Approaches to Minimize Murphy's Law Impact On "No single point of failure power supply systems."

Marian Bulancea
Engineering
Kepco Inc.
Flushing,USA
mbulancea@kepcopower.com

***Abstract*—Considering Murphy's law, "If anything can possibly go wrong, it will, and at the worst possible time", there is a myriad of problems which need to be solved by" No single point of failure power supply systems" by designers, integrators and users. The paper covers factors to be considered in design, installation and maintenance in context of 30+years of experience and lesson learned approach to building redundant, fail-safe power supplies for mission critical applications. Aspects explored are output redundancy, input redundancy, programming and I/O fail safe and overcoming environment challenges. These environmental challenges include methods for deploying fault tolerant systems in high temperature, wet, dirty, corrosive and explosive applications.**

Keywords—Fault tolerance, Fault tolerant control, Redundancy, Hot-Swap, Load Sharing

I. INTRODUCTION

The Murphy' Law states that "If anything can possibly go wrong, it will, and at the worst possible time". There are countless examples of it in today's culture which have been accepted throughout the world: for instance, that toast will always land butter-side down when dropped or that will begin to rain as soon as you wash your car.. Murphy's Law has been found to be highly relevant to hardware/software testing and many other types of engineering discipline.

Originated in the late 1940's, in a twist of fate Murphy's Law coincided with the founding of the Kepco power supplies company. The roots of Murphy's law were related to the military MX981 Project in the Mojave Desert (Edwards AFB) and what triggered the famous adage was the failure of strain gages. Kepco's inception was related to ideas initiated on the Manhattan Project at Los Alamos by Kepco's founders which led to pioneering discrete designs of operational power supplies. Kepco introduced a few concepts to serve multiple demanding applications, including Series KG, for precise strain gages.

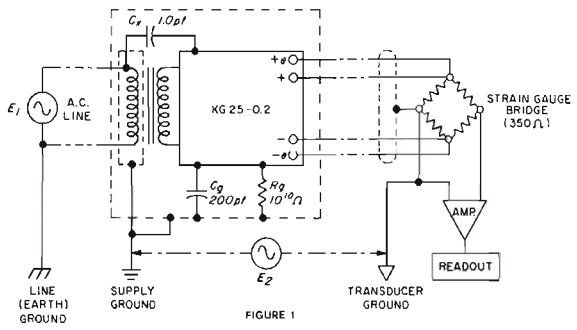
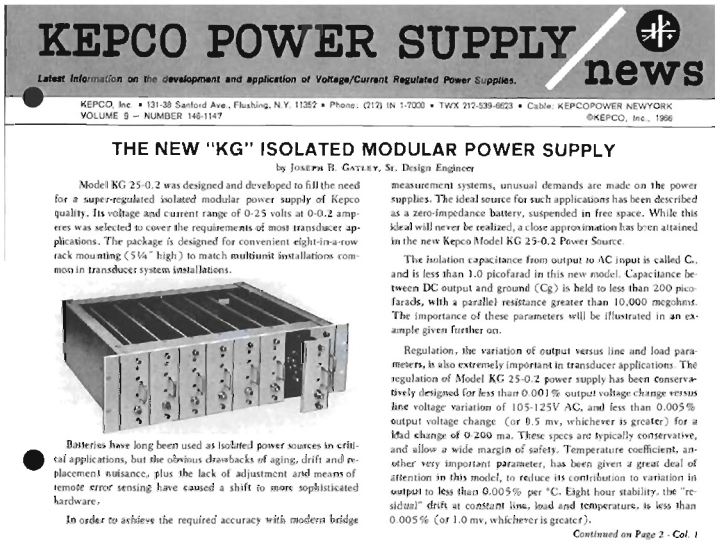


Fig. 1. Block diagram of Kepco's "KG" series, overall stability 50ppm.



KEPCO POWER SUPPLY news

Latest information on the development and application of Voltage/Current Regulated Power Supplies.

KEPCO, Inc. • 131-38 Sanford Ave., Flushing, N.Y. 11352 • Phone: (212) IN 1-7000 • TWX 212-539-6623 • Cable: KEPCOPOWER NEWYORK
VOLUME 9 – NUMBER 148-1147 ©KEPCO, Inc., 1966

THE NEW "KG" ISOLATED MODULAR POWER SUPPLY

by JOSEPH B. GATLEY, Sr. Design Engineer

Model KG 25-0.2 was designed and developed to fill the need for a super-regulated isolated modular power supply of Kepco quality. Its voltage and current range of 0-25 volts at 0-0.2 amperes was selected to cover the requirements of most transducer applications. The package is designed for convenient eight-in-a-row rack mounting (5¼" high) to match multiunit installations common in transducer system installations.

Batteries have long been used as isolated power sources in critical applications, but the obvious drawbacks of aging, drift and replacement nuisance, plus the lack of adjustment and means of remote error sensing have caused a shift to more sophisticated hardware.

In order to achieve the required accuracy with modern bridge measurement systems, unusual demands are made on the power supplies. The ideal source for such applications has been described as a zero-impedance battery, suspended in free space. While this ideal will never be realized, a close approximation has been attained in the new Kepco Model KG 25-0.2 Power Source.

The isolation capacitance from output to AC input is called C_i, and is less than 1.0 picofarad in this new model. Capacitance between DC output and ground (C_g) is held to less than 200 picofarads, with a parallel resistance greater than 10,000 megohms. The importance of these parameters will be illustrated in an example given further on.

Regulation, the variation of output versus line and load parameters, is also extremely important in transducer applications. The regulation of Model KG 25-0.2 power supply has been conservatively designed for less than 0.001% output voltage change versus line voltage variation of 105-125V AC, and less than 0.005% output voltage change (or 0.5 mv, whichever is greater) for a load change of 0-200 ma. These specs are typically conservative, and allow a wide margin of safety. Temperature coefficient, another very important parameter, has been given a great deal of attention in this model, to reduce its contribution to variation in output to less than 0.005% per °C. Eight hour stability, the "residual" drift at constant line, load and temperature, is less than 0.005% (or 1.0 mv, whichever is greater).

Continued on Page 2 - Col. 1

Fig. 2. Critical application redundant system with KG series 1966 [1]

In time this trend evolved, resulting in today's reliable power supplies such as Kepco's Series as HSP, HSF, and KHX, serving mission critical, no single point of failure, systems applications drawing upon expertise gained with earlier precise designs such as KG, but sharing such common roots as pluggability and redundancy.

