Safety Standards

of the
Nuclear Safety Standards Commission (KTA)

KTA 3701 (2014-11)

General Requirements for the Electrical Power Supply in Nuclear Power Plants

(Übergeordnete Anforderungen an die elektrische Energieversorgung in Kernkraftwerken)

The previous versions of this safety standard were issued in 1997-06 and 1999-06.

If there is any doubt regarding the information contained in this translation, the German wording shall apply.

Editor:
KTA-Geschaeftsstelle
c/o Bundesamt fuer kerntechnische Entsorgungssicherheit (BfE)
Willy-Brandt-Str. 5 • 38226 Salzgitter • Germany
Telephone +49 (0) 30 18333-1621 • Telefax +49 (0) 30 18333-1625

KTA SAFETY STANDARD

November 2014	**General Requirements for the Electrical Power Supply in Nuclear Power Plants**	KTA 3701

Previous versions of the present safety standard: 1997-06 (BAnz No. 187a of October 8, 1997)
1999-06 (BAnz No. 243b of December 23, 1999)

CONTENTS

Comments by the Editor:

Taking into account the meaning and usage of auxiliary verbs in the German language, in this translation the following agreements are effective:

shall	indicates a mandatory requirement,
shall basically	is used in the case of mandatory requirements to which specific exceptions (and only those!) are permitted. It is a requirement of the KTA that these exceptions - other than those in the case of **shall normally** - are specified in the text of the safety standard,
shall normally	indicates a requirement to which exceptions are allowed. However, exceptions used shall be substantiated during the licensing procedure,
should	indicates a recommendation or an example of good practice,
may	indicates an acceptable or permissible method within the scope of the present safety standard.

Basic Principles

(1) The safety standards of the Nuclear Safety Standards Commission (KTA) have the objective to specify safety-related requirements, compliance of which provides the necessary precautions in accordance with the state of the art in science and technology against damage arising from the construction and operation of the facility (Sec. 7 para. 2 subpara. 3 Atomic Energy Act - AtG) in order to achieve the fundamental safety functions specified in the Atomic Energy Act and the Radiological Protection Ordinance (StrlSchV) and further detailed in the Safety Requirements for Nuclear Power Plants as well as in the Interpretations of the Safety Requirements for Nuclear Power Plants.

(2) The safe enclosure of radioactive materials present in nuclear reactor plants necessitates the realization of an in-depth, multi-level technical safety concept (Defense in Depth). The present safety standard specifies the multi-level safety requirements for the measures and equipment of the electrical power supply in nuclear power plants.

(3) Based on SiAnf and the SiAnf-Interpretations, safety standards KTA 3701 through KTA 3705 specify requirements for the power supply of the safety-related power loads.

(4) The documents required in the nuclear licensing procedure for the electrical power supply of safety-related power loads are specified in ZPI, the collation of information required to be presented in the nuclear licensing and supervisory procedure for nuclear power plants.

(5) In the present safety standard, it is presumed that conventional requirements and technical standards (e.g. Accident Protection Requirements, DIN-Standards, VDE-Regulations) are adhered to under consideration of the safety-related requirements specific to nuclear power plants.

(6) The present safety standard contains the general requirements for the electrical power supply of the safety-related power loads in nuclear power plants.

(7) Requirements for emergency power generating facilities with diesel generator units in nuclear power plants are specified in safety standard KTA 3702.

(8) Requirements for emergency power generating facilities with batteries and rectifier units in nuclear power plants are specified in safety standard KTA 3703.

(9) Requirements for emergency power generating facilities with rotary converters and static inverters in nuclear power plants are specified in safety standard KTA 3704.

(10) Requirements for switchgears, transformers and distribution networks for the electrical power supply of the safety system in nuclear power plants are specified in safety standard KTA 3705.

(11) Requirements for ensuring a sustained resistance to a loss-of-coolant-accident of the electrical components and the components in the instrumentation and controls of operating nuclear power plants are specified in safety standard KTA 3706.

(12) KTA safety standards establish that the emergency power facilities end at the connection terminals of the power loads. Therefore, the requirements for the power loads are detailed in component-specific safety standards, namely KTA 3501 and KTA 3504.

(13) Requirements regarding fire protection of mechanical and electrical plant components are specified in safety standard KTA 2101.3.

(14) Requirements regarding lightning protection are specified in safety standard KTA 2206.

