21, rue d'Artois, F-75008 PARIS
http : //www.cigre.org

CIGRE US National Committee
2013 Grid of the Future Symposium

Technology Readiness for the Smart Grid

H. KIRKHAM C MARINOVICI
Pacific Northwest National Laboratory
US

G. FITZPATRICK
National Institute of Standards and Technology
US

K. LINDSEY
Lindsey Manufacturing
US

J. MCBRIDE
JMX Services
US

G.L. CLARK
Alabama Power Company
US

SUMMARY

Reluctance to adopt new technology into a utility application is understandable, given the critical nature of the infrastructure and the less-than-ideal experiences of some power companies. The authors of this paper have considered adapting the NASA approach of classifying technology readiness, but find it not quite appropriate because NASA was both the developer and the eventual user of the new technology it was evaluating, whereas a utility is ordinarily in the mode of a customer, acquiring a new product from a manufacturer. Instead of a generic scale of technology readiness, a scale of readiness is proposed specifically for the smart grid, based on the many standards that exist for the relevant technologies. In this paper we present an overall structure for organization of those standards.

The acceptance of new technology is organized into five SGL (Smart Grid Level) steps, numbered 5 through 9 to correspond approximately to the last five numbers of the NASA TRL scale. SGL 5 is a certification that the hardware and software of the technology is safe for the system into which is intended to be placed. SGL 6 is documentation that the system is safe for itself, and will have adequate reliability. It is thus clear that the steps differ from NASA's TRL in that technology development is not required; the transition is more one of documenting already existing system readiness, by making use of existing standards. Since SGL 6 describes a system that the standards validate is safe for the power system and for itself, it should not be restricted from being in a pilot-scale study, and achieving SGL 7. A larger-scale demonstration in a realistic environment will demonstrate interoperability and achieve SGL 8. Only when systems are installed and operating, and when disposal plans are in place will the designation of fully operable at SGL 9 be granted.

KEYWORDS

smart grid, standards, reliability, hardware tests, software tests, technology readiness, SGL

harold.kirkham@pnnl.gov

I. INTRODUCTION

There is a difference in TRLs as originally developed by NASA and its possible use in the smart grid. NASA had the two roles of developer and user of space systems. Utilities contemplating a system for the smart grid are not the developer of the new system, and they are unlikely to be the single user of the system. Therefore, while TRL is in principle a good way to document progress, a modified approach is needed.

The user of the system being developed for the smart grid might be a large utility, or a system operator, or a homeowner. If the TRL method is to be useful, it must serve its purpose of informing these users without hindering or favoring any of the developers. It must not add the burden of creating new standards, rather it could organize existing ones in a way that was more targeted to the business at hand.

The key to our proposal is to document progress through a defined sequence, and to organize that sequence in a way suited to the needs of the user. The user can "mix and match" to tailor the tests and the documentation to his specific needs. There are other approaches to assessing Smart Grid readiness, particularly for interoperability, an important aspect of the Smart Grid. Examples include the GridWise Architecture Council's Smart Grid Interoperability Maturity Model [1][2], and various software capability models. However, our proposed SGL approach extends beyond these methods in that it is more comprehensive and covers the performance of both hardware and software.

II. ADDING VALUE TO SMART GRID DEVELOPMENT

The TRL scheme at NASA serves to help estimate development cost (surely the original goal of the scheme), and documenting progress. These are both still required for a system headed for the smart grid, but the first of them is a matter for the developer, and is of little immediate concern to the ultimate user. The steps we propose differ from NASA's TRL in that technology development is not required, the transition is more one of documenting the readiness of an already existing system.

Development cost is part of the question of estimating profitability for the manufacturer. We consider this aspect of development to be not very relevant to the final outcome, whether the system being developed is an improved smart meter or an automatic recloser for a distribution circuit. We therefore set aside this application of TRLs.

The interest of the customer is in accessing information that shows that the system of interest is suited to its application. It is in the role "check-listing" a system destined for the smart grid that organized levels will be most beneficial.

The version of "levels" for the smart grid should be a documentable summary of tests, updated as qualification continues. The levels classify the purposes of the tests that are required to demonstrate suitability for the designation of a particular level.

