GRID MODERNIZATION LABORATORY CONSORTIUM
U.S. Department of Energy

Toward a Practical Theory of Grid Resilience

A Grid Architectural Approach

April 2018

S Widergren
B Kelley
R Melton
A Shankar
J Taft

PNNL-27458

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from the
Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062;
ph: (865) 576-8401
fax: (865) 576-5728
email: reports@adonis.osti.gov

Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
email: orders@ntis.gov <http://www.ntis.gov/about/form.aspx>
Online ordering: http://www.ntis.gov


This document was printed on recycled paper.
(8/2010)

Toward a Practical Theory of Grid Resilience

A Grid Architectural Approach

S Widergren[1]
A Shankar[2]
B Kelley[3]
J Taft[1]
R Melton[1]

April 2018

[1] Pacific Northwest National Laboratory
[2] Oak Ridge National Laboratory
[3] Lawrence Livermore National Laboratory

Contents

Figures

Tables

1.0 Introduction

A purpose of a good definition should be to support clear reasoning as an aid to superb decision making, but the standard "definitions" (yes, plural) of grid resilience are actually a hindrance to improving grid resilience. The usual approach to defining grid resilience conflates many issues in such a way as to obscure what should be done and it makes it very difficult for regulators to see how to pay for resilience measures of any significance (the events seem too remote and unlikely to be dealt with when there are other more pressing matters, except right after a big event; then there is a flurry of discussion about improving grid resilience but ultimately not much real action).

The purpose of this work is to provide practical means to make decisions about changes to the grid for resilience improvement purposes, starting with a better definition for grid resilience. The definition we apply in grid architecture work focuses on grid characteristics, not consequences, and clearly separates resilience from reliability.[1]

> Grid resilience is the ability of the grid to avoid or withstand grid stresses without suffering operational compromise or to adapt to and compensate for the resultant strains so as to minimize compromise via graceful degradation.

We have defined grid resilience as a three stage regimen based on a combination of risk assessment/vulnerability analysis and stress/strain models: resilience includes stress avoidance, stress resistance (passive response) and strain adjustment (active response). This differs from the usual approach of treating resilience as reliability for large scale, rare events. We further distinguish between resilience and reliability in a completely different way than is usually the case: grid resilience applies to the grid's response to stress up until a break of some kind occurs; the rest falls into the grid reliability category. In this light, the typical reliability measures still make sense: how often failures occur (SAIFI, CAIFI) and how long it takes to recover (SAIDI, CAIDI) fit this definition for both small frequent events and large rare ones. Electric utilities already parse out events in this manner (common small events vs. large rare ones) for reliability metrics reporting anyway. Figure 1 illustrates the Resilience/Reliability Domain concept.

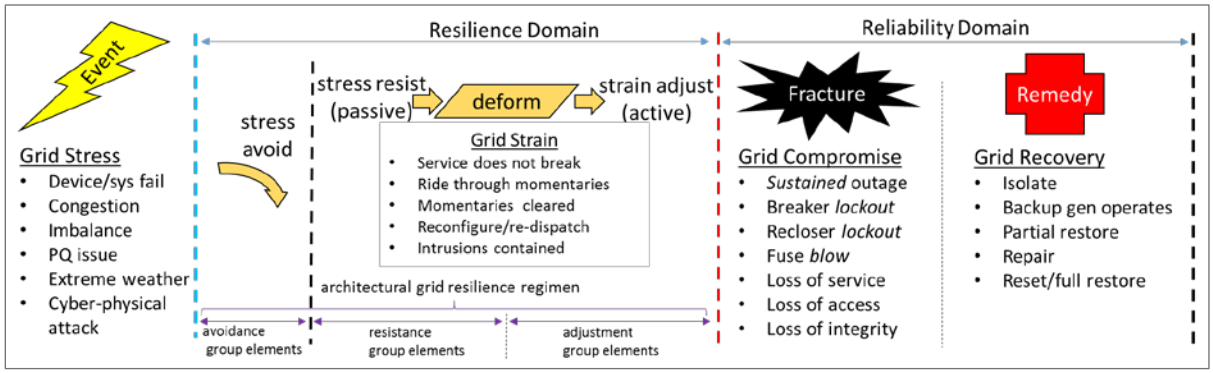

Figure 1. Resilience and Reliability Domains

This definition eliminates the "rare big event" issue and places the conflation of restoration people/processes/resources in the reliability domain, separating that from the inherent issues of grid structure and thereby converting the resilience problem into something more tractable for grid

