WHITEPAPER

DESIGNING FOR RELIABILITY

A guide to avoiding pitfalls in critical power system design

DEIF

If you are planning to install or upgrade a critical power system, keep reading – this whitepaper is for you. It will introduce you to some of the most important considerations in designing critical power systems, and it will help you avoid some of the pitfalls that can result in inadequate design, installation, maintenance, or testing. Draw on the tips and good advice below to design a system that gives you the reliability you need. After all, there is a reason why critical power systems are called "critical".

Being able to rely on dependable backup power is very important; in many businesses, power failure is simply not an option. Examples include life safety, medical, industrial process control, data centres, telecommunications, as well as television and radio broadcast systems. Despite the importance of critical power systems, however, they have been known to fail because of inadequate design, installation, maintenance, or testing. And when they do fail, a lot of money is wasted because lost production time, uptime, or other important operation parameters quickly add up. More importantly, the trust of your customers or even human life could be at risk.

We have prepared this whitepaper with tips and good advice on designing critical power systems. Hopefully, this will help you steer clear of some of the pitfalls that have put critical power systems out of action on several occasions in the past.

In hospitals, reliable critical power systems can literally be a matter of life or death

QUICK CHECK LIST

Here is an easy overview of our main recommendations. All are explained in further detail in this whitepaper.

- Involve critical power experts and vendors at an early stage of the project
- Set up a pre-project to qualify your installation plans
- Make sure that relevant staff is trained on using the critical power system
- Ensure that you can rely on full long-term support from your vendors
- Install your critical power system, and the day tank, in a safe place
- Design your critical power system so that it is protected against fire
- Carefully weigh the pros and cons of a PLC or multi-master power management system
- Select a control architecture that allows CTS/BMS/SCADA integration
- Define operating sequences in the system as needed
- Define and carry out tests to validate system functionality
- Set up a reliable DC power supply for controllers with full redundancy
- Design for redundancy when setting up controller communication lines
- Select gensets and engines that provide enough power while offering the lowest possible operating and maintenance costs
- Develop maintenance and testing schedules, and make sure that they are followed
- Test the critical power system under realistic operating conditions
- Replace system components as needed, and always follow manufacturer recommendations

GET THE EXPERTS INVOLVED AT AN EARLY STAGE

- Involve critical power experts and vendors at an early stage of the project
- Set up a pre-project to qualify your installation plans
- Make sure that relevant staff is trained on using the critical power system
- Ensure that you can rely on full long-term support from your vendors

Get critical power experts involved when selecting a critical power solution – the sooner, the better. If designing, installing, and maintaining critical power systems is not your core business area, you will almost certainly benefit from a constructive dialogue with experts who have extensive and proven experience with critical power. They can provide good advice, fresh ideas, and constructive criticism; whether you are working with a new installation or a retrofit project, this is certainly one of the most important aspects of the process.

You will almost certainly benefit from a constructive dialogue with experts who have extensive and proven experience with critical power

PRE-PROJECT

Set up a pre-project with your chosen vendor to qualify your critical power installation plans. The vendor's technical know-how and application experience will often give you a greatly improved solution that fulfils your requirements while taking full advantage of the features that the vendor's components offer.

Critical Power System Specialist René Kristensen of DEIF explains that dialogue in the early stages of a project is a very important factor. "Through dialogue with the customer, we learn what the customer's challenges are, and what he needs," he says. "We present and explain our view of the project, make some suggestions, and reach an agreement with the customer so that he gets the optimal solution".

A pre-project will often include one or more site visits, especially in case of complex retrofit projects, so that vendor technicians and engineers can see your current installation and challenges for themselves. They get an opportunity to talk to all relevant stakeholders in your organisation, for example the staff who operate and maintain the critical power equipment.

The outcome of a successful pre-project is a specification for a solution that addresses your pain points while taking full advantage of the vendor's experience and offerings, and which can be installed and commissioned with a minimum of delays or disruptions.

STAFF TRAINING

Talk to your chosen vendor about training your staff. Critical power solutions are mission-critical equipment, and the staff who will operate the equipment during regular maintenance and in emergencies must know how to do so, and be comfortable doing so. For example, your users need to know how to isolate individual system components for service or maintenance, and manually carry out switching operations in case the automated sequences fail. This is a crucial aspect of operating the critical power system and underlines the importance of staff training. "It's no use installing a great system if no one dares to press its buttons in case something happens", says René Kristensen. "We make a point of educating users on how to use our equipment".