III. SGL: THE SMART GRID READINESS LEVEL

For the purpose of the utility buying equipment for the smart grid, nothing below "lab validated" (what NASA would call TRL 4) is of interest. We therefore begin our levels at 5, aiming for a Level 9 that is broadly equivalent to "space qualified." It would seem perfectly appropriate to include in a Request For Proposals (RFP) the sort of tests to be done as this process unfolds, and to describe the documentation of evidence. The accumulation of documentary evidence is risk managements, an important part of overcoming risk-aversion.

Fig. 1, which was first shown in [3], shows the set of five levels that would work for elements of the smart grid.

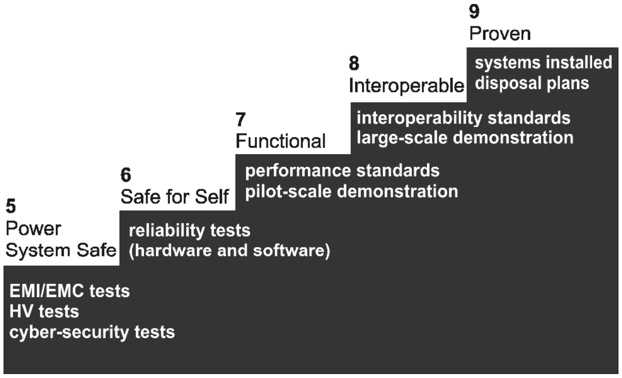

Fig. 1. Smart Grid Levels

On the tops of the steps are descriptions of the various stages that will be reached as tests are done to verify compliance with standards. On the right of the risers are examples of some of the things that need to be demonstrated by test in order to increase the "SGL" number. The tops of the steps summarize a state, the vertical risers the processes.

The first group of tests has to do with whether the system of interest is safe for the power system that it is to become part of. These days, one cannot leave out consideration of cyber-security, and achieving SGL 5 would require compliance with standards such as IEC 62443-2-4 standard [4]- Process Control Domain Security Requirements for Vendors (which aligns with Wurldtech Achilles Practices Certification (APC) process), or ISA99 Standards Roadmap and NISTIR 7628 [5]. We propose that the NIST catalog and the IEC 62443-2-4 standard be used to ensure cyber-security requirements are met before SGL 6 is granted.

For the hardware side of the system, experience can point the way. Transistor circuits started to get reliable in the late 1960s, and transistorized equivalents of electromechanical relays were installed in several utilities. Seemingly it had not been remembered that the high voltages and currents required by the original electromechanical devices had provided immunity to noise and transients, as well as the signal and the energy to operate the relay. Some early solid-state relaying systems failed in the noisy electromagnetic environment of the power substation.

Communication equipment in substations these days must demonstrate a level of noise immunity in tests such as those spelled out in IEEE Std 1613, the IEEE Standard Environmental and Testing Requirements for Communications Networking Devices in Electric Power Substations [6]. This is therefore the kind of hardware test that must be done before a system could be certified SGL 5.

There may also be a need to test insulation at high voltage (partial discharge according to IEC or IEEE standards, or withstand tests [7]), and such tests must be done for the system to get SGL 5 designation. Of course, at this and other levels, not all applications and not all users will require the same tests. The SGL allows a selection process from existing standards.

The tests required to win SGL 6 are aimed at ensuring that the system of interest is safe for itself. This sort of test might seem to be of little interest to the utility (why should I care if your stuff melts its wiring?) but of course there could be a cost impact to some future host utility if a system proved to be unreliable. An important concept is that there is some amount of "transferability" to a given SGL number. Therefore, tests of reliability are likely going to be done at some point, and the results added to the suite of documentation being accumulated.

For software, the white-box testing and black box testing should be completed, with the full documentation available to support compliance with the IEEE Standard for Software Test Documentation (IEEE/ANSI Standard 829 [8]), IEEE Standard of Software Unit Testing (IEEE/ANSI Standard 1008 [9]), IEEE Standard for Software Quality Assurance Plans (IEEE/ANSI Standard 730 [10]). (We have already proposed cyber-security testing before this level.)

New products sometimes must appear to some utilities as the ocean does to penguins on an iceberg. No one wants to go first. It has to be admitted that some of the reluctance is based on experience, such as the relaying experience described above. Broadly, the problems have been poor performance in the environment of the utility. But if the system or product is going to be used in a utility, it must at some point be put into a utility, somewhere. The achievement of SGL 6 means that the system has documented evidence of tests that show it is safe for the utility, and safe for itself. That should be enough to convince a utility to allow a pilot study.