Fig. 3. Redundant,hot-swap,fault tolerant,universal input HSP series [2]

For the past half century Kepco has been challenged to design power systems for critical applications, building expertise proven by analytical design, real events and lessons learned. A Murphy's Law event occurred in New York City on 9/11/2001 when the North World Trade Center tower was hit by a hijacked airplane at 8:46am. None of the sophisticated alarm reporting system installed in the building worked in spite of redundancy, because not only was some of internal power lost,

but as Murphy's Law predicted in its pessimistic tone, the tower with the communication antenna was hit first.

Fortunately, help for saving additional lives was initiated only a minute later at 8:47am from the ERS (Emergency Reporting System) Red Fire Box 8087 [3]. The first alarm came via the New York City Fire department (FDNY) intercom fire box (red box) system built by Norelco, and powered, since the early 1970's, by a simple and efficient design using Kepco operational power supplies. These cabinet-mounted supplies were naturally convection cooled, modular, and redundant. A current-stabilized system output utilized output modulation for intercom communication; it was designed to survive environmental challenges such as short circuits; noise pickup from grid cabling and insect nests built in conduits.

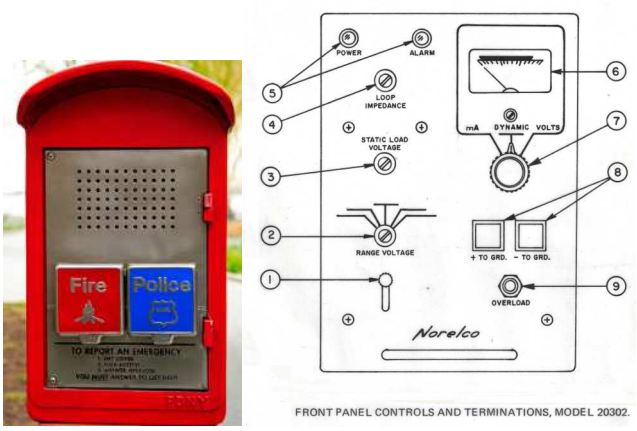


Fig. 4. FDNY fire box (left) powered by Kepco special supply OEM built.

Murphy's Law came calling again two years later and the same system of FDNY red boxes proved vital in responding to emergencies during the Northeast blackout of 2003 when most other forms of communications were cut off.

This caused the FDNY to acknowledge the mission critical aspect of this system, with the result that plans to obsolete this system were dropped and in response, an improvement was ordered based on another modular; hot-swap; redundant power supply, Kepco's series MST.

Fig. 5. Today's power for FDNY boxes is provided by Kepco's MST [4]

The upgrade was rolled since 2005 and works well today powering the second most common method of contacting the world's second largest fire department.

II. MISSION CRITICAL SYSTEMS EVOLUTION

Years ago, considering only compliance with mandatory safety standards or publishing calculated MTBF by common methods of computing reliability from Mil Hdbk 217 [5] were considered sufficient for a good design.

KEPCO noted that in the earlier years designs for compliance with only these basic requirements in mind contributed to increased chances of Murphy's law occurring. When power supply systems were designed with little or no thought to business continuity, equipment protection against surges and other ongoing power disturbances issues, Murphy's Law came quickly into action causing undesired equipment responses, degradation in performance specifications and ultimately, failures and outages.

During development of power supplies for critical applications in the early 1990's, the concept of industrial control systems based on triple modular redundancy applied to industrial safety-shutdown technology emerged. Interacting with customers and analyzing different applications using the same model series, significant differences in application brought home the fact that there was a need to alter the "one size fits all" approach and the realization that a power supply system must not have a single point of failure.

Since Murphy's Law tells us that if something can go wrong, then it will go wrong, it's up to us as designers to prepare ourselves for events and challenges faced by designs of critical systems. As a result of the unforeseen environmental disasters of Katrina and Sandy, the National Electrical Code added the mission critical systems classification to critical industries and locations since 2008. It was discovered soon after that mission critical power systems were not affected only by traditional ground environments or acts of nature, but from new challenges related to modern digital means of system control. Threats in the form of cyber-attacks, with their latest neologisms such as cybernetic war, malware, hacking, ransomware, etc. forced a higher degree of anticipation on what can go wrong from integrators, designers, users, plant maintenance and responsible parties. It forced analysis of mission critical systems from both components /parts level and as a system whole.

This allow us be cognizant of the failure possibilities and on the time scale to be prepared for that "worst" possible time. Creating a system for high availability is a continuous challenge, not only because the safety standards demands have increased, but also because it is necessary for designs to evolve based on observed failures and incorporate the lesson learned.

Why is high availability important for a mission critical system?

Besides ensuring the safety of personnel and of the buildings housing the equipment, fail safe is a must in an explosion-proof environment so that 100% availability also becomes a goal of mission critical systems. These are systems where no single point of failure can be allowed to exist. Because system availability has a direct impact on profit and a company's financial health, availability is commonly used as a key business metric in production-heavy organizations.

When equipment is running as much as possible, productivity increases and so do revenues. This means that failure of a system intended to be highly available affects not only a few hours of factory output which was supposed to produce non-stop, but also adversely affects the bottom line.

Power system failures may have a huge impact and cause damage to other equipment or ripple consequences into plant infrastructure (Murphy's Law again). In cases where a system fails to provide power to process sensors, safety shutdown valves, or other critical monitoring instruments, the result may be disabled sections of factories or a halt to a serial production flow. This is disastrous for products that may solidify in storage tanks or mixers; once that happen for products like cement, thermoplastic and thermoset resins ,the cost of clearing the pipelines may be enormous. In most instances plant idling or a large shift from normal plant operating parameters not only stops revenue but induces intolerable stress into the plant equipment. Thermal stress on equipment operating for years at high temperatures that is suddenly reduced, coming down to ambient levels, affects seals and gaskets, puts additional stress on bolts and flanges and can stress pipes to fracture.

Figure 6 below present architecture for a power mission critical system designed for high availability. Challenges of such mission critical power system include

- No single point of failure design

- Redundancy on Input and Output,

- Fault tolerant controls

- Independence of digital control and bus with options of analog control only or auto-switch to analog control in the case of digital control failure due to hacking or industrial process control computer failure.

