Trust In a Digital World - Examples of Why We Still Test

Benton Vandiver III, Alexander Apostolov
OMICRON electronics Corp USA

66th TX A&M Protective Relay Conference
College Station, TX

16 April 2013

Introduction

Role of FERC/NERC

Electric Industry Trends

Other Industries - Examples

Reasons to Test

Scope of Tests

Conclusions

Introduction

- The DOE quotes "Since 1982, growth in peak demand by population growth, bigger houses, bigger TVs, more air conditioners and more computers has exceeded transmission growth by almost 25% every year. Yet spending on R&D is among the lowest of our industries".
- The Smart Grid is “officially” founded under Title XIII, section 1301, of the Energy Independence and Security Act of 2007 to spur the modernization of the National Electric Grid. (SGIG initiatives in 2009 & 2011 fund projects.)
- “Smart Grid generally refers to a class of technology being used to bring utility electricity delivery systems into the 21st century, using computer-based remote control and automation. These systems are made possible by two-way communication technology and computer processing ***that has been used for decades in other industries***. They are beginning to be used on electricity networks, from the power plants and wind farms all the way to the consumers of electricity in homes and businesses.” (Energy.gov)

Role of FERC/NERC

- Defines the rulebook of (BES) grid operation through various reliability standards
- Fourteen (14) standards categories - containing 212 standards
- Over 15% are focused on Protection and Control (P&C) reliability
- Another 15% cover Cyber Security
- Today's digital Protection & Control System with digital communications network carries a 30% compliance focus!
- Adoption of Smart Grid technologies and the respective standards are considered key economic drivers for utilites and grid operators.
- But if PRC-005-1 is the most violated and fined of these 212 standards, then what impact will PRC-005-2 have?

Electric Industry Trends

- Monopoly vs. Deregulation and Diversification
- Energy Generation / Delivery / Consumption change by Govt Mandate
  - Good or Bad?
  - Does it make sense?
  - Is your bill lower today?
- Environmental and Technology Impacts
- Renewable Energy Push
- Smart Grid Inititative
- IOU’s & IPP’s must make a profit for investors
  - Cut anything seen as “non-essential”
  - Eliminate staff and replace with technology
  - It’s digital – why test it?
  - Replace it if it fails philosophy

Other Industries – Integrating Digital Systems

“While society continues to function at a high rate of speed, and operates on the existence of technology and technological advancements, the electric grid on which we operate is incredibly outdated.” (IEEE SmartGrid)

Other Industries have accelerated R&D to implement digital technology into their products – both for economic and competitive advantages. But testing these innovations are just as advanced - their focus is safety and reliability at the lowest cost.

> Automotive – sensors, computer, control, safety systems, performance

> Safety Industry – medical, consumer, commercial, electrical

> Aerospace – commercial jet, military jet, space-based systems

> Telecommunications - smart phone/TV, tablet, wireless, optics, cell, data centers

Would you drive, fly, or use an electrical product that had not passed all of its safety and operational tests?

Automotive

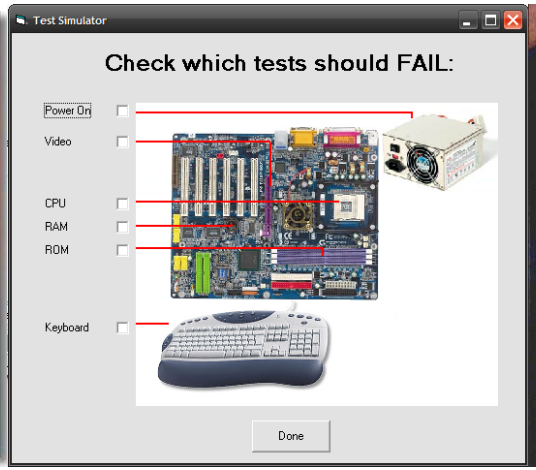
- The Auto industry is especially sensitive to safety related tests
  - Of course the “Crash Test” is part of this testing
  - Sensor and safety “systems” must be tested
  - performance, control, and operational tests too.
- Prototype vehicles have extensive “Road Tests” – why? Real world car testing requires real world conditions.
- Digital computer hardware & software control the engine, electrical, and safety systems. These require system tests to verify the interlocking and complexities of their decision making.
- System tests are divided into performance, comfort, reliability, and safety as each has separate goals to achieve – but each with the complete assembled vehicle.
- “System Tests" save 18%-20% of the product's manufacturing cost over its life cycle.

Safety Industry

Safety Industry defines “System Testing” as, "the next level of testing after Unit Testing and Integration Testing.”

“It's a critical testing best practice to perform system testing prior to rolling-out any product.”

> An estimated 40% of a product's cost is related to safety testing and standards compliance.