(15) Requirements regarding cable penetration through the reactor containment vessel are specified in safety standard KTA 3403.

(16) General requirements regarding quality assurance are specified in safety standard KTA 1401.

(17) Requirements regarding the testing manual are specified in safety standard KTA 1202.

(18) Requirements regarding the design of mechanical and electrical components in nuclear power plants against seismic events are specified safety standard KTA 2201.4.

1 Scope

The general requirements specified in this safety standard apply to the electrical power supply of those equipment in nuclear power plants that perform functions of safety-related significance during normal and abnormal plant operation and also during the control of design basis accidents.

Note:

The requirements for the equipment of the electrical power supply (e.g., regarding their circuit design concepts and design) differ according to safety-related significance of the supplied equipment. Accordingly, the present safety standard deals with the “Offsite power connections and station service facility” and the “Emergency power system” in separate sections.

2 Definitions

(1) Station service facility

The station service facility is the entirety of those plant components that serve to supply the connected power loads and to feed power into the emergency power system.

(2) Station service power

The station service power is the electrical power required for supplying the power loads necessary for the operation of a power plant unit and for supplying the emergency power system.

(3) Functional separation of offsite power connections

Offsite power connections are considered as functionally separated if neither of the two connections can influence each other through direct coupling. This requires, among others, a net topology that makes it possible for a nearby redundant power source to supply at least one of the two offsite power connections.

(4) Main offsite power connection

A main offsite power connection is the power connection through which the nuclear power plant unit delivers electrical power to, and can also draw electrical power from, the offsite power grid. The main offsite power connection comprises all electrical equipment between the low-voltage terminals of the main transformer and the busbar terminals of the power switch in the grid switchgear.

(5) Main offsite power connection, two-part

A two-part main offsite power connection is a main offsite power connection which, regarding electrical function and protection, consists of two separate interconnections between power plant and offsite power grid.

(6) Offsite power connection

An offsite power connection is an interconnection between the power plant and offsite power grid by which electrical power can be transmitted.

(7) Emergency power facility

An emergency power facility is the combination of a specific emergency power generating facility including all plant components that are necessary for the (emergency power) supply of the corresponding power loads.

(8) Emergency power operation

Emergency power operation implies that the power for the train is supplied by the respective emergency power facility.

(9) Emergency power (grid) connection

An emergency power connection is an offsite power connection by which electrical power can be drawn for the supply of emergency power loads. The emergency power connection comprises all electrical equipment between the power switches in the station service facility or in the emergency power facilities and the busbar terminals of the power switch in the grid switchgear or in an energy source independent of the emergency power system of the nuclear power plant.

(10) Emergency power system

The emergency power system is the entirety of the different emergency power facilities – different regarding power generation and task – in a nuclear power plant.

(11) Emergency power load

An emergency power load is a power load that is supplied from an emergency power facility.

(12) Supplying emergency power

Supplying emergency power means supplying the emergency power loads from emergency power generating facilities.

(13) Uninterruptible emergency power supply

An uninterruptible emergency power supply is an emergency power supply where the power supply from the emergency power facility sets in without interruption in case of failure of the power supply from the station service facility or from the offsite power connections.

(14) Additional offsite power connection

An additional offsite power connection is an offsite power connection from which at least that amount of electrical power can be drawn that is necessary for shutting down the nuclear power plant while sustaining the main heat sink. The additional offsite power connection comprises all electrical equipment between the power switches in the station service facility and the busbar terminals of the power switch in the grid switchgear.

(15) Station service switchover (short-term, long-term switchover)

A station service switchover is the switchover of the electrical station service supply from the main offsite power connection to the additional offsite power connection. Two cases are distinguished between:

a) Short-term switchover

   This is a switchover with an interruption time no more than a few milliseconds. A short-term switchover is performed when the voltages at the main offsite and additional offsite power connections – regarding amplitude, frequency, phasing and phase sequence – are identical or insignificantly different within a specified tolerance range.

b) Long-term switchover

   This is a switchover with an interruption time of a few seconds. A long-term switchover is performed when the voltages at the main offsite and additional offsite power connections – regarding amplitude, frequency, phasing and phase sequence – are larger than admissible for a short-term switchover. The switchover may be carried out depending on the residual voltage, i.e., only after the lessening voltage in the station service facility falls below a lower limit value, or it may be carried out after a preset time limit.

