An Energy-Efficiency Workshop and Exposition

Orlando, Florida

High-Availability Combined Heat and Power Systems for Critical Federal Facilities

Achieving Energy Security through Distributed Energy Resources

Whit Allen
Vice President
Sure Power Corporation
whitallen@surepowersystem.com
+1 (203) 790-8996 x16

Securing Key Infrastructure

- Post 9/11 Initiatives to Secure Key Components
  - Private Sector
    - Banking & Finance, Transportation, Oil & Gas, Information
  - Public Sector
    - Government Services, Health Services, Law Enforcement
- Top-down Approach: Backbone-level Systems
  - Highways, grids, pipelines, airports, communications
  - Focus on physical protection, manpower issues
- Supporting Assets Addressed as Afterthought
  - And no difference between concrete and reliable power

Communication Infrastructures

- By Contrast, Datacom Addressed Like Y2K
  - Recognized to be distributed, granular & ubiquitous
  - Executive Order issued immediately after 9/11
    - Business, government and defense depend on information
    - Protection program to secure critical information infrastructure
- Missing is a Y2K-like Perspective on Power
  - Electricity is the critical fuel of information infrastructure
  - Electrons are actually more essential than bits & bytes
    - They control electronically-operated analog infrastructure, too
    - Local power failures can propagate to cause widespread disruption
    - Line between physical and cyber blurred by digital control systems

Critical Power Infrastructure

- "Blue Cascades" Project
  - Federal, state and Canadian authorities
  - Boeing, Pacific Gas & Electric, Verizon, Qwest
  - Simulated terrorist attack on Northwest power grid
    - Attack could wreak havoc on nation's economy
    - Shutting down power and productivity in domino effect for weeks
- Critical Power is Highly Distributed, Multi-Tiered
  - Power is critical wherever it fuels a critical load
    - Nodes as large as a military base or small as a single pipeline valve
    - Some must be robust to run autonomously for weeks or longer
  - Neither feasible nor economic to harden public grid
- Responsibility falls on sector that owns nodes

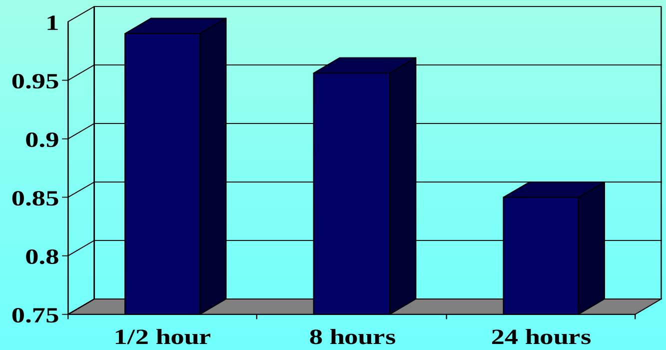
Shortcomings of Backup Power

Many Recognize Critical Importance of Power

- Military, telecom, hospitals, financial institutions
- Traditional protection involves emergency generators

However, Intended Only for Intermittent Use

- Best maintained fail to run for 24 hours 15% of the time
- Long-duration event beyond the ability of most to cope



Reliability of Emergency Diesel Generators

Source: *Emergency Diesel Engine Generator Power System Reliability* 1987-1993
Grant, G.M., et. al.,
Idaho National Engineering Laboratory
INEL-95/0035, February 1996

Distributed Generation (DG)

Power Generation at the Point of Use

- Eliminates reliance on vulnerable utility grid
- Ensures public service during sabotage or accidents

Variety of DG Technologies (and fuels) Available

- Reciprocating engines (natural gas, diesel, biofuels)
- Turbines (natural gas, steam, wind)
- Fuel Cells (natural gas, digester gas, hydrogen)
- Photovoltaics

Combined Heat & Power (CHP)

- Increases energy efficiency / reduces energy usage
- Reduces greenhouse gas emissions

Centralized vs. Distributed Energy

Central Utility Grid

- Large components far from uses
- Vulnerable to widespread failure
  - Miles of unprotected transmission lines
  - Dependence on just a few critical links and nodes

Distributed Energy Resources

- Redundant sources located at the point-of-use
- Short, protected connections to the load
- Can be designed to be extremely fault tolerant
  - Multiple paths for electricity to reach the consumer
  - No single component or link could cause disruption
- Multiple, small systems less attractive for saboteurs