The depicted system operates with triple redundancy on input power, on DC to sustain a failure of one of the AC/DC modules as well as survive a control system failure. This is in parallel with other simultaneous challenges, such as load short circuits, remote error sense failures or current share bus failures. It shows the need for N+2 redundancy for a minimum check list Murphy's law contingencies and explains why such systems increase in complexity, cost and size.

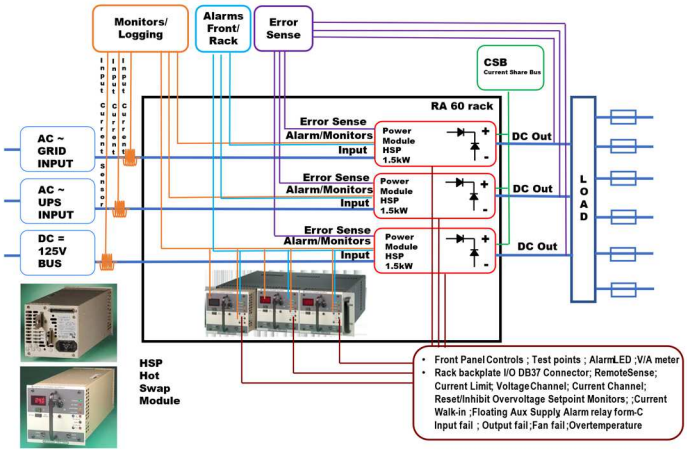


Fig. 6. Mission critical power system with high availabilty. [6]

III. CHARACTERISTICS OF CRITICAL SYSTEMS

"RAMSS" ACRONYM: RELIABILITY; AVAILABILITY; MANAGEABILTYSAFETY; SERVICIABILITY

RAMSS encompass five inter-related characteristics of a mission critical system. Originated by IBM as RAS (reliability, availability, and serviceability) for data processing machines, the concept was later updated with additional attributes to serve critical application analysis for systems and components [7]. Considering these attributes and their interactions and how to incorporate them into product life will yield increased availability to the mission critical system.

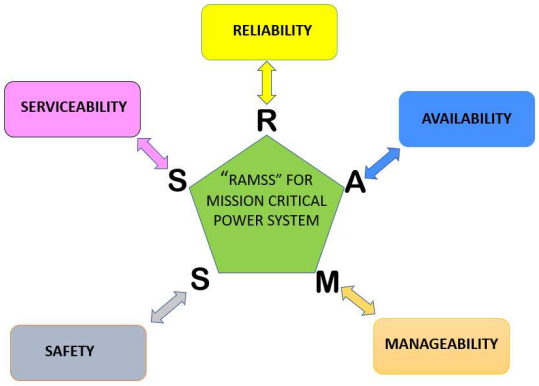


Fig. 7. Mission Critical System characteristics interdependence. [8]

1) RELIABILITY

Reliability refers to the probability that the system will meet certain performance standards and yielding correct output for a desired time duration.

$$R(t)=e^{-\text{time}/MTBF}=e^{-\lambda t} \qquad (1)$$

where: time = Mission Time, duration [hr.]

MTBF= mean time between failures is the average (expected) time between two successive failures of a component. [hr.]

$$MTBF=\frac{1}{\lambda} \quad MTBF=\frac{Total\ Operating\ time}{Number\ of\ failures}\ [\text{hr.}] \qquad (2)$$

λ=failure rate also known as FIT=failures in time

$$\lambda\text{=failure rate} \quad \lambda=\frac{Number\ of\ failures}{Total\ Operating\ time}\ [1/\text{hr.}] \qquad (3)$$

Reliability is dependent on MTBF, but MTBF does not mean average life or expected life, or alike. Applying in (1) MTBF and mission time show the probability of a unit working during a mission time smaller or larger than MTBF.

TABLE I. PROBABILITY OF UNIT WORKING IN TIME

Mission Time	Probability of units working
0.1*MTBF	90 %
1*MTBF	37 %
2*MTBF	13 %

The probability of failure represents the risk of failure and can be used to help plan for the number of spares needed to achieve ideal availability.

2) AVAILABILITY

Availability is the percentage of time when that system is operational.

MTTR = mean time to repair or recover from failure [hrs.]

$$MTTR = \frac{Total\ Downtime}{Number\ of\ Failures\ `} \quad [\text{hrs.}] \qquad (4)$$

$$A = \frac{MTBF}{MTBF+MTTR} \quad \text{availability} \quad [\%] \qquad (5)$$

Because modern equipment utilizes systems which are redundant, modular and hot-swap,
MTBF is higher and MTTR lower than older systems.

$$A = \frac{Uptime}{Uptime+Downtime} \quad \text{availability [hrs./year]} \qquad (6)$$

The table below compares the downtime and the corresponding availability. It is easier to express availability in number of digit nine or in a more intuitive way as downtime per year [10].

TABLE II. PROBABILITY OF UNIT WORKING IN TIME

Downtime	Availability
36.5 days/year	90% (1-nine)
3.65 days/year	99% (2-nines)
8.76 hours/year	99.9% (3-nines)
52 minutes/year	99.99% (4-nines)
5 minutes/year	99.999% (5-nines)
31 seconds/year	99.9999% (6-nines)
3 seconds/year	99.99999% (7-nines)

System Availability is calculated by modeling the system as an interconnection of parts in series and parallel.

Availability in series

For components in series the availability for n components is:

$$A_s = A1*A2*A3*....*A_n \quad \text{or} \quad A_s = \prod Ai \qquad (7)$$

Where: A_n = availability of component n; i=1.n components

For n identical components $As = A^n$ (8)

In series systems; availability will not be higher than lowest component availability. If one component fails, system fail

Availability in parallel

For a simple calculation in this case, we need to introduce

$$\text{Unavailabilty} = 1 - \text{Availabilty} \qquad (9)$$

Components in a parallel configuration are either identical or similar with the same function. Assumptions are that the components failures are not arbitrary and components are fail-safe.

$$Ap = 1 - \text{Unavailabilty (Parallel system)}$$

$$Ap = 1 - \prod(1 - Ai) \qquad (10)$$

where i =1...n system components.

For n identical components.

$$Ap = 1 - (1 - A)^n \qquad (11)$$

In parallel systems availability would be higher than the most available component. The system in parallel configuration fails, if all of its components fail.
A system in parallel is called redundant.