[1] JD Taft, Electric Grid Resilience and Reliability for Grid Architecture, PNNL, November 2017, available online: https://gridarchitecture.pnnl.gov/media/advanced/Electric_Grid_Resilience_and_Reliability.pdf

architecture purposes. In this approach, the relevant time scales are very much shorter and are related to the transition from the resilience domain to the reliability domain.

Resilience is better understood in terms of *vulnerability to* external events. Events occur when they occur, but vulnerability is an intrinsic characteristic of the grid that can be represented as a part of extended grid state.[2] Vulnerability is a function of grid architecture, design, and implementation, as well as asset condition. Consequently, utilities must deal with grid vulnerability, not just events or contingencies. Events may occur at any time but vulnerability exists continuously.

> Grid resilience should be understood in terms of grid *vulnerability*, not in terms of hypothetical large rare events. This changes the focus from the indeterminate future to the present *because grid vulnerability exists presently*, not at some possible but unlikely future date. Resilience elements comprise countermeasures to grid vulnerabilities.

1.1 More about Stress Avoidance, Stress Resistance, and Strain Adjustment

In order to support practical application of the resilience definition, we further define the three principal elements of the resilience domain.

By viewing resilience in a risk management framework, we can gain insights into resilience and resilience–improving measures. In risk management terms, risk management strategies fall into any of several categories:

- Avoidance – applying safeguards that protect against the risk
- Acceptance – the consequences are known and if the risk is realized will be dealt with
- Transfer – the responsibility for the consequences are transferred to another party
- Mitigation – the impact of the risk is reduced

We shall employ the avoidance, acceptance, and mitigation concepts here.

Stress refers to how a system internally deals with external duress applied to it in terms of something akin to elastic deformation, i.e. the system bends a bit but returns to its original shape when the external disturbance is removed. Alternately we may view it as the buildup of internal forces that resist the external duress. For example, a feedback control system that performs regulation will exert internal control force to maintain its control variable at the regulation set point when a disturbance occurs, applying more control force as needed (up to its limit), and then automatically returning the internal corrective control action (internal force) to its nominal value when the external disturbance abates. A transmission tower will experience the buildup of internal mechanical force in response to wind loading and will return to proper shape if its stress limit is not surpassed. A **stressor** is therefore an external (to the systemic scope being considered – more on that later) source of duress that disturbs system operation, potentially to the point of causing degradation of performance or outright failure.

Stress Avoidance – action on the stressor so that stress on the system does not happen (is avoided). Stress avoidance refers to measures taken to ensure that potential stressors never impact the grid in the first place.

[2] GMLC, Extended Grid State Definition Document, October 2017, work in progress, GMLC Sensing and Measurement Strategy Project. Vulnerability is part of the Asset Condition group.

Examples:

- Vegetation management – removes the stress from vegetation physically contacting the system
- Placement of a flood wall around a nuclear reactor containment building so that tsunami waves do not impact the building
- Animal guards – placement of guards prevents animals from contacting energized conductors and thereby causing a short circuit
- Preventive maintenance – avoids conditions leading to equipment failure (think of as "re-hardening")
- Software containers – allowing email and attachments to be opened only in a safe container (sandbox) so that viruses cannot be accidentally unleashed in an information system
- Equipment placement – avoids contact with a stressor, for example, by placing equipment above high-water mark or below ground, depending on what is appropriate

Stress avoidance may be quantified using the ratio of the number of threat stressors pre-emptively acted against divided by the total number of stressors identified. A more nuanced version that provides some weighting of the stressors could be to use the sums of pre-emptively addressed risks (probability times value at stake) divided by the total sum of risks, but this approach starts to re-blur the line between resilience and reliability that was established by the basic definitions above and so is not preferred. A third option would be to use just the probabilities and not the values at stake, thus avoiding the line blurring problem. Note that in this case a sum of probabilities will not necessarily add to unity.