"It's no use installing a great system if no one dares to press its buttons in case something happens"

René Kristensen, DEIF

AFTER-SALES SUPPORT

When selecting a critical power solution vendor, make sure that the vendor is able and willing to provide after-sales support for years. After all, your critical power solution should be a long-term investment, so you need long-term access to technical support, firmware upgrades, and spare parts. A good vendor can also advise you when it might be a good idea to upgrade system components to take advantage of technological innovations.

SELECT THE RIGHT LOCATION

- Install your critical power system, and the day tank, in a safe place
- Design your critical power system so that it is protected against fire

Your critical power system needs to be installed in a place where it is safe from any foreseeable incident that could adversely affect operation of the system, and where fire-fighters or utility personnel can easily access it. There are many parameters to consider depending on the location. Flood or earthquake protection and safeguarding against unauthorised access are two examples of important factors that you might need to consider.

Always design your critical power system so that it is protected against fires. If possible, design the system so that a fire will be contained, or slowed down. If the system interfaces with a CTS, BMS, or SCADA system, use this connectivity to send and receive warning and alarm signals. Install fire sensors near the day tank that can prevent tank refill operations if there is a fire nearby. And select a day tank material that is resistant to fire.

Fukushima disaster made worse by installation location

The 2011 nuclear disaster at Fukushima, Japan, was caused by a tsunami higher than the installation's seawall. Most of the emergency generators designed to provide backup power for the plant's reactor cooling pumps were located below seawall level and were flooded, as was the switching equipment. A subsequent investigation commission report concluded that the disaster had been avoidable, but that the plant operator had failed to meet basic safety requirements.

Source: Report on the Fukushima Daiichi accident by the International Atomic Energy Agency

DEVELOP YOUR OPTIMAL SYSTEM DESIGN

- Carefully weigh the pros and cons of a PLC or multi-master power management system
- Select a control architecture that allows CTS/BMS/SCADA integration
- Define operating sequences in the system as needed
- Define and carry out tests to validate system functionality
- Set up a reliable DC power supply for controllers with full redundancy
- Design for redundancy when setting up controller communication lines
- Select gensets and engines that provide enough power while offering the lowest possible operating and maintenance costs

No two power installations are the same, and critical power system requirements therefore vary greatly. Work with your solution vendor to design a system that meets your requirements to the letter. Here are a few suggestions for developing a system design that is optimal for your facility.

CONTROL ARCHITECTURE

You need controllers capable of switching between power sources and controlling load groups as needed. The question is which control architecture to use.

The traditional approach is using Programmable Logic Controllers (PLCs). Robust and reliable, PLCs are a widespread, tried and tested solution in many environments. A PLC is based on ladder logic, and the original programmer can relatively quickly change its configuration, often without modifying the controller hardware. Sequences (see below) can be defined for each individual application at code level using a series of IF-THEN clauses. However, when a single PLC is used to control a critical power system, the system is very vulnerable to controller failure.

A multi-master control architecture protects the system against individual controller failure

Another option is using a multi-master power management system (MM PMS). Such a solution is often based on a standardised hardware and software architecture and is therefore easy to reconfigure or expand for any application or sequence, even if you did not originally design it. This makes MM PMS solutions very service friendly.

Most importantly, the multi-master architecture protects the system against individual controller failure.

When deciding on a control strategy and selecting controllers, consider whether your critical power system needs to interface with a CTS, BMS, or SCADA system. This is particularly important with fire safety; see above. If the ability to send, receive, and process input from other units on the network is important, your controllers should be able to do this. Again, a MM PMS solution will often be comparatively easy to integrate into a building management system if its communication protocol(s) and connectivity features are compatible with the system used.

SEQUENCES AND TESTS

What should your critical power system do in case of power supply problems? For example: If a grid transformer fails to deliver the power needed at a load point, is it sufficient that another grid transformer delivers the power, or should a start signal be sent to one or more gensets right away? Scenarios such as this form the basis of operating sequences in the system; these sequences decide how the critical power system should react to any foreseeable situation. Defining these sequences is a major consideration when setting up the critical power system.