3) MANAGEABILTY

Manageability is a system characteristic which represents the ease with which the system can be monitored and maintained to keep it performing, secure, and delivering agreed upon levels of availability. Manageability functions can aid in establishing when preventive maintenance or service should take place. They are:

a) System monitoring .data logging and alarms.

These functions keep track of the system's ability to perform its function. Logging generates a history of activity, which can provide valuable information associated with a failure. Alarm schemes vary from predictive warnings, to alarms indicating when a failure has occurred or system shutdown when a monitored parameter (such as voltage or temperature) has exceeded a threshold.

b) Configuration and Control

includes setting up a spare components strategy. Another key aspect is configuring a system for security. Implementing controls can ensure authorized access and protection against hostile activity by tier access. Operators/Users are only allowed in different system sections based on skills and when required by task performance and degree of interaction needed with loads, controls or input sources.

c) Field deployment and upgrades

This phase includes efficient spare part set-up and minimizes diversity. It takes into consideration the lead-time for spare delivery from vendors,distribution. Employment of HOT-SWAP modules will expedite installation of systems, updates, and scalability.

d) Asset Planning and Retire

In the Wear Out phase (see Fig. 11), manageability and serviceability functions can be a great burden. Hence this phase is typically characterized by a time of increased service and repair, which will lead to replacement of the system. As systems require replacement, key management functions include preserving the retiring system's state for migration, removing the system from asset inventory, and adding the new systems (assets) to the inventory. In addition, preserving the system errors, failures and service history, when captured by good management tools in Early and Useful Life phases, can be valuable in preparing a management strategy for the next generation of systems.

4) SAFETY

Safety system attribute is essential for safe performance to ensuring public safety. Power supply systems have potential to expose people and sites to the:

•Electric Shock: Create dangerous path for electric current through the human body leading to injury or death.

•Energy Hazards: High energy/ temperature due to high current, capacitive discharge in operation may produce a shock or burns by touch live points inside.

•Fire: May result as overload, abnormal operating conditions or fault in some system insulation. Fire barriers need to be incorporated to prevent in such condition a fire spread to adjacent components or equipment

•Heat Related Hazards: High temperatures on touchable surfaces in normal operation.

•Mechanical Hazard: Injury or damage resulting sharp edges or corners, flying parts, or enclosure instability.

Compliance with regulatory agencies ensure a high safety level at the component level.

System failure modes are defined as:

a) Fail-operational systems continue to operate when their control systems fail and As example may be power supplies which loss voltage regulation max specs from a 0.2% to a 5% but performance degrade is tolerable by the system , or case of remote error sense controlled units when sense wires are disconnected and open sense protection may cause an output voltage jump but not enough to eliminate the module from system or the programming analog parameters via digital busses are lost and unit default to a preset predetermined value of analog control via a voltage or divider resistors.

b) Fail-soft systems are able to continue operating basic with reduced performance in case of failure. An example will be HSP units in a fan failure conditions, hazard creating fault ; a fan failure will allow the units to operate at reduce power (for a rated 1000W), fan less operation derate them to 300W and while alarm flag of fan failure is raised the unit controls would not exclude it till the over-temperature sensor and protection will act.

c) Fail-safe systems become safe when they cannot operate and they exclude themselves from operation .An example will be a unit entering OVP (overvoltage) condition ; that must fail safe as it may influence other units in overvoltage or trigger the input protection of components downstream. Same for units exhibiting OTP (overtemperature) condition exist as they create a fire hazard if not excluded.

d) Fail-secure systems maintain maximum security when they cannot operate. Units in a redundant system with OR-ing (blocking diode) exclude themselves when cannot operate

e) Fail-Passive systems Fault-tolerant systems avoid service failure when faults are introduced to the system.

For most high availability systems, a failure will lead to a behavior described above.

When power supply systems feed the control systems managing an overall process or plant, they have to comply with Functional Safety per IEC 61508. Functional Safety was developed in response to the growing need for improved confidence in safety systems and the desire to design safety systems in such a way as to prevent dangerous failures or to control them when they arise. A Safety Instrumented System (SIS) is designed to prevent or mitigate hazardous events by taking a process to a safe state when predetermined conditions are exceeded maintaining Functional Safety. Each SIS has one or more Safety Instrumented Functions (SIF). Every SIF within a SIS will have a SIL level. SIL stands for Safety Integrity Level. A SIL is a measure of safety system performance, in terms of probability of failure on demand (PFD). SIL is measured on a scale of four levels. SIL1 is the lowest level of safety protection and SIL4 the highest.

A challenge in such power supplies design is also that often are required to work on wet, dirty, corrosive and/or explosive environments. An example of a design which meets SIL3 probability of failure on demand is KEPCO's KHX units. The KHX series sealed construction and abilities make them Explosion-Proof safe while ensuring the highest ingress protection possible. An outdoor rated enclosure NEMA type 3; 3R; 4; 6P or IEC IP65/66/67/68/69/69K. allows them to operate safely in harsh extreme weather, rain, water or submersible proof applications with output power up to 1500W with natural convection cooling or ability to be integrated cooled by recirculation of different mediums: mineral oil, antifreeze (ethylene glycol).

Fig. 8. Kepco KHX 1500w series ,explosion proof,submersible,multicooling option natural ,fan,liquid circulation

KHX units up to 300W feature natural convection cooling

Fig. 9. Kepco KHX 300w series ,waterproof IP67,IP69K fanless

The SIL rating of a device reflects the degree of reliability in which the product has to fail safely. KHX includes the OVP (overvoltage protection) OTP (overtemperature) protection which will switch off the unit, creating a safe state of no output voltage if such conditions occur. KHX's build-in OR-ing and Free-wheeling (Fly-back) diodes will isolate the unit to ensure a safe single or redundant bulk supply with load current balancing.

High availability of Functional Safety systems is affected by components deployed in Hazardous /Explosive Environments as the most important characteristic will be a failure mode compliant with the functional safety of installation requirements.

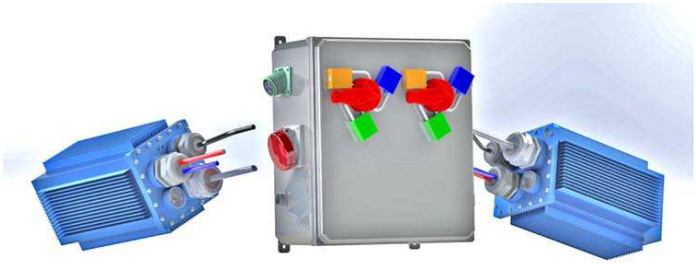


Fig. 10. Redundant hot-swap system for explosion proof using KHX.