Stress Resistance – a strengthening (hardening) of the system so that stressors have minimal or no impact on the system and so system operation is not degraded. The stress is effectively absorbed or rebuffed. Stress resistance is a limited mitigation strategy that can be quantified by the amount of "spare" internal capacity for elastic compensation that is available to deal with disturbances. Stress resistance occurs within the bounds of a nominal operating paradigm and with nominal operating parameters and settings and so we may think of it as limited deformation within the elastic bounds of the component or system– removal of the stressor allows the component or system to spring back into shape automatically. In other words, stress resistance is intrinsic to grid structure and normal system function.

Examples:

- Protective enclosures – the system or equipment is shielded from the stressor. The enclosure absorbs the energy of the stress
- Hardening of electronics – adding shielding, thermal management subsystems, and electrical filtering suitable for substations (as opposed to data centers) to substation servers, routers, and Remote Terminal Units
- Wind resistance – increasing wind resistance hardens against tower collapse in severe weather
- EMP/GIC shielding and decoupling – electromagnetic shielding and capacitive decoupling of low frequency/DC currents in transmission systems hardens against EMP and GIC-induced stresses
- Encryption – the difficulty in accessing the protected information is increased

Stress resistance may be quantified by specific measures for each component, subsystem or whole system. For broad applicability across scales, the measure can be expressed as a percentage of a baseline capacity or available control action range. Thus these measures would be dimensionless.

Strain is the change in a system (beyond elastic deformation) that occurs in response to externally applied force or disturbance. The nature of the change may be parametric, structural, or modal. A parametric change would be a new value for a set point, threshold, or other system operating value intended to compensate for a disturbance to limit system degradation. A structural change would be a reconfiguration of a device, circuit, or subsystem (example: isolation of a circuit fault and switching of circuits to re-route power as in FLISR). A modal change would be a switching from one operating paradigm or algorithm to another, again to limit system degradation.

Strain Adjustment – flexibility of the system to adapt to stress. Strain adjustment is a mitigation strategy.

Examples:

- Structural reconfiguration – the distribution system under stress shifts loads from one feeder to another via circuit switching, thus minimizing the impact of the stress on the first feeder
- Load management – stress on the system is reduced by reducing demands via responsive loads
- Rerouting communications – a communication network changes routing tables to alter data flow paths in order to reduce performance degradation due to congestion
- Use of reserves – a bulk energy system uses spinning reserves to compensate for load and generation changes within a given level of operational flexibility
- Modal change – switching the use of storage from augmenting system inertia to shaving peak load in a contingency situation

Note that for strain adjustment it is particularly important to be able to measure the stress and strain on the system.[3]

Strain adjustment may be quantified by the percentage change in nominal operation caused by the strain adjustment. For the circuit fault example, the measure could be the percentage of load maintained (1.0 – fraction of load lost, expressed as a percentage) after the adjustment, based on nominal load before the disturbance. These measures would therefore be dimensionless. The structures of many grid systems are naturally expressed using graph (or network) representation. Electric distribution systems and control system communication networks, for example, are systems that are amenable representation as a set of vertices (or nodes) that are connected by edges (links). Graphs have well defined measures, including some that help to quantify robustness. One may utilize these measures to quantitatively evaluate the resilience of grid systems.

Consider a FLISR-enabled electric distribution network modeled as a graph: edges represent components, such as reclosers, switches and circuit breakers that can be opened or closed; vertices represent the electrical conductors and buses. The state space of such a modeled system represents all combinations of component opened/closed states. One measure of the capacity for strain adjustment of such a system is the size of this state space: a system with a larger state space has a greater capacity to adapt to change than a system with a smaller state space. Other graph/network robustness measures may also be applied to derive specific and quantitative values for resilience that can be used to evaluate the system as its structure changes and evolves over time.