3 General Requirements

(1) For the electrical power supply of a nuclear power plant unit regarding heat removal while sustaining the main heat sink at least two offsite grid supply possibilities shall be available.

Note:

The terminology “heat removal while sustaining the main heat sink” implies heat removal using power loads that are connected to the station service facility.

(2) The following power supply possibilities shall be available for the electrical power supply of the safety-related power loads in a nuclear power plant unit:

a) the main generator of the nuclear power plant,

b) two offsite grid connections,

c) emergency power facilities with diesel generator units and with batteries on the nuclear power plant site, and

d) one emergency power (grid) connection or one power supply facility that is independent of the emergency power generating facilities of the nuclear power plant.

   Note:

   The term “emergency Power (grid) connection” is used in the following to reference both of these power supply possibilities.

Note:

Appendix A shows examples of circuit design concepts for the electrical power supply of a nuclear power plant.

(3) In a multi-unit nuclear power plant, each nuclear power plant unit shall be equipped with an individual emergency power system that is assigned to that one plant unit alone.

(4) Power may be demanded from the emergency power generating facilities only if the possibilities specified under para. (2), items a) and b), for supplying electrical power to safety-related power loads are not simultaneously available. However, a power demand from one train of the emergency power generating facility is admissible for testing purposes.

(5) The electrical power supply to the safety-related power loads shall be designed to be of such reliability that this supply is not the determining factor of the unavailability of the supplied systems.

(6) The electromagnetic compatibility of components shall be demonstrated dependent on their safety-related significance.

(7) The reliability of the electrical power supply of safety-related power loads shall be demonstrated. In this context, all components and auxiliary systems of the electrical power supply shall be taken into account.

4 Offsite Power Connections and Station Service Facility

4.1 General Requirements

4.1.1 Requirements for the circuit design concepts

(1) The circuitry and spatial arrangement of the offsite power connections and the station service facility shall be such that a single failure initiating event inside the nuclear power plant or a single failure initiating event within the electrical power supply of the nuclear power plant or near the offsite power connections cannot cause a longer failure of all offsite grid supply possibilities. Such a failure initiating event and its mechanical sequential damages (e.g., broken mast, cable breakage) shall not lead to a mechanical failure of all of the power supply connections specified under Section 3, para. (2), items b) and d).

(2) Equipment shall be installed that, in case of a separation of the power plant unit from the offsite power grid, would automatically cause a switchover of the power plant unit to station service power (load shedding to station service power).

4.1.2 Interconnections of the offsite power connections or the station service facility with the emergency power system

(1) Interconnections of the offsite power connections or the station service facility with the emergency power system shall be designed such that they are automatically disconnected in case of failure of the plant unit's onsite and offsite grid supply possibilities. The equipment for reconnecting to the re-available offsite power connections or station service facility shall be designed such that each redundant train of the emergency power system can individually be reconnected.

(2) Unavoidable operational influences (e.g., from switching operations or ground shorts in the station service facility) shall not cause any systematic failures in the emergency power system.

(3) Externally or internally caused failure-related electrical transients or fault conditions (e.g., voltage drop, overvoltage, consequences of a phase failure, short-circuits, lightning effects on power lines) shall not lead to any inadmissible impairments of safety-related equipment. The respective proof may be performed experimentally or by simulation.

4.1.3 Testability

(1) The equipment of offsite power connections and the station service facility that serve to supply the emergency power system shall be designed such that they can be checked regularly and completely during a power plant unit shutdown and, as far as necessary for reliability reasons, also during normal operation.

(2) Tests and inspections shall not prevent necessary protective actions.

4.1.4 Monitoring

The equipment of the offsite power connections and station service facility that serve to supply the emergency power system shall be monitored by measurements and signals regarding their functional capability and operating condition.

4.2 Offsite Grid Supply Possibilities

4.2.1 Design

(1) Each one of the two offsite grid supply possibilities specified under Section 3, para. (2), item b), shall by itself be able to supply all trains of the emergency power system.

(2) The offsite grid supply possibilities specified under Section 3, para. (2), items b) and d), shall be functionally separated and protectively decoupled from each other.

(3) The offsite power grid connections specified under Section 3, para. (2), item b), shall normally be connected to different voltage levels. If this is not possible due to the grid conditions near the nuclear power plant, the offsite power sources shall at least be connected to separate switchgears and protectively decoupled from each other.