To comply with the environmental challenges and maintain a high SIL level, design complexity increases. In the above application the use of an active rack/distribution box in the explosion-proof environment satisfies safety, but reduces the system reliability due to extra components such as switches and disconnects as well as explosion-proof and ingression-proof interconnects, plugs and receptacles. This will decrease MTBF and increase MTTR. The result is that the system maintains its SIL rating, meeting functional safety but at a lower availability (then system in Fig,6). For such system to provide a high availability, a redundant active rack is needed or 2*N+x approach. A N+x approach is not practical as with passive racks due to active racks lower MTBF.

5) SERVICIABILITY

Refers to the ease of recovering from (or preventing) failures; how effectively/efficiently the system can be kept running. It focuses on diagnostic tools, accessibility of components and availability of replacement components. Serviceability is the set of metrics for features that support the timely execution and completion of maintenance conducted on a system. It may be separated in two sets of actions:

- Corrective Maintenance includes all the actions taken to repair a failed system and return it to an available state.

-Preventive Maintenance includes all the actions taken to replace, service, upgrade, a system to retain its operational or available state and prevent system failures.

Implementing concepts in serviceability such as redundancy, modular design; plug-in and hot swap will work to decrease the MTTR and reduce the need for preventive maintenance at short intervals, monthly or quarterly.

IV. ANALYTICAL ANALYSIS FOR FACTORS AFFECTING AVAILABILTY

From the previous formulas for reliability and availability it is obvious that a major focus is to increase MTBF and reduce MTTR . The figure below represents a typical life cycle of a product and its analysis will reveal lots of area for improvements

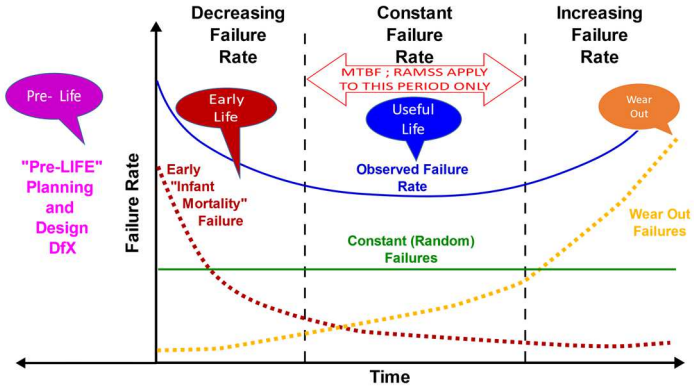


Fig. 11. Product Life cycle failure rates [9]

Consider the "bathtub curve" above. It depicts the failure rate over time of a system or a product. A product's life can be divided into four phases: Pre-Life, Early Life, Useful Life and Wear Out. During each phase, different considerations must be made to help a failure at a critical or unexpected time .The chance of a hardware failure is high during the initial life of the module. The failure rate during the rated useful life of the product is fairly low. Once the end of the life is reached, failure rate of modules increases again.

Failures during a products life can be attributed to the following causes:

Pre-Life Design failures: This class of failures take place due to inherent design flaws in the system. In a well-designed system this class of failures should make a very small contribution to the total number of failures

This is the time when the design for x (Design for Excellence) helps to include all the obvious or low probability chances that Murphy's law will challenge the design

Design for Manufacturability; Design for Assembly

Design for Testability; Design for Usability

Design for Serviceability; Design for Reliability

Design for Transportability; Design for Safety

Design for Accessibility; Design for Simplicity

Early –Life Infant Mortality: This class of failures appear on the newly made prototypes production samples. Process analysis, Design Verification/Validation, Test to Failure and Burn in Test approaches will help, as will HALT/HASS (highly accelerated life test; highly accelerated stress screening). along with This class of failures can be attributed to design or manufacturing problems like poor soldering, leaking capacitors, etc. These failures should be caught and will not be present in systems leaving the factory.

Useful Life : Random failures may occur during the useful life of a system component. This is the time period when MTBF is calculated and almost all of the "RAMSS" characteristics of highly available systems will apply. Most of these failures can lead to system failures. The pre-life MTBF is calculated by a few standards (e.g., MIL HDBK 217F, IEC 61709and Belcore /Telcordia) or may come from demonstrated MTBF in case of a product with enough mission time through demonstrated failures.

$$MTBFfield = \frac{\sum(Total\ units\ ship * field\ operating\ time)}{\sum(Unit\ failures\ or\ units\ returned\ for\ repair)} \quad (12)$$

An intrinsic analysis of component failures in power systems provides useful information and lessons to learn from installed products

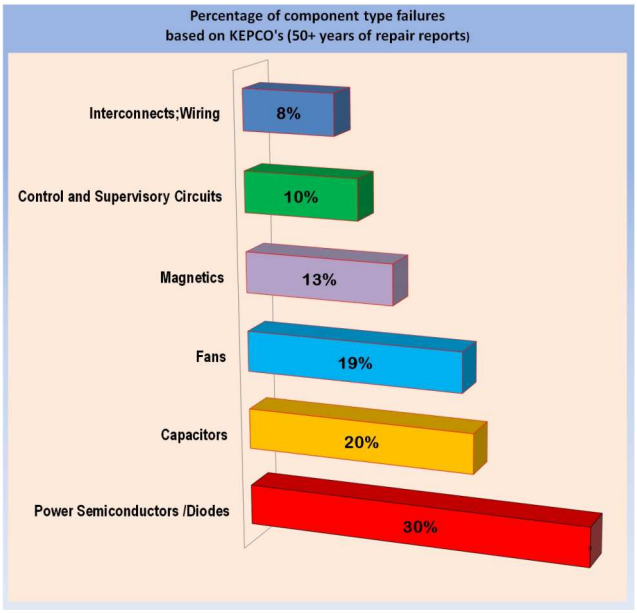


Fig. 12. Component type failures based on Kepco's repairs and field returns

The conclusion drawn from the analysis was that components are prone to failures due to Voltage Stress, Thermal Stress, Mechanical Stress, Aging and Other causes (Improper storage, ESD, Counterfeits). Components types with the highest failures:

1) **Power components**. Take the brunt force of operation of the power supply and are vulnerable to bad heat sinking, thermal interface errors, surges, spike, overvoltage, overcurrent conditions or exceeding the safe operating.
2) **Capacitors.** All types of capacitors. tantalum, electrolytic, and multilayer ceramic capacitors all have their own unique ways of breaking down. They fail due to aging or from voltage, thermal and mechanical stresses.
3) **Fans.** As electromechanical, moving parts fans have highest failure rate and their operation can be highly influenced by environment such as mounting orientation, shock and vibration, and obstruction of vent areas.
4) **Magnetics.** The majority of power magnetics are custom-designed with hand-wound construction. This can lead to many issues and also exposure to abnormal factors which stress insulation as surges, spikes, and temperature and humidity exceeding insulation class limits
5) **Control ICs** have an unusual region of operation in the transition to normal operation, they are susceptible to noise or oscillation and may cause power semiconductor failures just by improper timing and phase.
6) **PWB and interconnect failures**. Failures include advanced corrosion due to exceeding rated pollution degree, leaking electrolytics, plating corrosion on connector contacts, solder joints failures on components, lugs and harness wires; loose connections due to thermal cycling and opening of safety fusible resistors; PTC due to abnormal input conditions; or frequent shorts in operation.

Wear Out: This phase begins when the system's failure rate starts to rise above the "norm" seen in the Useful Life phase. In a power supply system, mechanical moving components such as fans, switches, relays, and frequently used connectors, are the first to fail. As shown in the component failure graph above, a mix of other component classes will lead to failure. Most ICs and electronic components last about 20 years under normal use within their specifications. The key in extending a system's operational life relies on maintenance, replacement plans and the use of serviceability features and practices. In Kepco's 75+ years of history we have seen mission critical systems that still operate after 30+ years of service and many regular power supplies reaching 50+ years.

V. SYSTEM AVAILABILITY. CALCULATION EXAMPLE.

The following example shows the Availability calculation for the system in Figure 6.
The System component diagram schematic is shown below:

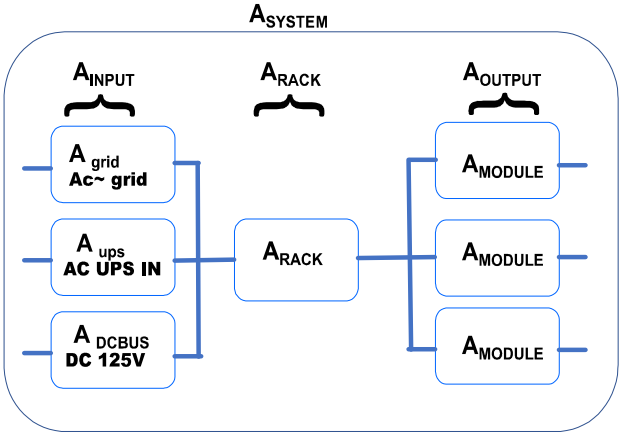


Fig. 13. System availability block diagram of system in figure 6

Applying formulas for a group of 3 subsystems in series

$$A_{system} = A_{input} * A_{rack} * A_{output} \quad (13)$$

1) A_{input} triple redundant input system (parallel)
   a) AC input from Grid.

A typical US power grid availability may be as a low 99.5%
A_{grid}=0.995 as result U_{grid}=1- A_{grid} U_{grid}=0.005

   b) AC input from UPS.

Using formula (5) and for a typical UPS MTBF of 500000 hrs. and MTTR=6 hrs.

$$Aups = \frac{MTBF}{MTBF+MTTR}$$ A_{ups}=0.99998888 U_{ups}=0.0000112

c) DC input from 125VDC Battery Bus.

A DC plant bus in a 2N configuration has a typical MTBF =2,058,600 hrs. and MTTR = 2.60630 hrs.

A_{dcbus}= 0.9999987 U_{dcbus}=0.0000013

As a result, the system input section availability will be

$$A_{input}=(1-U_{grid}*U_{ups}*U_{dcbus}) = 0.9999999999$$

2) A_{rack} Rack enclosure hosting the AC/DC modules is a component in series within system.

Using rack MTBF rack =2650000 hrs. MTTR=1hr.

$$Arack = \frac{MTBF}{MTBF+MTTR} \quad (14)$$

A_{rack}= 0.999999622

3) A_{output} DC output part of system consist of a Redundant N+2 derived from input requirements.

$$Amodule = \frac{MTBF}{MTBF+MTTR} \quad (15)$$

A_{module} = 0.99999375

$$Aoutput = 1-(1-A)^n \quad (16)$$

A_{output} = 0.999999999999999755859375

Replacing in formula (12) result the mission system critical availability will be: A_{system}=0.999999618, a six nines .

This represent a high availability system and per above conclusion shows that the weakest link is the component in series (rack enclosure), even it has a large MTBF.

To achieve an availability beyond six nines in this application a 2N system (addition of a similar system in parallel) is need it

$$A2nsystem = 1-(1-Asystem)^2 \quad (17)$$

$A2nsystem$ =0.999999999999854076

That is an impressive twelve nines (12 9's)

Same real-life example will be used to present the importance of manageability and serviceability characteristic to sustain availability. A typical recording of these values is presented on the chart below (Figure 14) where two failures were noted close together on an N+3 system. One unit was indeed failing completely its shutdown imminent. Analyzing the green channel of input current waveform provides an indication ahead of actual failure, a noisy waveform not like the other redundant units of the system shown in red; yellow, blue, dark green and dark blue. After spare replacement a more stable input current is seen on same channel, in line with the others.