Now we can see the SGL scheme at work: guiding the development of a product in a way that the ultimate user can be assured of safety and good performance. SGLs can help overcome reluctance to adopt new technology. In achieving this, no new standards are written: use is made of existing standards. But the standards are organized in a way to facilitate progress from factory to field.

The next levels of SGL are more specific to the product than the lower ones. SGL 7, for example, is gained only after a pilot study has shown overall satisfactory performance. In the past, pilot studies have been repeated because a user demands independent evidence of something. A goal of this SGL work is to avoid that repetition. At level 7, the compliance tests for this are becoming specific to the product. If a product works, say, on a particular 33-kV system, it should work on another. The documentation will be important, and transferable.

SGL 8 requires that interoperability is shown in a large-scale demonstration. Interoperability is an important element of the standards collected in the NIST catalog.

What is probably the least anticipated of all requirements is the need for disposal plans at SGL 9. In the past, disposal has been something that took place after the engineers who installed the system had retired. A relay lasted longer than an engineer, so it was the responsibility (or the chore) of the next generation to decide what to do with the old hardware.

With an increasingly software-driven smart grid, experience with our own computers makes it seem inevitable that we will be replacing stuff at a much higher rate, though the impact of that possibility remains to be fully grasped. User reluctance to adopt short system lifetimes seems to these authors to be justified. It may be that further smart-grid development should be devoted to considering the matter.

The conventional approach would be to engage in almost endless life-extension, which may mean software upgrades. If that is to be the case, then software upgrades will have to be a lot more straightforward than we are accustomed to on our own computers, and the software will have to meet the same sort of qualification tests as the original. The utility engineer must learn to accept that.

But in the end, when equipment must be scrapped, it is important to dispose of it properly. That is not merely a matter of being tidy, or even of being green: it is self-interest. There exists a large-scale business of counterfeiting electronics [11].

The counterfeit electronics is not intended to work. It is intended to make money. By inserting a small fraction of complete rubbish into a supply chain, the counterfeiter can make a good living, while the system vendor experiences a somewhat high failure rate. If the stuff makes it as far as the final customer, the failure may turn out to be critical.

Counterfeiting consists of re-using old parts and pretending they are new. There is no need for the part to do other than broadly resemble the part being imitated. It will be “re-topped” and inserted into a reel of genuine parts where the board-stuffing machinery will never notice the difference. Some examples of this kind of forgery are shown in Figure 2. The external company identification is forged, as well as the part identification, which need not relate to the actual part used in the forgery other than having the same general appearance.

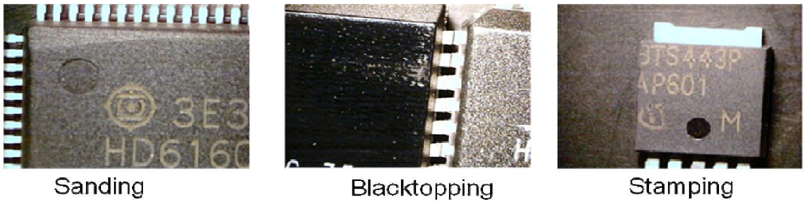
Sanding Blacktopping Stamping

Figure 2 Counterfeit electronics

By arranging for proper disposal of the parts that are used in the smart grid, their re-use in counterfeiting is denied. Since the number of parts may be in the tens of millions, that is important.

IV. MISSION ASSURANCE

In general, maintenance needs drive design. As engineers, we may realize it only deep in the recesses of our minds, but the reality is that we use methods in our various fields that demonstrate the truth of it. Maintenance was why radio tubes had sockets, and since the 1920s, radio resistors did not.

A system that can be easily and cheaply repaired may be allowed to have a higher probability of failure. That higher failure rate occurs not because we design a thing to fail, but because we do not take the extraordinary measures that we would take if repairs were impossible or costly. For example, a circuit board that is destined for the deep ocean as part of an optical amplifier might cost more than $1M/day to repair, because of the need to use a large ship in the recovery process. A lot of work goes into avoiding that repair!