(4) The additional offsite power grid connection shall be designed such that it can enable shutdown of the nuclear power plant unit while sustaining the main heat sink. The dynamic loadings from a long-term switchover during a design basis accident shall be taken into account.

(5) In case of demand, the additional offsite power connections shall be automatically connected. The triggering criteria and triggering limit values and the time delays for these automatic connections shall be specified in coordination with the emergency power generating facilities such that the emergency power generating facilities are not unnecessarily connected. The design of the station service switchover shall normally by such that, both, a short-term switchover as well as a long-term switchover can be performed.

(6) The additional offsite power connections may be mutually used by several nuclear power plant units. A mutually used additional offsite power connection shall be designed such that it can enable the simultaneous shutdown of all supplied nuclear power plant units while sustaining the main heat sinks.

(7) The emergency power (grid) connection and its power supply points in the nuclear power plant shall be designed such that – regarding residual heat removal of the nuclear power plant unit – the minimum electrical power required for supplying one residual heat removal train including all necessary instrumentation, control and auxiliary equipment is made available.

Notes:

(1) Regarding the required electrical power for the residual heat removal, no additional superposed design basis accident (e.g., loss-of-coolant accident) need be assumed.

(2) In the case of nuclear power plants with emergency residual heat removal systems, one emergency residual heat removal train may be sufficient for residual heat removal.

(8) The emergency power (grid) connections shall normally allow for their manual connection in a demand case. An automatic connection is admissible, provided, the power of the emergency power (grid) connection is designed for the maximum automatically connectable power load.

(9) Emergency power (grid) connections may be mutually used by multiple nuclear power plant units. The power of the mutually used emergency power (grid) connection shall be designed for a simultaneous residual heat removal of all connected nuclear power plant units and the power specified under para. (7).

(10) At least one interconnection to the offsite grid (e.g., the emergency power (grid) connection) shall, in the near vicinity of the nuclear power plant, be constructed as a ground-buried cable connection.

4.2.2 Measures upon failures of the offsite power supplies

(1) The repair of failed offsite net connections shall be initiated without delay.

(2) In case of external hazards a simultaneous failure of the main and additional offsite power connections in the near vicinity of the nuclear power plant cannot be ruled out; thus, it is necessary that, within three days, either one offsite net connection shall be repaired, or another supply possibility made available.

(3) The electrical power of the supply possibilities specified under para. (2) shall be sufficient for removing the residual heat and for preventing any inadmissible release of radioactive materials. In case of multi-unit power plants, the corresponding electrical power shall be sufficient for all nuclear power plant units.

4.3 Operation and Maintenance

(1) All components of the electrical power supply of safety-related power loads shall normally be designed and arranged with regard to enabling a clear overview, easy maintenance and short repair times (e.g., by accessibility and exchangeability).

(2) Unambiguous instructions for the operation and maintenance shall be available. The respective manufacturer specifications shall be taken into account.

(3) Functional degradations and damages shall be removed without delay.

(4) The operation and maintenance of software-based equipment shall meet the requirements of the plant-specific IT-safety concept considering the therein specified safety levels.

4.4 Quality Assurance, Tests and Inspections

4.4.1 General Requirements

The objective of quality assurance is to demonstrate for the components of the electrical power supply of safety-related power loads that the demand frequency of the emergency power generating facility is minimized.

Note:

General requirements for quality assurance are specified in KTA 1401.

4.4.2 Commissioning Tests

Commissioning tests shall be performed to demonstrate the function of the electrical power supply in their interaction with the process engineering systems and the instrumentation and control equipment. The commissioning tests shall normally be performed under the most realistic conditions possible.

5 Emergency Power System

5.1 Boundary Limits of the Emergency Power System

The emergency power system comprises all electrical equipment including the corresponding auxiliary system starting from the infeed switches of the emergency power facilities to the connection terminals of the emergency power loads.

Note:

Appendix B shows an example for the boundary limits of an emergency power system.

5.2 Basic Requirements

(1) All safety-related power loads of a nuclear power plant unit shall be connected to emergency power facilities. These power loads shall, in particular, be those required to safely shutdown the reactor, to keep the reactor in the shutdown condition, to remove the residual heat and to prevent any inadmissible release of radioactive substances.