There are several factors that need to be taken into account when defining the sequences. In addition to ensuring enough power for the connected loads, the sequences must also, for example, safeguard against short circuits by ensuring that there is never too much power on the generator busbar at any time.

Mains faliure → **Start signal** → **Starter ON** → **Nominal RPM** → **Hz/V OK** → **The breaker closed**

Sequences decide how the critical power system should react to any foreseeable situation.
Defining these sequences is a major consideration when setting up the critical power system.

You must also define a testing programme for the critical power solution that includes genset load tests and full system tests. In any critical power system, both types of test are absolutely necessary in order to see how the system will respond to actual conditions. Your testing programme must be tailored to actual installation conditions; work with your solution vendor to define the tests that are necessary for your facility based on your requirements, sequences, and installed components.

An example of a maintenance and testing schedule is provided at the end of this whitepaper.

WHAT IS A LOAD TEST AND A SYSTEM TEST?

During a **load test**, a genset is subjected to a heavy load, such as 80%, revealing how it performs in high-load conditions.

During a **system test**, the critical power system is switched to island mode, powering the connected loads using the gensets alone before switching back to grid power. This test validates that all breakers work as they should and all gensets start as required.

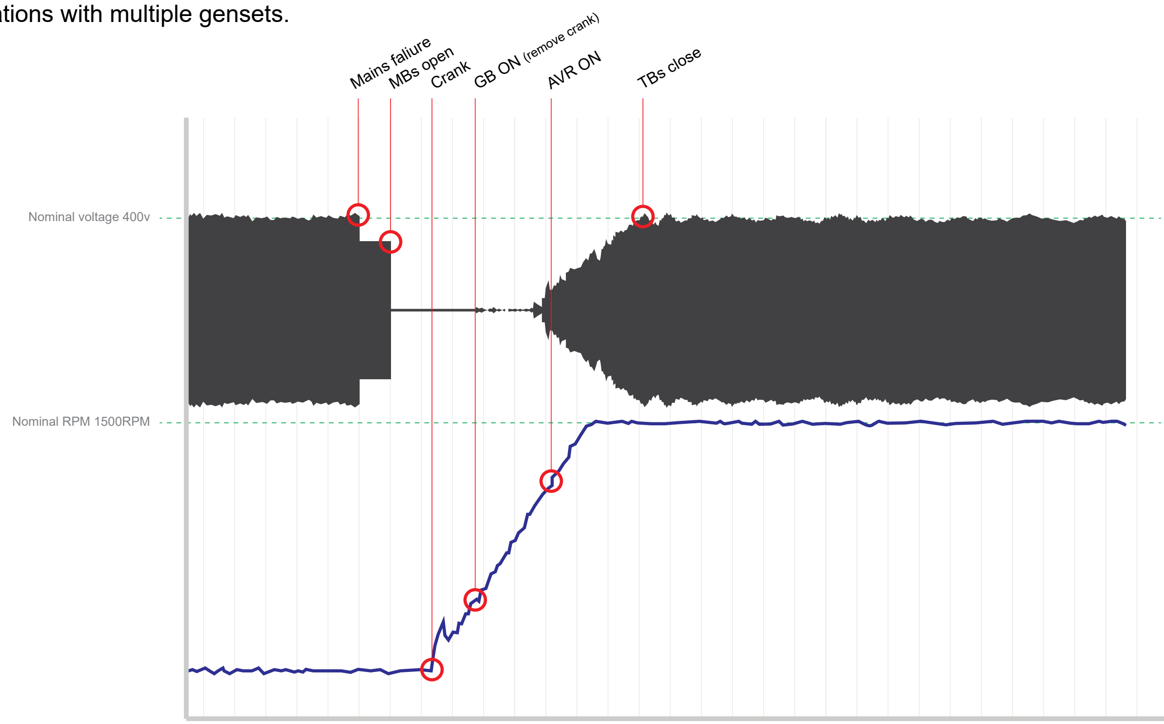
START-UP CRITERIA

Gensets can start up and deliver power in several ways, and selecting the right approach is key. There are two major issues here: First, your critical power system may be required to deliver full power within a set time limit. Second, gensets produce high inrush currents during start-up, and those inrush currents may cause problems in your system.