For such an application, it is worth spending considerable time and energy on designing for long life, and testing to be sure. This process is known as mission assurance, and it has many aspects. A circuit board design may have a thermal study done to check heat flows on it, and a prototype or a mock-up may be thermally imaged. Electromagnetic tests (for example [12]) might be appropriate. A vibration study may be done, and some mechanical support may be reinforced before the thermal/bump-and-vibrate test (AKA shake-n-bake). The question of how far along such a path something intended for the smart grid should go is not easily answered. Given that some power components generate 120-Hz vibrations, vibration tests may sometimes be in order. That being the case, the SGL system must account for the need.

Life expectancy, mean time between failures, reliability, and spares policy must become design considerations for anything going into service in the smart grid. As new users of equipment (energy suppliers, services and so on) move into the smart grid, they must encounter unbiased requirements. These requirements will be different for different products, and for different users, so that while the SGL numbers may have the same overall meaning, the details of what qualifies a product for a given level is different.

Thus, the estimated MTBF may be a respectable 100,000 hours (about 11 years) for a home-user interface, but may have to be ten or more times that for a high voltage sensor. For systems with MTBF of 100,000 hours and an assumed exponential failure rate, almost 9% of the systems will fail every year – including the first![1] The chance of any particular device lasting until its MTBF is simply (1/e) = 36.77%.

V. CONCLUDING REMARKS

The requirements for achieving a given SGL must be realistically tailored. We propose that a layering of requirements can be developed for smart grid systems. Complying with the full set of mission assurance requirements and disposal requirements is not relevant at all points in a development program. However, new systems can be allowed into limited field trials only if they are demonstrated to the owner or operator of the system where they are to be installed to be safe.

We think that a sub-system being developed for the smart grid should be acceptable for a pilot-scale test in a power system if all the tests up to Level 6 are passed and documented. Claiming that a subsystem is “functional” (SGL 7) should require demonstration at pilot scale. Demonstration (and documentation) of interoperability, disposal plans and a large system demonstration should be required before the claim of “proven” (SGL 9) would be justified.

[1] If failures occur in a given system at a constant rate λ, the probability of survival at the end of time T is simply $P = \exp(-\lambda T)$. This equation is known as the exponential failure law, and it is quite representative of real systems with low failure rates. This is the mode at the bottom of the “bathtub curve.” The value λ is the reciprocal of the mean time between failures, or MTBF. For 90% of the systems to be functioning after 10 years the MTBF must be 95 years. Proving that value by test is not trivial.

We acknowledge that this paper is unlikely to be the last word. We therefore propose that a Smart Grid Level system be tailored in collaboration with the various stakeholders: the utilities, a representative of the customer, NIST and the manufacturers.

BIBLIOGRAPHY

[1] http://www.gridwiseac.org/about/imm.aspx

[2] *2010 Smart Grid System Report*, U.S. Department of Energy Washington, DC 200585, February 2012. See http://energy.gov/oe/downloads/2010-smart-grid-system-report-february-2012

[3] Technology Readiness and the Smart Grid, H. Kirkham and C. Marinovici, ISGT 2013, DOI 10.1109/ISGT.2013.6497804

[4] IEC 62443-2-4 A baseline Security Standard for Industrial Automation Control Systems. Available: http://www.us-cert.gov/control_systems/icsjwg/presentations/fall2011/D2-24-0200pm_Track1_Ahmadi-Holstein_rr_Title-BaseSecStandIndAuto.pdf

[5] NIST Smart Grid Interoperability Panel Catalog of Standards, Available: http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/SGIPCatalogOfStandards

[6] IEEE Standard Environmental and Testing Requirements for Communications Networking Devices in Electric Power Substations, IEEE Standard 1613-2003, May 2003

[7] Lindsey, Keith E., "Practical Aspects of Using Line Sensors in the Field", 2010 IEEE PES General Meeting, Paper 2010GM0920. DOI 10.1109/PES.2010.5589557

[8] IEEE Standard for Software Test Documentation, ANSI/IEEE Std 829-1983, 1983

[9] IEEE Standard for Software Unit Testing, ANSI/IEEE Std 1008-1987, 1987

[10] IEEE Standard for Software Quality Assurance Plans, IEEE/ANSI Standard 730, 1989

[11] Counterfeit Military Components and Chips, Available: http://www.darkgovernment.com/news/counterfeit-military-components-and-chips/

[12] MIL-STD-461: Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment, DOD, 2007