(2) The emergency power switchgears shall at all times be kept energized such that the emergency power loads can draw their power from the station service facility or from an offsite grid connection and, in case the aforementioned power supplies fail, from the emergency power generating facilities.

(3) In the design of the emergency power facilities,

a) a simultaneous failure of the plant unit's onsite and offsite power supply, and

b) a failure of the unit's onsite power supply with continued power supply from the offsite power grid

shall each be superposed with one of the accidents or one of the external hazards considered in the design of the nuclear power plant.

(4) The design of the emergency power facilities shall, additionally, take the dynamic loads from a simultaneous occurrence of a long-term switchover and design basis accident into account.

(5) The design of the emergency power facilities shall ensure that the electrical conditions for the corresponding power loads are fulfilled even under the most unfavorable ambient conditions and the operation related and accident related loadings.

Note:

The electrical conditions for the supply of the consumers include, in particular, the allowed tolerances of voltage, current or frequency both in the static and in the dynamic range.

(6) A sufficient power production and operational availability of the emergency power system shall be ensured over the entire operating life of the nuclear power plant.

5.3 Protection against Failure Initiating Events within the Emergency Power System

(1) The emergency power system shall be designed, constructed and operated such that failure initiating events within the emergency power system and within the correspondingly supplied emergency power loads will not prevent the required supply of emergency power in a demand case. The following failure initiating events within the emergency power system shall be considered:

a) random failures of components of the emergency power system, i.e., single failures that shall be covered by redundancies as specified Section 5.6, and

b) common cause failures, such as multiple failures occurring simultaneously or in short succession of each other that have a common cause within the system itself.

(2) The possibility and effects of common cause failures in the emergency power system shall be analyzed. Depending on the results of these analyses, additional measures shall be taken at the component or the system level such that a violation of the protective goals (cf. Basic Principles, para. (1)) does not anymore have to be assumed (robustness against common cause failures).

Notes:

(1) In the case of electromechanical components or simple electronic modules, the probability of occurrence of common cause failures can be reduced largely enough (e.g., by choice of suitable components, test cycles, critical load tests) such that no additional measures against common cause failures are required.

(2) In the case of components that contain complex (programmable or non-programmable) electronic modules for performing protective, controlling and monitoring functions, a significantly higher common cause failure potential must be assumed than in the case of electromechanical or simple electronic modules. To avoid that common cause failures will affect more than one redundancy, fault- controlling and fault-preventing measures are available at the component level and fault-controlling measures at the system level.

5.4 Protection against Failure Initiating Events within the Nuclear Power Plant

The emergency power system shall be designed, constructed and operated such that failure initiating events within the nuclear power plant will not prevent the required emergency power supply in a demand case. Failure initiating events within the nuclear power plant, e.g., fire or pipe rupture, shall be considered.

5.5 Protection against External Hazards

(1) The emergency power facilities shall be protected against the same external hazards as the process engineering systems the power loads of which are supplied by these emergency power facilities and which must remain functional during and after the external hazard. The protection concept of the emergency power facilities against external hazards shall be coordinated with the protection concept of the corresponding process engineering systems.

(2) The protection concept of the emergency power systems shall take into account that, in case of a failure of individual equipment caused by very rare human induced external hazards not considered in the design of the equipment, other equipment will fulfill the safety related task.

5.6 Redundancy

The circuit design concepts of the process engineering systems and the corresponding emergency power facilities shall be coordinated such that the redundancy of the emergency power generation and distribution systems corresponds to the redundancy of the process engineering systems. The emergency power system shall fulfill its function even during tests or repair procedures and the simultaneous occurrence of a single failure only as far as this requirement also applies to the corresponding process engineering systems. In the overall analysis of a design basis accident, the occurrence of a single failure and the repair case shall be assumed once in the entirety of the equipment and facilities available for the control of the design basis accident.

5.7 Functional Independence

(1) In order to be functionally independent, the emergency power system shall consist of redundant non-interconnected trains each of which has individual feed-ins as well as individual emergency power generating and distribution facilities, cable ducts and auxiliary systems.

(2) In exceptional cases emergency power loads may be supplied from more than one train of an emergency power facility, if the required reliability of the supplied system can, thus, be achieved and it is demonstrated for each individual case that the reliability of the emergency power system is not inadmissibly reduced by this measure. These interconnections shall be designed such that no failure possibility to be considered can cause the sequential failure of more than one train.

