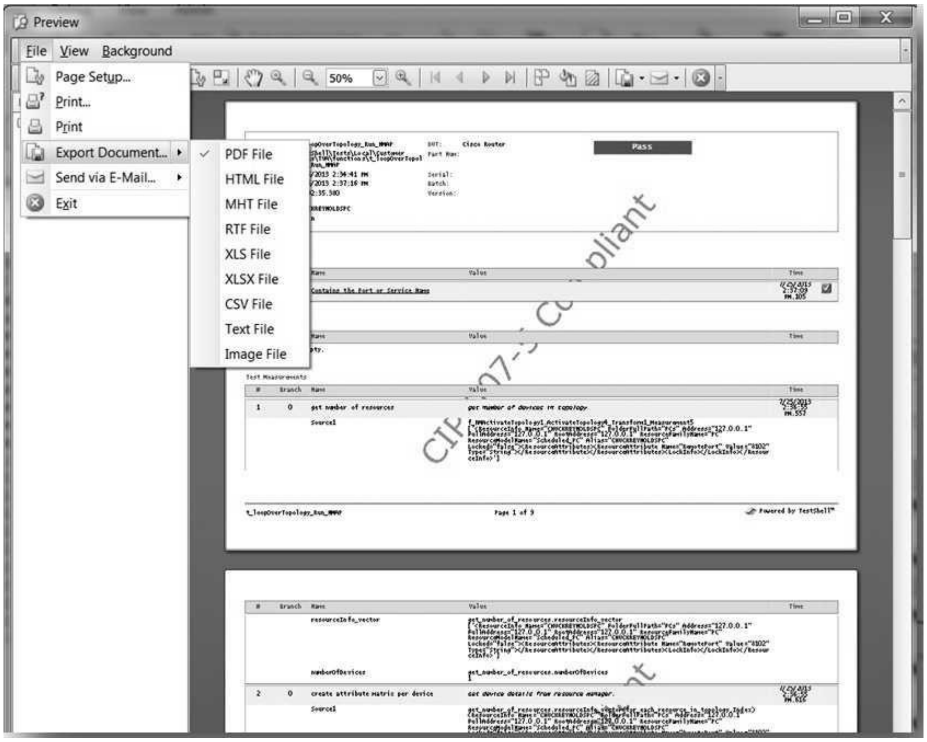


Figure 5. CIP report.

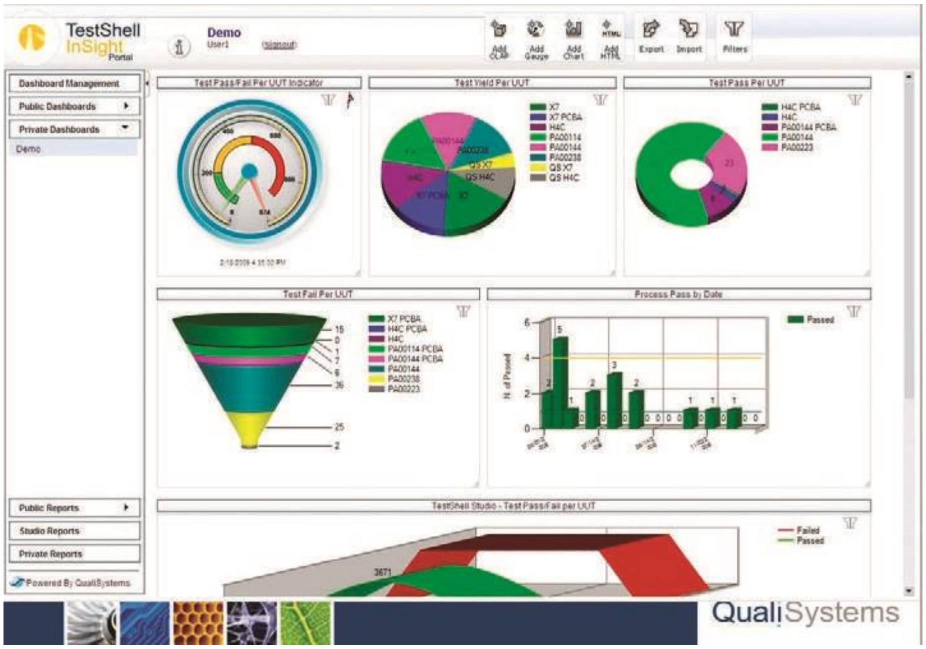


Figure 6. Dashboard.

for object hierarchies, which can represent relatively simple nested resources such as chassis, blades, and ports or complex, pre-integrated resource stacks such as converged infrastructure and ‘‘data center in a box’’ solutions (Figures 1 and 2).