Problems with inrush currents can occur, for example, if your system relies on step-up transformers between your gensets and the busbar. When the current from a genset reaches the transformer, the unmagnetised transformer will appear as a short circuit to the genset. This will result in a transitory high inrush current which can, in the worst cases, cause the generator to trip because of overcurrent. To safeguard against this, select a solution that lets you control how much current is drawn from the genset to the transformer. By doing so, you can avoid spikes, and the current is gradually ramped up without causing short circuits.

If your critical power system needs to deliver full power within a set time limit, or if high inrush currents could cause problems, you need to select a start-up procedure that meets these challenges

The Close Before Excitation (CBE) feature found in intelligent DEIF controllers is one such solution. With CBE, the genset breaker is closed when the genset is running at, for example, 200 RPM, connecting the genset to the step-up transformer and the busbar. The alternator, however, is not excited immediately. Excitation starts at 900 RPM, and the voltage ramps up to nominal values. Through this procedure, inrush currents are limited. Another benefit is limited circulating currents in applications with multiple gensets.



CBE <10 SEC. START SEQUENCE

Mains faliure	Start signal	Starter-on	Nominal RPM	Hz/V OK	TB closed	Sequence
0,5	1	2,5	2,5	2	0,5	Sec.
0,5	1,5	4	6,5	8,5	9	Total

The CBE feature from DEIF closes all breakers before exciting the gensets. This controlled way of producing excitation means that when the genset does produce power, it does so without inrush current spikes and in a controlled manner.

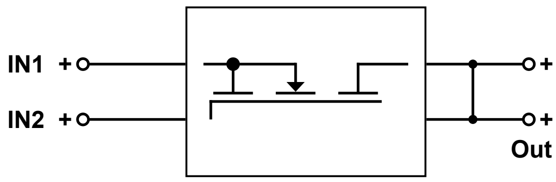
The feature can also be used to get full backup power fast. With traditional start-up procedures, gensets are connected to the busbar sequentially before closing the breaker to the load. Each time an additional genset is powered up, it needs to be synchronised with the ones that are already running. This takes time and delays the availability of full power. With CBE, any number of gensets can be connected to the busbar and started all at once. It is not necessary to synchronise the gensets with one another. Full backup power can therefore be available within approximately 10 seconds, no matter how much power is needed. This is important in applications such as hospitals or data centres.

For hospital applications, EU regulations require full backup power to be available within 15 seconds of a grid blackout while the US FPA stipulates a 10 second limit.

In large installations with several gensets, this may not be possible with traditional start-up methods. If your critical power system design does not rely on step-up transformers, or if getting full backup power quickly is not a priority, traditional start-up procedures can be employed. If equipment protection or fast start-up, or both, are important, however, you need to find a way of solving these issues.

REDUNDANT CONTROLLER POWER SUPPLY

Ensuring reliable DC power with full redundancy for your controllers is a critical design consideration. If these key components are not able to switch between power sources, the critical power system simply will not work.



DEIF recommends installing a diode module that provides three power sources, ensuring power for controllers even if one power source fails

Always set up a redundant power supply so that if power source A fails, power source B is ready to take over. DEIF recommends installing a diode module with an outlet powering the controllers. The diode module has inputs for connecting power sources such as a grid connected power supply and generator starter batteries. Its output feeds a battery that provides a third source of backup power. Having three power sources ensures that there will always be power for the controllers, even if one power source fails.

The DEIF controller monitors the diode module, so if a failure occurs on one of the primary supplies, it will send out an alarm to the DEIF controller that will send through to the BMS/SCADA system. Always make sure that the redundant power sources you install can actually affect system reliability!

"We sometimes see that users only have one UPS (Uninterruptible Power Supply) unit as their power supply. There can be more than one power source feeding the UPS, but if the UPS itself fails, this redundancy is ineffective, as it is not possible to distribute the redundant power", says René Kristensen. Two separate UPS systems are the preferred solution.