Important clues to increase manageability and a wealth of information obtained from a single input current sensor

The measured current value axis will provide indications of:

- Unit unplugged/removed from rack: ~0A
- Unit input failed (AC grid, AC Ups, DC battery bus)
- Unit plugged with circuit breaker OFF: ~0.07A (EMI caps and resistor across line-neutral)
- Unit plugged but defective "dead "and circuit breaker ON: ~0.11A input (due to additional capacitors after CB)
- Unit plugged and idle: ~0.25A (current share not enable /improperly set, or with DC fault and no DC output due to overvoltage/overcurrent /over-temperature)
- Unit operating normal: >0.25A

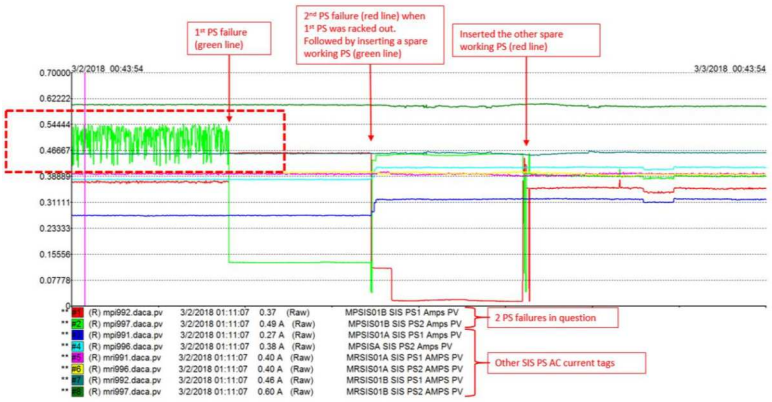


Fig. 14. Monitoring Input current of a N+3 system provide important clues.

VI. IMPROVE AVAILABILTY BEYOND SIX" NINES"

From above observation there are few areas to focus in achieving this goal.

Design a system with failure in mind to account for Murphy's Law. Executing proper FMEA (failure mode analysis for design DFMEA process PFMEA) helps understanding the application, environment and communicate design intent

Design for Poka-Yoke. Based on the axiom that 'Nobody is Perfect', Murphy's Law is inevitable, and designing with Poka Yoke (avoiding defects and mistakes by preventing, correcting, or drawing attention to human errors as they occur) in mind is the best possible approach. This is defensive design, which highlights the areas where environment and human intervention could possibly be detrimental to the system. The environment in which the system operates can have a great impact on its availability:

-Input power effects on system, proper grounding, floating neutrals, spike and surges, brownouts; power outages duration.

-Ambient effects, temperature and humidity levels and cycles, shock and vibration patterns, dirt and dust, water ingression; explosion-proof; corrosive chemicals, salt spray, pollution degree, altitude, storage conditions for spares, EMI/EMC interference, electromagnetic radiation.

-Human factors and usability: improve access time for personnel access; reduce time to remove a hazard; expedite site access credentials and install a subsystem clone environment to prepare spares and adjust spare output voltage, current limit, etc. so no live adjustments are required.

Tradeoff Specification Performance vs Availability

Some state of art specifications may need to be sacrificed to achieve a no-fault condition. One example is that power supplies in load-sensitive applications must have remote error sense of redundant units connected in parallel to load regulation point to compensate for load wire drop, and only in that condition will they meet published load regulation. Unfortunately meeting the best specification introduces a single point of failure when the remote error sense is disconnected, cut or bad contact due to corrosion. If that occurs all the redundant supplies will crowbar in overvoltage condition. This is not acceptable and therefore error sense connections are made as far downstream as possible, but in a controlled location, typical inside a cabinet hosting each sense to each redundant module's output ahead of main load distribution point. The single point of failure is eliminated but load wire voltage drop remains uncompensated; the voltage regulation specification is less precise due to a slight shift in output voltage from load to no load.

Design With Thermal Goal in Mind

Arrhenius equation [12],[13] is a formula that correlates temperature to the rate of an accelerant (in our case, time to failure). Using the Arrhenius equation temperature related FIT (failures in time) can be estimated given the qualification and the application Applying it to MTBF shows that for every 10°C of a power supply's environment lower than 50°C, it almost double MTBF. Since temperature is listed as one of the important causes of failure on the component failure list (Fig. 12) and because fans, through their limited life contribute by far to a reduced MTBF, there are a few design approaches that will improve availability.

Create a design goal of fan-less power supplies (natural convection cooled). Beside elimination of high FIT, component packaging of the system component can be sealed and prevent water and moisture ingress reducing environment exposure and subsequent failures

Implement the redundant system with current balancing (force current share) feature. That ensures that each paralleled module will deliver almost equal current and as such they will operate at a 50% power rating for N+1 systems and 33% for N+2 systems. As a result, the internal temperatures of modules balance (share) the load will be significantly lower, resulting in double or triple the MTBF.

Keep it simple and safe (KISS) design shall be employed.

Maintain a balance between thermal and energy efficiency and reduce the component counts.

Analyze circuit response in transient conditions.

Consult datasheets and application notes very carefully during design.

Use proven design topologies which make designs adaptable and tolerant to external perturbations; pay attention to the control circuitry, loop testing, and deratings.

Employ universal input AC or DC with PFC to prevent harmonics immunity.

Utilize GaN, SiC and highly efficient technologies to reduce heat dissipation. New technologies allow significant derating of power component breakdown voltages and ensure proper operation and long life of these components.

Reduce losses by boosting efficiency with techniques such as ZVS (Zero Voltage Switching).

Eliminate dissipative elements and improve efficiency of current sensing or eliminate the need for preloads to ensure minimum PWM (pulse width modulator) duty cycle.

One example of conflicting trends is MOSFET vs OR-ING blocking diode topologies. MOSFET solution have the benefit of reducing power dissipation by about 10-15W with the result that operating temperature and MTBF are lower.

The overall MTBF of the OR-ing diode solution is actually higher because it is a simple single proven component, while the MOSFET solution requires two power devices (to eliminate stress on the diode body), a controller makes it more complicated and it is a serial system, hence a lower MTBF. Controller behavior may sometimes cause an undesired response in the event of transitory stages or startup conditions blocking conduction till stable. Therefore, in high availability systems the KISS approach will prevail.

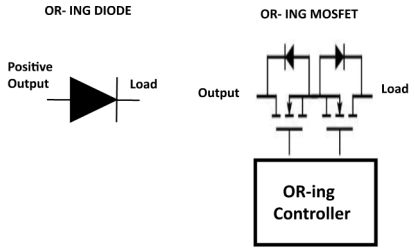


Fig. 15. Comparison of OR-ing topologies Diodes vs MOSFET

Design For Availability

Keeping spare parts physically close to the system helps to quickly replace failed components, reducing the MTTR and, therefore increasing availability. When MTTR need to be reduced; an onsite spare location with 24-hour maintenance on premises can make repair within a 30 min plus up to 1hr for access to special areas. Compare that to an MTTR of up to two weeks when ordering spares from a remote warehouse.