Obstacles to Implementation

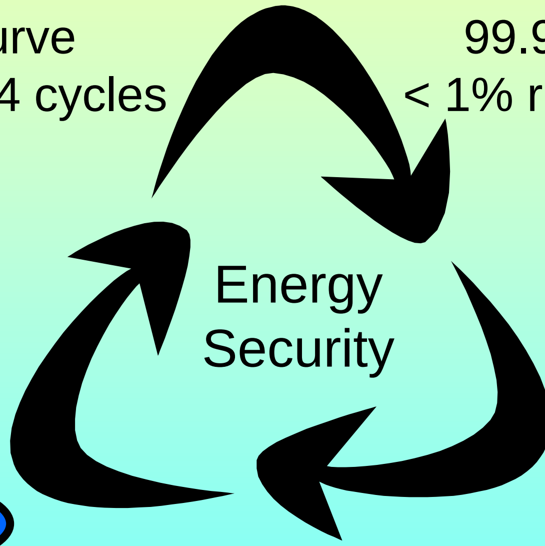
- Grid Interconnection
  - AC interconnection is an issue with many utilities
- Economics
  - Gas vs. Electric "spark spread" operating cost
  - Prime mover capital costs and standby backup charges
- Reliability
  - The best DG units are still only 96% available
  - Synchronization and interdependence issues
- Adaptability
  - Modularity and scaleability
  - Not core competency of facility managers

Critical Facility Requirements

Power Quality and Availability

CBEMA curve
< 20% sag for 4 cycles

99.9999% availability
< 1% risk of failure (20 yrs)