[3] C. Rieger, "Resilient Control Systems Practical Metrics Basis for Defining Mission Impact," INL, August 2014, available online: https://inldigitallibrary.inl.gov/sites/sti/sti/6269308.pdf

2.0 Resilience Element Groups, Resilience Strategy, and Element Allocation

We recognize two groups of architectural resilience elements: stress resistance elements and strain adjustment elements. By classifying elements this way, the process of selecting which to apply can proceed by first developing a resilience strategy, followed by allocation of resilience elements from the two element groups, as indicated by the strategy. Figure 2 illustrates the general process flow.

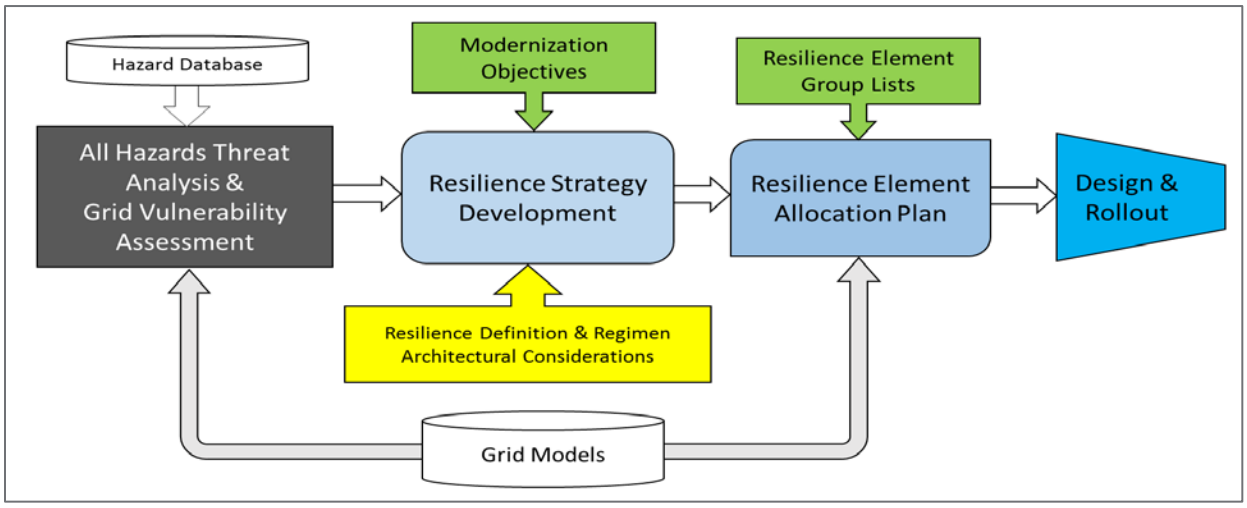

Figure 2. Resilience Strategy and Element Allocation Process

2.1 The Tension Between Grid Stress Resistance and Grid Strain Adjustment Approaches

On this basis, we can start to consider and classify approaches and concrete measures that would reduce grid vulnerability by improving resilience. In doing so, we may encounter a tension between grid resistance to stress (hardness, but more than that) and grid adjustment to strain (accommodating the impact of stress to limit degradation). A key decision (or set of decisions) involves determining how much stress avoidance or resistance to incorporate and how much capacity for strain adjustment to implement. The strategic decision about this should be made at the resilience strategy development step to set the stage for the creation of the resilience element allocation plan, but explicit selections will still have to be made at the allocation stage. This is specific to any particular grid and utility.

An example of the tension in these three resilience countermeasure group choices is system inertia. For the purposes of resisting stress, we may want a large amount of inertia (for stability), whereas for the purpose of accommodating strain we may want very little (to be agile). It may be necessary to consider other factors to resolve such choices when an element may be related to multiple resilience element groups.

See Appendix B–Appendix D for classifications of resilience principles, architectural elements, and communication network security measures according to the resilience regimen described above.