DESIGN FOR REDUNDANCY THROUGHOUT YOUR CRITICAL POWER SYSTEM

Your critical power system provides redundancy for your facility in case of grid blackouts. However, you also need to think about redundancy in the critical power system itself. Here are three quick tips for achieving full redundancy in your critical power solution:

- Choose a multi-master power management system (MM PMS) to safeguard against individual controller failure
- Set up at least one redundant power supply option for your controllers
- Make sure that there is a redundant communication channel between controllers and other units in your critical power system

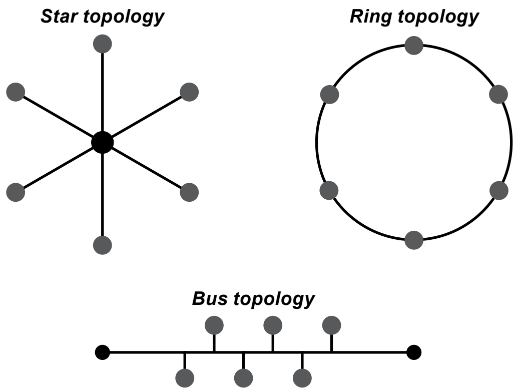
"It's important to think about redundancy all the way through the critical power system. One weak link in the chain is enough to bring down the whole system," says René Kristensen.

CONTROLLER COMMUNICATION

Ensure that the controllers in your critical power system can always communicate with the rest of the system, and with one another. This is just as important as ensuring a redundant power supply: without communication, your system will not work. Here are a couple of points to consider:

Use a communication protocol with two physically separate lines, such as the CAN bus used in DEIF controllers. If you route the wires for both channels in the same cable tray, of course, this may not achieve much; an incident that takes out CAN A would probably take out CAN B, too. For controllers installed wide apart, however, using two physically separate channels greatly increases reliability. Design your system to allow for this when at all possible.

Choose a network topology that provides redundancy. A single-string link network is vulnerable, in that all controllers further down the line will lose all communication if the first cable link is broken. Use ring or star networks instead, as they provide better network redundancy. If the connection to a particular node fails in a star network, for example, the connections to all other nodes will still be available. The entire star network can be replicated in two physical locations to increase security, for example by setting up two parallel CAN bus networks using a star topology. If a ring network is broken in one place, communication between nodes will still be possible by using the rest of the ring network.



Single-string link networks are vulnerable to communication failure. Use ring or star networks whenever possible, as they provide better redundancy

Select cables that allow efficient communication. The question of whether to select copper or fibre cables is a question of distance: Copper cables can handle a total of 300 metres of cable length, which is not enough for major installations. When controllers and other units are spaced further apart, choose fibre cables that carry signals for longer distances.

GENSET RATING AND ENGINE SIZE

If your gensets do not deliver sufficient power in emergency situations, your critical power system will not be able to carry out its duties. Carefully calculate how much backup power you need, and for how long, and select gensets that deliver the necessary power. Select a genset able to deliver the necessary power at its optimum duty point (often 70% of full load). By doing so, you increase the likelihood of getting uninterrupted backup power for as long as you need it.

Select gensets and engines that provide enough power while offering the lowest possible operating and maintenance costs

When selecting engines to drive your gensets, consider the total purchasing, operating, and maintenance costs, and system redundancy. Several smaller engines may be cheaper than one big one and provide a modular expansion approach and power supply redundancy. On the other hand, service staff may spend more time on service and maintenance with more engines, and operating one engine may be simpler and more effective.

INSUFFICIENT CRITICAL POWER IS AS BAD AS NO CRITICAL POWER

In November 2017, the city of Mainz, Germany, was hit by a 20-minute grid blackout. A local glassworks had a critical power system, but it was unable to provide enough power to keep the molten glass in production sufficiently hot. With not enough power to keep manufacturing going, the factory incurred costly production losses and production and delivery delays.

Source: Süddeutsche Zeitung

LOAD GROUP CONTROL

In many applications, a BMS (Building Management System) manages all consumers onsite. The BMS knows how much generator power is available at any given time and uses this information to prioritise load groups in case of a grid blackout. In case of a blackout at a hospital, for example, the BMS might prioritise power for the intensive care unit and operating theatres.