5.8 Spatial Separation

The redundant trains of the emergency power facilities shall be spatially separated or protected from each other such that failure initiating events in one train cannot affect other trains and, also, that an individual, plant internal failure initiating event will not lead to the failure of more than one train.

5.9 Emergency Power Balances

(1) Power balances shall be prepared taking all accidents of the design basis accident analysis of the nuclear power plant into account. This applies in particular to the failure of the plant unit's onsite and offsite power supply that occur

a) without a simultaneous failure within the process engineering systems,

b) simultaneously with one of the considered design basis accidents in the process engineering systems, and

c) simultaneously with one of the considered external hazards.

(2) The power demand shall be determined individually for each train of the emergency power system.

(3) In addition to all of the electrical power loads supplied by the emergency power facilities, the machines directly driven by the emergency power generators shall be included in these power balances.

(4) In preparing the power balances, the sequentially various power requirements during the individual accident sequences to be considered shall be taken into account.

(5) The power balances shall take the static operating range and transient procedures into account.

(6) When initially creating the power balances, the uncertainties in the concept of the electrical power supply shall be accounted for by including a safety margin.

Note:

Component specific safety margins are specified in safety standards KTA 3702 through KTA 3704.

(7) The power balances shall be updated regularly and shall not be older than five years.

5.10 Interruption and Delay Durations

(1) The interruption or delay durations admissible for each emergency power load shall be determined regarding the time span between a failure of the plant unit's onsite and offsite power supply and the setting in of the emergency power generation facilities. The power load groups shall be correspondingly assigned to the respective emergency power facilities.

(2) The equipment of these emergency power facilities shall be designed such that the admissible interruption and delay durations are not exceeded.

Note:

The admissible interruption and delay durations result from the design basis accident analysis of the individual power plant.

5.11 Initiation and Termination of Emergency Power Operation

(1) The emergency power operation shall be initiated whenever the power supply of the corresponding emergency power busses from the station service facility fails or is not anymore within the tolerances for voltage or frequency admissible for the emergency power load.

Note:

The requirements for the equipment for generating and processing the signals for initiating the emergency power operation are specified in safety standards KTA 3501 and KTA 3702.

(2) The emergency power facilities shall be designed such that, for a period of at least 30 minutes after demand of an emergency power generating facility, no manual actions are required for the operation of the emergency power facilities.

(3) If the control of design basis accidents requires a longer period than 30 minutes without manual actions, this shall also apply to the corresponding emergency power facilities.

(4) The emergency power operation shall normally be terminated as soon as the supply from the station service facility or from a sufficient other source is again reliably available.

(5) When ending the emergency power operation, certain types of emergency power diesel generators cannot be restarted during the phase of shutting-down. A renewed demand case during this phase shall be taken into account.

Note:

Shutting down these types of emergency diesel generators may be carried out, e.g., train by train in staggered intervals.

5.12 Protection

The engineered protection equipment in the emergency power system shall be designed such that defects or failures are reliably detected, that the necessary disconnections are performed and erroneous actuations from operational transients are prevented. An actuation of the engineered protection equipment shall initiate appropriate alarms.

Note:

Component specific requirements are specified in safety standards KTA 3702 through KTA 3705.

5.13 Testability

(1) The equipment of the emergency power system shall be designed such that a regular and complete inspection is possible during plant unit shutdowns and, if required for reliability reasons, also during normal operation.

(2) The equipment of the emergency power system shall normally be designed such that the inservice inspections specified in Section 5.16.5 can be performed and that no manipulation of the wiring will be required.

Note:

The opening of disconnect terminals, e.g., is not considered to be a manipulation of the wiring.

(3) Tests and inspections shall not prevent necessary protective actions.

(4) Defects or failures occurring during tests and inspections in the train tested shall not cause failures in other trains.

5.14 Monitoring

The equipment in the emergency power system shall be monitored by measurements and alarms regarding their functional parameters to ascertain their functional capability and operating condition.

5.15 Operation and Maintenance

(1) All components of the emergency power supply shall normally be designed with special regard to clear overview, easy maintenance and short repair times (e.g., by accessibility and exchangeability).

(2) Unambiguous instructions shall be available for operation and maintenance. The respective manufacturer specifications shall be taken into account.