3.0 Characterizing Resilience

Due to the multi-dimensional nature of grid resilience, any approach to characterizing it must be composed of multiple components. To identify these, we must be clear on the scope of grid resilience. In Figure 1, we list a number of grid stressors:

- Exogenous impacts such as tree taps or vehicle damage
- Device/sub-system/system failure or fatigue
- Transmission congestion
- System imbalance
- Power Quality disturbances
- Extreme weather, including GIC
- Cyber-physical attack, including EMP

In addition, we consider such stressors as:

- Distribution circuit constraint violations (thermal, voltage, protection)
- Communication network congestion and performance constraints vs. increasing data flow
- Accidental damage (cutting optical fiber during construction, etc.)
- Changes in fuel availability for generation
- Changes in water availability for cooling

We also include stressors related to operational issues and non-circuit exogenous forces:

- Integration of new systems or capabilities and/or third party ESOs
- Impact of software upgrades
- Operator errors and errors in configurations
- Changing requirements due to new regulations and/or social issues
- Impact of unevenly distributed and increasing connection of non-utility responsive/interactive devices and systems to the grid

3.1 Systemic Scope (Scale)

Resilience and reliability both must be considered in terms of systemic scale. This means that the concepts of Resilience Domain and Reliability Domain can and should be applied at various scales, from single device to whole grid interconnections and at all levels in between. For example, if a single device fails, it enters the Reliability Domain. The circuit or system to which it is attached may stay in the Resilience Domain or may enter the Reliability Domain depending on the consequences of the device failure and the grid reaction to it.

Example: a fault occurs in a section of a partially-meshed distribution feeder. A FLISR[1] system isolates the faulted section and performs line switching to quickly (definition of "quickly" depends on the utility involved) restore power to all of the feeder but the faulted section. In such a case, the faulted section has entered the Reliability Domain, but the rest of the feeder has remained in the Resilience domain.

This concept also resolves a potential ambiguity in the definition of a stressor. When a component fails, it become as stressor on the sub-system to which it belongs and therefore to the whole system. The concept may be viewed as a reverse recursion in that failure of a sub-system becomes a stressor on the whole system. However, when considering the failed component, some stressor (current overload, ice buildup, degradation through aging, etc.) has to have caused the component failure. In the case of a cascading failure (component fails → sub-system fails → system fails), we may view the stressor that caused the original component failure to be the root stressor.

The systemic scope concept must be applied in this manner generally, otherwise it will not be possible to separate resilience from reliability, which would defeat the entire purpose of creating the new definitions. We also need the concept of systemic scope to properly define resilience measures.

3.2 Temporal Scope

For electricity delivery, the start of a sustained outage is the transition point from the domain of resilience to the domain of reliability. Thus momentaries are *power quality* issues that stress the grid and therefore are part of the resilience domain. However, the definition of the time span of a momentary can vary from utility to utility. This is perfectly fine; it means that the boundary between resilience domain and reliability domain is determined by each utility in an appropriate manner, thus requiring no changes to reliability metrics.

The combination of the concepts of systemic scope and temporal scope provide the means to resolve classification issues without the need to resort to non-deterministic methods.

3.3 Resilience Measures

Resilience measures are divided into three groups by regimen: those that apply to stress avoidance, those that apply to resistance, and those that apply to strain adjustment.

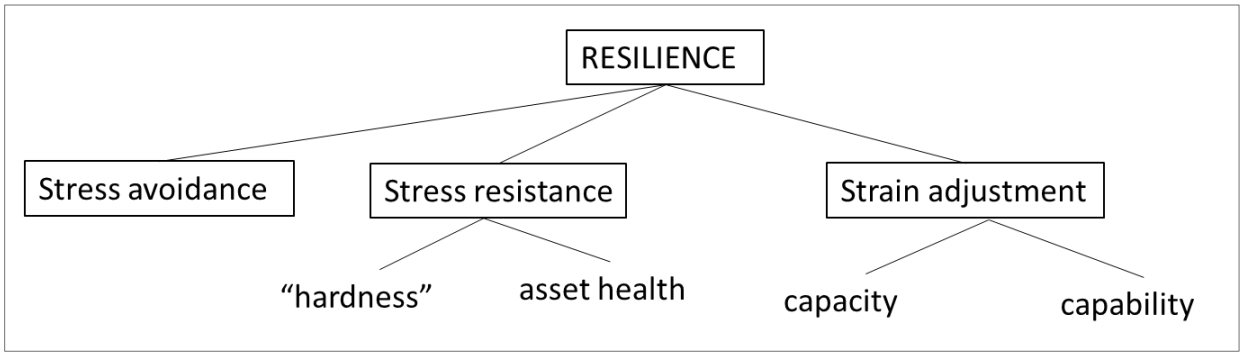

Figure 3. Resilience Groups and Sub-Groups

[1] Fault Location, Isolation, and Service Restoration

All resilience elements have the characteristic of mitigating one or more vulnerabilities. Table 1 clarifies the nature of the mitigations for the three primary resilience groups.