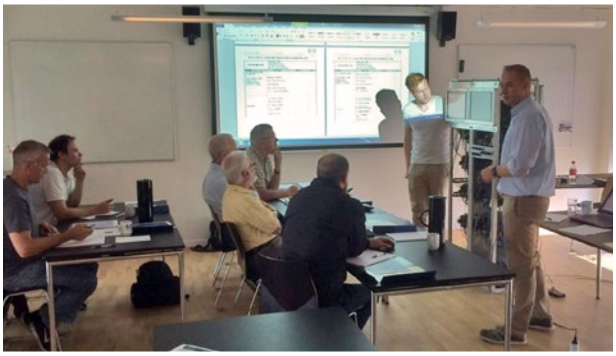
Instead of using a BMS to prioritise power distribution as needed, based on 4-20 mA signals from PLCs or controllers, consider using dedicated, intelligent load controllers. The advantage is that such load controllers will be integrated into the PMS system, making communication and control more efficient. All controllers in such an integrated system will always be aware of the positions of all breakers in the system and the exact load at all load points, and they can use this detailed information to make more intelligent power management decisions.

Using dedicated load controllers allows you to achieve more intelligent control in accordance with the general system design than when using a BMS

By contrast, a BMS only receives relatively simple control information and therefore cannot control the system with the same level of detail. Many BMSes, moreover, are not custom-made for critical power and therefore may not necessarily deliver optimal critical power system control. Using dedicated load controllers allows you to achieve more intelligent control in accordance with the general system design than when using a BMS.

FAT AND SAT

A Factory Acceptance Test (FAT) and a Site Acceptance Test (SAT) are great tools for verifying that you are getting the critical power system you need.



Testing is an unavoidable part of ensuring that everything works as it should

A FAT is carried out when the critical power system has been designed and constructed in the workshop, prior to onsite installation. Focusing on the control logic and controller layout, the FAT verifies that all requirements in the tender material have been met. This includes checking how everything works, verifying the user interface, and so on. Once a FAT has been completed and signed by the vendor and customer, everyone is in agreement on the layout and functionality of the system, and no details have been missed. As a customer, the FAT gives you confirmation that you are getting the system you wanted; you have seen it in action, and you know that it works as it should. If the system does not meet tender requirements, the FAT will highlight this, and you can take it up with your vendor.

Once the FAT is completed, and the solution has been installed, connected, adjusted, programmed, and commissioned, a SAT is carried out to ensure that the system actually does what it was designed to do in the application it was designed for. A SAT can include a load test of one or more gensets, and a full system test to verify that all sequences work as they should. The test verifies that the functionality verified during the FAT is also observed in actual operating conditions. When the vendor and customer are happy, the SAT report is signed, and the system is operational.

FATs and SATs are excellent verification tools for both vendor and customer

FATs and SATs are excellent verification tools for both vendor and customer. They officially record what has been achieved until now, providing a solid basis for further feature discussions. For example, if a system fails a FAT because it does not fulfil tender requirements, you can take this up with your vendor. Conversely, if you find, after having signed a FAT report, that you need more features than specified in the original tender material, your vendor is entitled to charge you for the extra work needed to develop and install them, as you have formally agreed that the solution fit your stated requirements.

"We always recommend doing these tests", says René Kristensen. *"During a FAT, we make sure that we're in complete agreement with the customer on how everything should work. And the SAT is a great way of checking that the customer gets a solution that works on site, and of spotting details that need to be adjusted if it doesn't"*.

PLAN FOR MAINTENANCE, TEST, AND COMPONENT REPLACEMENT

- Develop maintenance and testing schedules, and make sure that they are followed
- Test the critical power system under realistic operating conditions
- Replace system components as needed, and always follow manufacturer recommendations

Once your critical power system has been designed and installed, you must maintain and test it regularly. All mechanical components deteriorate over time, and you must take steps to ensure that you can rely on them when the need arises.

Perhaps the most important piece of advice is to make sure that the responsibility for carrying out maintenance and test tasks, and acting on test results when necessary, is clear within your organisation. Assign tasks to specific personnel or departments, and follow up regularly to check that they have been carried out. In a busy working week, skipping maintenance and testing of the critical power system may seem unproblematic, especially if everything seems to work and personnel resources are needed elsewhere. If such tasks are not carried out according to schedule, however, you run a significant risk of malfunctions when the critical power system is needed.

Make sure that the responsibility for carrying out maintenance and test tasks, and acting on test results when necessary, is clear within your organisation

Define a preventive maintenance schedule, and adhere to it. Always follow manufacturer recommendations to determine when you should service your breakers or replace your measuring relays, for example. Be aware of operating conditions; high humidity or heat, for example, may require you to carry out particular tasks more often than set forth in the recommendations.