(3) Functional degradations and damages shall be repaired without delay.

(4) If a random failure including sequential failure occurs during repair work within the emergency power system and the remaining part cannot fulfill its safety function, then the reactor plant shall be brought into a safe condition.

Note:

A safe condition can be achieved, e.g., by an immediate repair or by shutting down the reactor plant. Immediate repair shall be given preference in those cases where the repair work can be concluded faster than the shutdown of the reactor plant.

(5) The operation and maintenance of software-based equipment shall meet the requirements of the plant-specific IT-safety concept considering the therein specified safety levels.

5.16 Quality Assurance, Tests and Inspections

5.16.1 General requirements

(1) The quality assurance for the emergency power system components shall be demonstrated.

Note:

General requirements for quality assurance are specified in KTA 1401. The component specific requirements regarding quality assurance are specified in safety standards KTA 3702 through KTA 3705.

(2) All information necessary regarding an unambiguous identification of the configuration of components of the emergency power system shall be specified.

Note:

This may be carried out in form of a specific configuration-identification documentation.

5.16.2 Design review

Regarding the design review by the proper nuclear authority or its appointed authorized expert (under Sec. 20 AtG), documented proof shall be provided that the electrical components, electrical modules, components and systems have been designed, tested and assembled in accordance with the safety-related requirements.

5.16.3 Demonstration of suitability, type tests and routine tests

(1) After completion of the development of the component type, type tests shall be performed on fabrication samples to demonstrate the essential characteristics of the component. A type test, e.g., in accordance with VDE-Provisions, may be accepted as valid demonstration.

(2) If the deployment in nuclear power plants requires safety characteristics (e.g., resistance to design basis accident conditions and to seismic events) which cannot be demonstrated by the type-test, then supplementary qualification tests shall be performed. The resilience to the most unfavorable ambient conditions at the place of installation shall be demonstrated.

(3) Staggered qualification requirements may be specified for the components of the emergency power system in accordance with the different safety-related significance of the supplied equipment.

(4) If the analysis specified under Section 5.3, para. (2), leads to the requirement of robustness of the components against common cause failures, then supplementary proofs shall be presented within the framework of the suitability or type tests. In the case of complex (programmable or non-programmable) electronic modules the proof shall be performed as specified in **Appendix C**.

(5) Routine tests shall be performed with the goal of detecting material and fabrication defects. They shall basically be performed on each piece of the delivered lot. In the case of series produced items, tests on random samples are admissible based on the statistical certainty involved.

(6) A routine test performed in accordance with VDE-Provisions is acceptable, provided the application in the nuclear power plant does not require proof of additional safety characteristics. Otherwise, expanded routine tests shall be performed. In this context, it shall be demonstrated that product-specific fabrication tests were performed.

5.16.4 Commissioning tests

Commissioning tests shall be performed to demonstrate the fulfillment of the specified safety-related requirements and of the functioning of the electrical power supply in its interaction with the power plant and the process engineering systems and the instrumentation and control equipment. The commissioning tests shall normally be performed under the most realistic operating conditions possible.

5.16.5 Inservice inspections

Inservice inspections shall be performed to ascertain that the functional capability of the electrical power supply is maintained. They shall be performed during operation or during shutdown of the nuclear power plant and in specified time intervals that are obtained from reliability considerations and from a mutual coordination with the functional tests of the respective process engineering systems.

5.16.6 Testing after maintenance or repair

(1) After completion of any maintenance and repair tasks which had required an interruption of the functional capability, the restoration of this functional capability shall be demonstrated by an enveloping test.

(2) In as far as the deployment of modified equipment becomes necessary, this equipment shall fulfill the requirements specified under Section 5.16.3.

5.16.7 Test documents

Test documents shall be provided which specify the individual tests and inspections corresponding to the different test types. Additionally, the required auxiliary means and equipment for testing and the preparations for testing shall be specified.

5.16.8 Testers

(1) The type tests specified under Section 5.16.3 shall be demonstrated by test reports presented to the proper nuclear authority or its appointed authorized expert (under Sec. 20 AtG). The qualification tests specified under Section 5.16.3 shall be performed in agreement with the proper nuclear authority or its appointed authorized expert (under Sec. 20 AtG).