Environment

Low Emissions (NO_X, CO_2)
Energy Efficiency

Economics

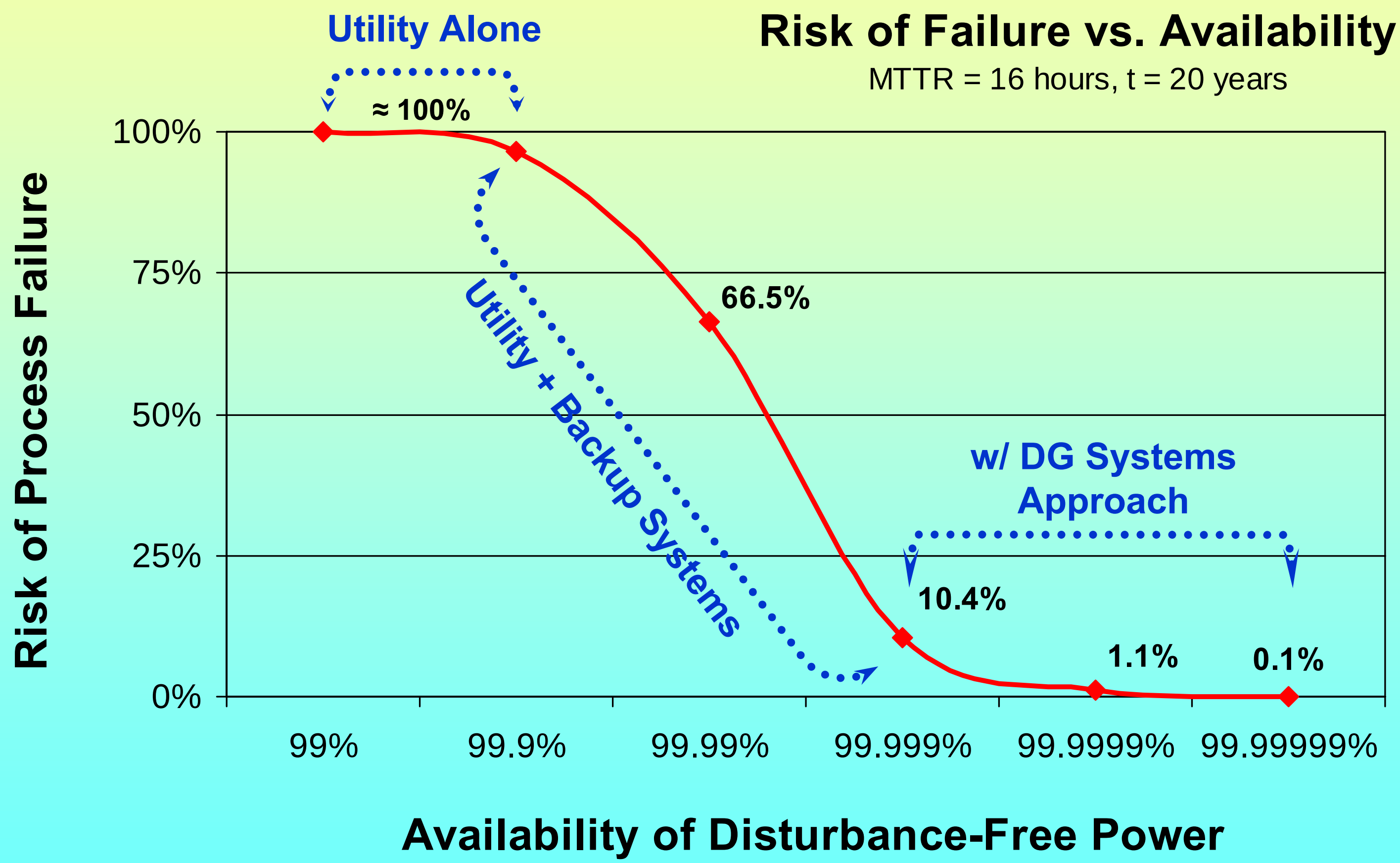
↓ Capital expense
↓ Operating expense

Myth of the "Nines"

(Number of hours in a year) X (unavailability) = downtime

Nines	Availability	Unavailability	Downtime	
"one nine"	90%	10%	876	hours
"two nines"	99%	1%	87.6	hours
"three nines"	99.9%	1.0.E-3	8.76	hours
"four nines"	99.99%	1.0.E-4	53	minutes
"five nines"	99.999%	1.0.E-5	5.3	minutes
"six nines"	99.9999%	1.0.E-6	32	seconds

Risk of Failure Comparison



So Where Does DG Make Sense?

<u>Sure Power's Thesis</u>

DG makes sense where:

1) Serious consequences occur when a critical system experiences a one-second power deviation; and

2) The cost of a traditional grid + backup system, normally purchased to protect the critical system, would pay for a high availability DG system

Systems Approach Required

Probabilistic Risk Assessment (PRA)

- Components can be modeled in a complex system
- Formal, defensible, reviewable design process

Allow service without power disruption to load

- Repair, maintenance, failure, growth, reduction, etc.

Eliminate cascade and single points of failure

Address real world common-cause limits

- Become dominant when unavailability reaches 10^{-6}
- Simple is better than complex

Benefits of Systems Approach

- Increased availability, lower chance of failure
  - compared to conventional systems (1% vs. 67%)
- Economic value
  - both capital costs and operating costs
  - lower losses, greater efficiency, spark gap opportunities
- Environmental leadership
  - reducing greenhouse gas emissions
- Modularity
  - allows customers to better match expense to real load
- Space savings
  - compared to conventional approaches

You can download a white paper with more detailed information on power quality, reliability, availability and the risk of failure:

"Power Impacts on the Cost of Risk – Tools for Championing Power Quality and Reliability Initiatives from a Risk Management Perspective"
http://www.surepowersystem.com/pdf/power_impacts_on_cost_of_risk.pdf

Thank you.
Questions?

Whit Allen
Vice President
Sure Power Corporation
whitallen@surepowersystem.com
+1 (203) 790-8996 x16

An Energy-Efficiency Workshop and Exposition

Orlando, Florida

Whit Allen:

Question on reliability versus risk (probability) of failure.

Consequences of Power Event

Damage function models have changed

- Industrial Age
  - time of power outage = business downtime

    i.e. *(5-minute)* power <u>outage</u> = *(5-minute)* business <u>downtime</u>
- Internet Age
  - short power fluctuation = long business downtime