Table 1. Resilience Group Characteristics

Stress Avoidance	Stress Resistance	Stress Adjustment
Preventative action	Supports normal operation mode	Planned response outside of normal mode of operation
Ancillary to operational components and structures	Operational components and structures unaltered	Exercises alternative operational structure or configuration
	Normal coordination-control-decision process	Corrective action coordination-control-decision process
	Sustains economic or other operational objectives-based decisions	Impacts economic or other operational objectives- decisions

Figure 3 extends the classifications to sub-groups for resistance and adjustment in a manner that is helpful in developing ways to quantify the impact of resilience measures.

Table 2. Resilience Groups and Sub-Groups

Resilience Group and Sub-group	Comments
Stress Avoidance	Prevention of stress events from occurring in the first place
Stress Resistance Asset/sub-system/system hardness	Inherent strength; how much stress can be applied before a component or system begins to yield (degrade performance) (analogous to yield point: amount of stress that can be applied before transition from elastic to plastic deformation)
Stress Resistance Asset/sub-system/system health	Ability to accept rated load (power, data flow, computational burden, etc.) without degradation of operation or excessive loss of life
Stress Adjustment Adjustment capacity	Reserve ability to handle stress that may arise (e.g. generation flexibility)
Stress Adjustment Adjustment capability	Ability of a grid to actually use available compensation capacities – this implies functioning mechanisms to invoke and control whatever capacities are present and useable

Unlike traditional measures of resilience that focus on the amount of damage that is done by external events or the time to recover, these characterizations suggest norms that focus on intrinsic grid characteristics. The measures of these factors must be consistent with good practices in the creation of proper metrics and norms.[2]

[2] See Appendix A.

3.4 Foundational Support for Resilience

A number of capabilities or measures are needed to support all of the resilience groups outlined above. One practical way to recognize these is when they apply to all three resilience groups. Table 3 lists some key foundational elements.

Table 3. Resilience Foundational Elements

Foundational Resilience Element	Description/Comments
Situational Awareness	All of the groups and the measures that fall within them require some form of situational awareness, whether in the form of real time sensing and measurement or knowledge of system vulnerabilities and stressor impacts (either forecasted or determined after the fact)
Planning/Design for Resilience	None of the resilience measures happens by accident or can be relied upon to emerge spontaneously from other aspects of grid architecture and so must be planned and designed in. Planning includes development of a resilience strategy; design includes allocation of resilience measures.
Interoperability	While possibly viewable as a resilience measure for IT systems, in the larger sense this applies to all sorts of interconnection issues, including mechanical, electrical, communication, control, coordination, and data/information exchange interconnections and so applies not just to IT systems but to general grid codes/interconnection agreement issues

4.0 Final Comments

We have defined grid resilience with a broad scope in terms of hazards to grid operation and grid vulnerabilities, but have separated out the external events from intrinsic grid characteristics in order to get at architectural issues. The scope includes not just hazards to the physical grid and not just cyber-physical vulnerabilities, but also hazards that come about from changing requirements and other exogenous forces, as well as operational issues like system upgrades, maintenance, operator error, and configuration errors.

By separating out issues as we have, it is possible to classify resilience improvement options into three categories: stress avoidance, stress resistance, and strain compensation. Doing so facilitates the development of a resilience strategy, followed by a resilience element allocation plan. Using these definitions will assist utilities and regulators in sorting out priorities, strategies, and action plans for improvement of grid resilience.