Create variable test topologies via a software graphical user interface that allows drag and drop of resource objects onto a canvas, visually ascertain availability, design and sanity-check connectivity, and save the entire topology as a higher-level object in the resource library so that it can be reused later or by other engineers.

Schedule resources and entire test topologies through a common calendaring system, preventing test disruptions (Figure 3).

Manage connectivity remotely by generating patching or cabling requests to lab administrators or, if Layer 1 switches are in use, automatically connecting test topologies.

Make device provisioning error free by building automation objects for common provisioning tasks that can be launched from a right-click menu from a graphical test-topology view. Device provisioning can include uploading OS images, resetting device configurations to baselines, or creating routing adjacencies between virtual switches (Figure 4).

Create auto-discovery and auto-baselining processes that leverage an extensive array of control interfaces, graphical-user-interface automation, and scripting capabilities to streamline the management of inventory and device states to a compliant baseline.

Automate compliance regression tests in a fully documentable, repeatable fashion. Automation can be created through integration of existing automation scripts as testing objects as well as through creation of new test-automation objects through screen, graphical-user-interface, and other capture processes.

Generate comprehensive audit-compliant test result reports (Figure 5).

Produce custom business-intelligence dashboards to allow managers to analyze and collate data from the testing activities and metrics for input into planning initiatives (Figure 6).

Lab and test automation's beneficial impact on CIP compliance testing

Adoption and deployment of a lab-automation framework in the CIP compliance-test lab leads to significant, positive impacts for electric utilities:

Sustainable auditability. With automation comes built-in documentation of test processes, since the object-oriented method of creating, modifying, and maintaining template test elements creates an ongoing and live documentation for test composition and methodology. Automated lab-equipment maintenance processes with documented schedules provide proof of the compliance of the testing environment. Automated testresults analysis offers robust reporting that gives solid proof of compliance and compliance efforts.

A dramatic increase in the velocity of compliance test-cycle completion. Organizations routinely report time savings of upwards of 70% in their test cycles once they have automated the processes of allocating lab devices, provisioning devices, running tests, and generating reports. This acceleration ensures test coverage, reducing compliance risks.

Significant savings in lab CAPEX and OPEX. Organizations deploying lab-automation software report increases of 50% to 200% in device utilization, leading to capital budget savings, less depreciation waste, and accompanying savings in space, power, and cooling costs.

Conclusion

Electric utilities and industrial-control entities are under tremendous pressure to maintain a sustainable compliance regimen for continuously evolving CIP standards. Deploying test- and lab-automation software ensures that the compliance-testing process is reliable, rigorous, repeatable, and highly auditable. Using a lab- and test-automation tool set, electric utilities can build a sustainable platform for CIP compliance testing that protects their critical infrastructure, adheres to NERC CIP regulations, and protects their bottom lines. C

CHUCK REYNOLDS is the founder and CTO of Technical Systems Integrators, Inc. (TSI). TSI is a leading provider of solutions for test life-cycle management, electronic design automation, and product data/product life-cycle management in the United States, serving customers since 1987. Reynolds holds a bachelor's degree in computer science and electrical engineering from Duke University and a master's degree in engineering management from the Florida Institute of Technology. He is a member of ITEA and has over 30 years of involvement in testing. To learn more about TSI's CIP compliance automation libraries and professional services, or to reach out to Reynolds, visit http://www.tsieda.com. E-mail: creynolds@tsieda.com

ALEX HENTHORN-IWANE is the vice-president of marketing for QualiSystems, the leading supplier of lab infrastructure-management and test-automation software. Prior to joining QualiSystems, Henthorn-Iwane was the vice-president of marketing at Packet Design, Inc., a provider of network-management software. He has over 20 years of experience in senior-management, marketing, product-management, and technical roles at networking and security startups including Cosine Communications, Lucent Technologies, Livingston Enterprises, and Fibronics. He holds a bachelor of arts from the University of California, Berkeley. To learn more about QualiSystems, please visit http://www.qualisystems.com. Email: Alex.H@qualisystems.com