    i.e. *(4-cycle)* voltage <u>sag</u> = *(32-hour)* business <u>downtime</u>

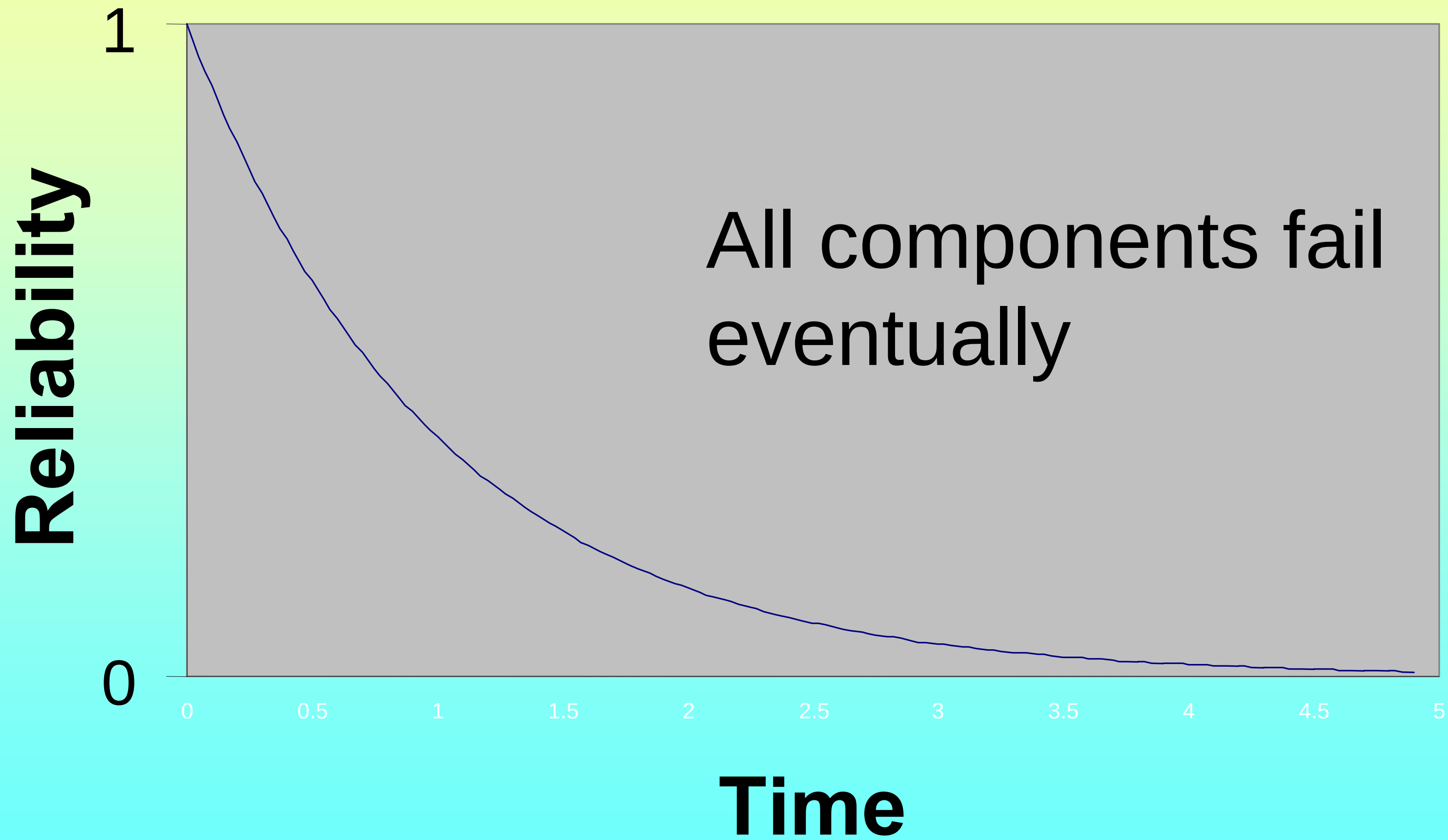
INDUSTRY EXAMPLE	**ELECTRICITY TOLERANCE**	**MTTR[2] OPERATIONS**
Data Center	.008 seconds / CBEMA curve	16 hours[3]
Semiconductor Manufacturing	20% voltage sag for (4) cycles	32 hours

Reliability as Measurement Tool

The probability that a system or component will operate for a given time

- can be function of time, events, environment
- Reliability tends towards 0 (all things fail)
- $R = 1 - P_f$ (Probability of Failure)
- most useful for analysis of missions during which equipment may not be repaired
- mission length must be known
- Failure rate λ expressed in failures/hour (simplified concept for calculations; most items wear and do not have constant failure rates)
- Mean time to failure MTTF = $1/\lambda$
- $R = e^{-\lambda t}$, $P_f = 1-e^{-\lambda t}$

Reliability w/ Constant Failure Rate



Availability as Measurement Tool

Probability that a system will function at a future instant in time

- most useful in analysis of repairable systems
- does not require defined mission length
- described in "9s" i.e. 0.999 or 99.9% = three "9s"
- constant rate of repair is assumed (easy to calculate)
- rate of repair μ expressed in repairs per hour
- Mean Time to Repair MTTR = $1/\mu$
- A = MTTF / (MTTF + MTTR), $A = \mu / (\lambda + \mu)$
- $U = 1 - A$, $U = \lambda / (\mu + \lambda)$ [U is more useful when $A \approx 1$]
- MTTF + MTTR = MTBF = Mean Time Between Failure

Calculating Power Risk

For a given availability, find probability of failure:

- $U = 1 - A$, $U = \lambda / (\mu + \lambda)$, solve for λ
- $P_f = 1 - e^{-\lambda t}$, where t = mission length

Data center backup power system (2N) example:

- 99.99% availability, $A = .9999$, $U = .0001$
- 20-year mission, $t = 20 * 8{,}760$ hours
- MTTR = 16 hours, $\mu = 0.0625$ per hour
- $P_f = 66.5\%$

One System Example