Appendix A

Metrics and Norms

Appendix A

Metrics and Norms

Common terminology for performance measures is “metrics.” This is an unfortunate choice from a rigor standpoint, but it is widely used and should not think we will change the usage in the utility industry. For our purposes however, we must adopt somewhat more rigor in terminology, as well as practice.

Some utility “metrics” actually measure the opposite of what they are supposed to measure. A good example is the set of reliability metrics commonly used in the electric power industry. Most of these reliability “metrics” actually measure unreliability.

Properly speaking, what we want for most of our purposes are norms, in the terminology of abstract mathematical spaces.

- Norms measure the “size” of a thing
- Metrics measure the “distance” between two things
- Norms are said to induce metrics

We want the definitions of resilience measures to be as nearly orthogonal as possible, so in practice we should define them in an inner product space. Underlying this space we need a basis that lets us define norms in terms of two key parameters: time and extent (systemic or geospatial).

Appendix B

Regimen Classification: Resilience Concepts/Principles

Appendix B

Regimen Classification: Resilience Concepts/Principles

Stress Avoidance	Stress Resistance	Strain Adjustment
Maintenance	component/system/structure hardening	ULS normal failures approach
Positioning	system stability (operational)	system agility (operational)
Design for avoidance of stress (high-water example)	buffering	redundancy
Stress detection (enables “block and shield”)	structural hardness	sectionalizing/partitioning/separating
Extensibility (functional)		configurability
		adaptive hardening
		adaptive operations
		graceful degradation

Appendix C

Regimen Classification: Grid Architecture Elements

Appendix C

Regimen Classification: Grid Architecture Elements

Stress Avoidance	Stress Resistance	Strain Adjustment
Fuel stockpiling	redundancy	energy resource flexibility
Modularity and (de)coupling	component backups/no critical SPF	net load flexibility (behind the meter)
Interface standards	core/edge structure	reconfigurable power circuits along with associated control regimes
Interconnection standards	layering & platforms	reconfigurable communication networks
Maintenance – preventive and information driven	laminar networks	low tech backups – manual/electromechanical PAC
Equipment certification and testing	grid energy storage	distributed architectures: coord, PAC, data/analytics
Monitoring (e.g., perimeter, equipment, etc.)		parametric adaptation (fast)
Improved prediction of exogenous factors like weather and loads		structural adaptation (slow)
		operational mode adaptation

Appendix D

Regimen Classification: Communication Network Security Measures

Appendix D

Regimen Classification: Communication Network Security Measures

Stress Avoidance	Stress Resistance	Strain Adjustment
Honeypots	Crypto: link layer, group, and application layer	Rate limiting for DOS attacks
Air gaps (physical network isolation, data diodes)	RBAC (RADIUS and TACACS; AAA; NAC)	Wire speed behavioral security enforcement
Secure code development (against buffer overflow, self-modification; remove unnecessary protocols)	Mutual authentication; EAP and media independent identity protocols	Packet tamper detection
Manufacturing supply chain security management	X.509, secure key generation and management, scalable key management	SUDI 802.1AR (secure device identity)
	Firewalls	SIEM
	IPS, including SCADA IPS signatures	Storm detection and traffic flow control: traffic policing and port blocking
	Containment: Virtualization and Segmentation (VRF – virtual routing and forwarding, MPLS VPN and VLAN); data separation	ARP inspection; DHCP snooping
	Tamper resistant device design, digitally signed firmware images, firmware/patch authentication and integrity verification	Control plane protection (coarse packet classification, VRF-aware control plane policing)
	Digitally signed commands	MAC layer monitoring
	Unicast reverse path forwarding (IP address spoofing prevention)	ARP inspection; DHCP snooping
	Code hardening (against buffer overflow, self-modification; remove unnecessary protocols)	Access detection and mitigation (i.e. port shutdown
	Six wall physical security for devices and systems	Data quality as tamper detection
	Anti-counterfeit measures	Threat manager systems
	Unicast reverse path forwarding (IP address spoofing prevention)	Security policy manager systems (some functions)
	Security policy manager systems (some functions)	Adaptive security posture
	Hierarchical QoS	
	Access control: VLANs, ports	

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99352
1-888-375-PNNL (7665)

http://gridmodernization.labworks.org/