Make sure that your maintenance schedule includes all components of your critical power system. Even the most insignificant component in a system can cause problems if it malfunctions in an emergency. There are several tools and procedures available for defining a maintenance schedule; one approach is to base it on the MTBF (Mean Time Between Failures) rating of individual system components.

Develop a testing schedule for the critical power system, and adhere to it. When testing the system, always do so under realistic operating conditions. It is not enough to cut the grid measuring voltage to the control system; you need to observe what happens if the grid power to everything, including breakers, goes offline. Otherwise you will not know the full consequences of a grid power failure, and you cannot take corrective action.

Always test all components that the emergency power system interfaces with. A power system is only good enough if all components actually work. For example, make sure to test the UPS or batteries powering the controllers.

Electronic components get more prone to failure as they get older

After 10 to 12 years, consider replacing the entire control system. Electronic components get more prone to failure as they get older, and particularly in hot environments, the longevity of electronic components may be significantly reduced because of material degradation. Also, replacing old controllers with new ones may mean that you get new features that increase safety and provide operational benefits such as improved connectivity, monitoring, remote control, and troubleshooting.

SAMPLE MAINTENANCE AND TESTING SCHEDULE

You can use the sample schedule below as a source of inspiration when setting up your own maintenance and testing schedules. Work with your hardware and solution vendors to develop a schedule that takes your equipment, operating conditions, and requirements into account.

Every day	Check preheating		
Every week	Partial test for 10 minutes; synchronised switching on and off of gensets		
Every month	Check oil, coolant, and fuel	Load test – gensets loaded to 80% capacity without interruption of external power supply – power from the genset is exported to the grid	System test – interruption of grid supply without synchronisation –1-hour test
Every six months	Check start battery fluid level		
Every year	Replace engine oil, oil filter, fuel filter, and air filter		
Every 3 years	Lubricate contactors / circuit breakers	Replace UPS batteries**	
Every 5 years	Replace start batteries*		
Every 10 years	Replace measuring relays on contactors / switches	Replace genset control system	

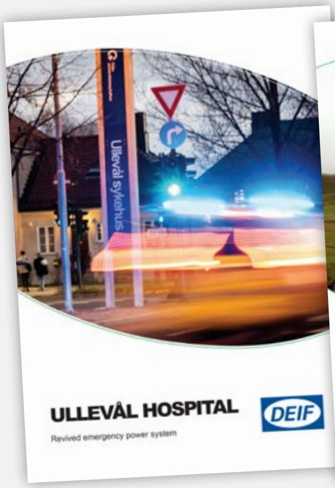
* Or as needed – measure battery voltage during start-up
** Depending on make and type, do this every third to fifth year
*** Depending on make and type, do this every 10, 15, or 20 years

CONCLUSION & CONTACT INFORMATION

Whether you need backup power from your critical power system regularly or only rarely, you must take steps to ensure that it is always available and ready for operation when the need arises. This is not just a matter of ensuring that there is sufficient fuel for the generators. Reliable critical power is the result of careful system design, installation, maintenance, and testing. In the foregoing, we have discussed some of the pitfalls that you must take steps to avoid; hopefully our advice has given you inspiration and tools that you can use to implement a system that suits your requirements and keeps your operation running.

For more information on designing critical power systems, contact DEIF. We have the experience and know-how to help you steer clear of the pitfalls and design a system that delivers the emergency power you need, when you need it.

FIND MORE INFORMATION:



Case story:
Ullevål Hospital, Norway

Ullevål Hospital goes from a decentralised, fragmented system to one with full control and remote monitoring with DEIF.

Case story:
Bakkafrost, Faroe Islands

Bakkafrost relies on DEIF for critical power control about once a month. Hundreds of millions of dollars are at stake for the Faroe Islands salmon farm

➔ **deif.com/land-power/cases**

White papers:
Find more free whitepapers, for example on the advantages of using multi-master power management systems in critical power.

➔ **deif.com/whitepapers**

DEIF A/S
Frisenborgvej 33, 7800 Skive, Denmark
Tel. +45 9614 9614