Employing a Fault tolerant design with redundancy allows repair at a preventive maintenance or if it is Hot Swap type allow live replacement with no downtime (Zero MTTR).

While reliability is exclusively dependent on the MTBF, the major impact on increasing MTBF comes from design factors, especially conservative derating of components, use of well proven circuit topologies, and elimination or reduction of fan risk elements from the design.

Availability is different from reliability as it takes MTTR repair time into account.

In example below if cooling function is selected as redundant then availability increases. Because function can be approached as two parallel systems. Kepco KHX present such a case where the unit delivers up to 1000W in natural convection (or in case of fan failure). When fans are operating, output operation of up to 1500W can be sustained at ambient of 50ºC. Calculating MTBF with fans result in a decreased number therefore may be perceived not as an improvement on reliability, but from availability things are different if system

operating conditions are limited to 1000W of output power. Calculating availability for the redundant cooling function of parallel system of a natural convection cooled with MTBFfanless=198000 hrs. or operating in fan fail mode and the forced convection cooled MTBFfan=75000hrs.

TABLE III. AVAILABILTY FOR A FAULT TOLERANT COMPONENT

KHX POWER SUPPLY AVAILABILTY		
	KHX Fan	***KHX Fan- less or in (FAN FAILURE mode)***
Max Power [W] @ 50ºC	1500	1000
DERATING IF USED as 1000W supply @40ºC	None	None
INTERNAL TEMP . FOR MTBF CALCULATION (º C)	50	65
MTBF [Hrs.]	75000	198000
MTTR [Hrs.]	1	1
AVAILABILTY [%] when Fault tolerant is not allow	99.99867 % (Four Nines)	99.99949% (Five Nines)
UNAVAILABILTY	1.333E-05	5.050E-06
AVAILABILTY [%] KHX UNIT(@1000W output 40ºC) used in Fault Tolerant Mode	99.9999999933% (Ten Nines)	

shows this fault tolerant function increases availability >10 9's

Design For Maintainability refers to how quickly technicians detect, locate, and restore asset functionality after downtime: the higher the maintainability, the higher the availability.

Design For Serviceability Modular architectures promote fault isolation to a contained, replaceable part and decrease MTTR. Include system health monitoring and failure alarm systems. Design to eliminate preventive maintenance. Remove the need for calibration using lower offset parts. Eliminate need to replace/clean filters often.

System self-test and diagnostics capabilities: The faster a faulty component is located the faster can be repaired.

Design for Preventive Maintenance with common tools.

Implement redundancy or use plug-in, hot swap modules to reduce MTTR even further, so system maintenance can be done on a live system, allowing a set of procedures and a checklist of proper maintenance steps to be implemented.

VII. CONCLUSION

Murphy's Law tells us to prepare ourselves for the worst in order to be better designers, engineers, integrators or critical thinkers. There's a good chance for a design that something will go wrong and will fail and failure can't be always prevented. A few of the means to improve the odds in favor of the design were presented above with the intention of making us cognizant of those opportunities for failure. Murphy's law still challenges installations which must not have a single point of failure.

The most recent Murphy's Law challenge came dealing with spares procurement availability or new system orders lead-times. Not only was the semiconductor or capacitor sourcing chain disrupted by lack of production capacities, it also came at the worst possible time, a worldwide pandemic plus the war in Europe which exponentially amplified the component lead-time crisis. Kepco's ability to source components was less impacted and deliveries times increased in weeks not months or years. All due the lessons learned in other times where the supply chain was disrupted by previous prime-time events such as the oil crisis of the 1970's or union strikes of the past. Starting from design with basic components, purchasing from at least three unique vendors that are located apart from each other, all of these, along with proper planning and minimum inventory help in cushioning the impact of Murphy's law.

When commissioning mission critical power supply system the most important criteria is to select a power supply provider that has the "know-how", experience and longevity in this field. Select suppliers that offers an extended warranty to help ensure your system continues to function for decades not years and you will always be able to call for support with sales and application engineers.

When system integrators pick an establish vendor who will be there in the next decades, it ensures that spares will always be available over long periods of time encompassing the useful life of the system.

In technical fields almost everything is achievable for a price. Sometimes the cost of mission critical power supply systems with no single point of failure is high due to complexity and the requirements of avoiding a single point of failure and other safety constraints, but an experienced integrator will always recognize the fundamental question:

What is the cost of downtime or total cost in case the mission critical system loses its availability?

REFERENCES

[1] **** Kepco Power Supply News Vol. 9 No. 146-1147 (1966)

[2] Paul O'Boyle and Steve Kugler, Fault Tolerant Power Systems , Electronic Design, November 3, 1997

[3] NewYork_City_Fire_Department,Wikipedia,July24,2022 https://en.wikipedia.org/wiki/New_York_City_Fire_Department

[4] Mark Kupferberg, Approaches to Implementing Fault Tolerant Power Systems,Kepco Currents Vol.9 , No. 2, February 1999 https://www.kepcopower.com/newsfaul.htm

[5] *** Military Handbook - Reliability Prediction of Electronic Equipment, MIL-HDBK-217F Notice 2, Feb 28, 1995

[6] Paul O'Boyle, Redundancy And Hot Swapping Keep Systems Running, EE Times, August1994

[7] Byron Radle and Tom Bradicich,Whitepaper What Is RASM?,National Instruments, March 5,2019 https://www.ni.com/en-us/innovations/white-papers/13/what-is-rasm-.html

[8] Rudolph Frederick Stapelberg, , Handbook of Reliability, Availability, Maintainability and Safety in Engineering Design" Springer - ISBN 978-1-84800-174-9 , 2009

[9] Bathtub curve ,Wikipedia,https://en.wikipedia.org/wiki/Bathtub_curve, May 21,2021

[10] Daniel P. Siewiorek and Robert S. Swarz,Reliable Computer Systems: Design and Evaluation,3rd ed.,(A K Peters/CRC Press,2019).

[11] Arrhenius_Relationshuip, Reliawiki, October 21, 2021. https://www.reliawiki.com/index.php/Arrhenius_Relationship ,

[12] *** JEDEC JESD91A, Method for Developing Acceleration Models for Electronic Component Failure Mechanism,August 2001

[13] *** ASME RAM-1-2020: Reliability, Availability, and Maintainability of Equipment and Systems in Power Plants Paperback – June 30, 2020