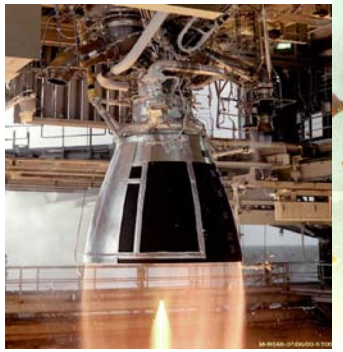
Aerospace

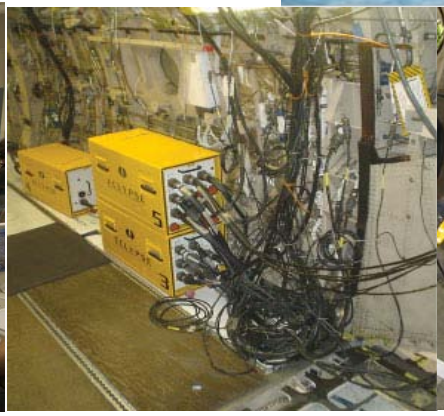
It goes without saying that the Aerospace industry performs system testing:

> Components must individually pass their own unit testing,

> then sub-assemblies of these components must pass integration testing,

> and finally the entire aircraft must pass rigorous system testing.





Telecommunications

Defines testing as "The process of performing a variety of simulation tests on a system to explore its functionality or to identify integration problems. System Testing is required before and after any system is put in place." (This industry spends an estimated 30% of their budgets on testing.)

> Most widely used products & services, everyone knows when there's a problem. Next to Aerospace, largest testing budget allocation.

> Exposure – Apple, June 24, 2010 iPhone 4 released. July 10, CNET announces problem. $100M USD Apple laboratory fails to find flaw.

iPhone 4S →

Reasons to Test

- Digital Devices are not single function
- Smart Devices require a realistic testing scope
- P&C systems are often distributed
- Component testing won’t ensure the P&C system works
- Digital Relay logic is embedded - multiple functions and I/O status
- Legacy testing processes decommissions the Digital Relay
- Communications based P&C require a systems approach
- Modern test equipment is capable of expanded testing role
- Reliability and availability of the P&C system depends on correct testing methodolgy
- Our industry is as important as all the others, maybe more so...

Our Own Industry Experts...

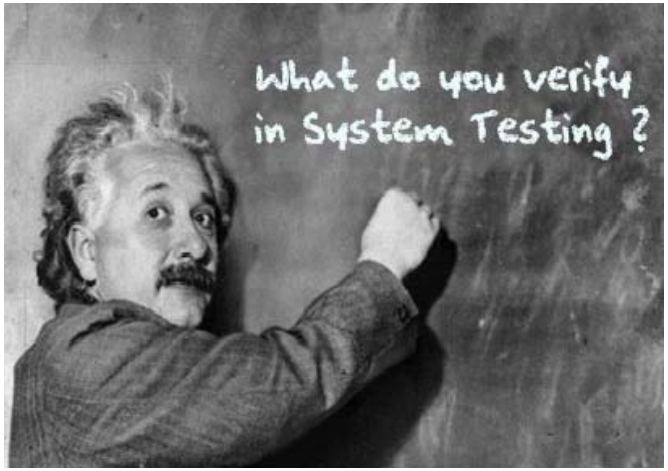
"In general it means that one should manage the use of systems and equipment based on the principle that **any IED is not an isolated device**; **it is part of a system** and should be looked at within the context of the **complete system**."

"Management of applications regarding their behavior, performance and location is important. Especially when applying open multi vendor systems. Testing varies depending on the internal implementation between IEDs, whether the application is distributed to multiple IEDs as part of the vendor's diversification for either security or redundancy goals, and for backup solutions when individual components fail in order to maintain the protection. **Single function testing cannot provide answers as to whether or not these are working correctly**."

(UCA-IUG System & Network Management document v2-2008

Why System Testing?

- Schemes
- Time
- Manpower
- Security
- Redundancy
- Reliability
- Accuracy
- Predictability
- Safety
- Expectations
- Complexity
- Distributed Architecture
- Regulations
- Economics
- Good Engineering Practice



What Are The Key Requirements?

- A level of complexity or interconnected processes that cannot be easily separated into reduced Black or White box tests.
- Single function test stimulus will not result in the expected operation due to conflicting control logic
- Requirement that all protection logic schemes are operating correctly per the system application.
- Must be supported by the engineering process
- Manufacturers must provide details on the IED application(s) and its system responses
- Definition of a FRS for the system test to be performed due to the system complexity

What Are The Key Requirements?

- Correct simulation of power system faults and abnormal operating conditions including simulation of multiple device interlocking and apparatus status.
- Verification of the fault clearing times required of the protection application, (i.e. if sub-cycle clearing is required of the primary zone protection then the proper system simulation should be used to prove it.)
- Verify that critical logging and report functions operate per the required protection application, missing events or data logging could put regulatory compliance in jeopardy.
- Verify protection logic for simultaneous occurrence of abnormal system events, evolving faults, power swings, SIPS, UFLS, etc…

What Are The Key Requirements?

- Need Positive tests that verify correct performance of the application boundaries.
- Need Negative tests that define correct selectivity and security.
- Verification of possible protection system component operational issues due to CCVT transient response, CT saturation / remanence, communication mal-operation, harmonics, etc..
- Verify adaptive settings for known power system conditions or operational configurations.
- Support accurate time synchronization of system simulations and time stamps with tested protection and measurement devices.
- and more...

Conclusion - System Testing Requires Commitment