(2) The routine tests specified under Section 5.16.3 may be performed by plant experts. Additionally, it shall be specified in the course of the design review, which of the tests specified under Section 5.16.3 shall be carried out in the presence of the proper nuclear authority or its appointed authorized expert (under Sec. 20 AtG).

(3) The commissioning tests specified under Section 5.16.4 shall be carried out in agreement with the proper nuclear authority or its appointed authorized expert (under Sec. 20 AtG).

(4) The inservice inspections specified under Section 5.16.5 and the testing after maintenance or repair specified under Section 5.16.6 shall be performed by the power utility in agreement with the proper nuclear authority or its appointed authorized expert (under Sec. 20 AtG).

5.16.9 Test Certificates

(1) All tests performed shall be documented by a test certificate in accordance with safety standard KTA 1202, Sec. 3.5.

(2) The tests and inspections specified under Section 5.16.3 shall be documented by test certificates.

6 Interconnections between the Units of a Multi-Unit Nuclear Power Plant

6.1 Deployment Conditions

(1) The use of interconnections between the three-phase alternating current power facilities of the plant units is admissible, provided, they are carried out with the goal of

a) preventing start-ups of emergency power generators during planned shut-downs in the station service facility (maintenance),

b) reducing the operating time of emergency power generators in case of demand, and

c) creating an alternative power supply in case of an unavailability of emergency power generators when these emergency power generators are demanded.

(2) Electrical power interconnections shall normally not be planned between the direct current busses of neighboring nuclear power plant units.

(3) Direct current power loads may be supplied from direct current power facilities of neighboring nuclear power plant units, provided, the feed-in is reliably de-coupled.

6.2 Basic Requirements

(1) Interconnections between nuclear power plant units shall be designed for the electrical power to be transmitted. The upper and lower limit values of voltage and frequency admissible for the individual power loads shall be observed.

(2) Only one type of design shall normally be used for the interconnections between nuclear power plant units.

Note:

Appendix D shows examples for the design of interconnections between the nuclear power plant units.

(3) The electrical power to be supplied through interconnections to other nuclear power plant units shall be taken into account when designing station service facilities, emergency power generating and emergency power distribution facilities.

(4) The interconnections between the switchgears of nuclear power plant units shall be designed and operated such that they do not determine the non-availability of the power supply for the safety-related power loads in the individual nuclear power plant units.

6.3 Circuit Design Concept

(1) The circuit design concept of the interconnections between the station service switchgears of neighboring nuclear power plant units shall be correlated to the subdivisions of these facilities.

(2) The circuit design concept of the interconnections between the emergency power switchgears of neighboring nuclear power plant units as well as of the connections between the station service switchgear of one nuclear power plant unit and the emergency power switchgear of another nuclear power plant unit shall be in accordance with the train design concepts of the respective emergency power facilities.

(3) It shall be possible to disconnect the interconnections between nuclear power plant units at either end.

6.4 Selectivity

The individual interconnections between nuclear power plant units shall be equipped with engineered protection equipment such that the selectivity within each nuclear power plant unit is maintained.

6.5 Monitoring and Interlocking

(1) In each nuclear power plant unit, the switching and load condition shall be displayed for those parts of the interconnections that are part of the respective nuclear power plant unit.

(2) Inadmissible switching conditions shall be prevented, preferably, by technical means and by supplementary administrative measures.

(3) Signaling links between the plant units shall be galvanically decoupled.

6.6 Quality Assurance, Tests and Inspections

6.6.1 General requirements

The quality assurance of the interconnections between the units of a multi-unit nuclear power plant shall be demonstrated.

Note:

General requirements for quality assurance are specified in KTA 1401.

6.6.2 Commissioning tests and inspections

Commissioning tests and inspections shall be performed to demonstrate that the specified requirements are met. The commissioning tests and inspections shall normally be performed under conditions that are as realistic as possible.

7 Additional Requirements for the Interconnections between Emergency Power Facilities of the Units of a Multi-Unit Nuclear Power Plant

7.1 General Requirements

The interconnections between the emergency power switchgears of nuclear power plant units and the interconnections between the station service switchgear of one nuclear power plant unit and the emergency power switchgear of another nuclear power plant unit shall meet the requirements of Section 6 and, additionally, of Sections 7.2 through 7.5.

7.2 Functional Independence

Interconnections to emergency power switchgears shall be designed such that none of the failure possibilities to be considered can lead to the failure of more than one train of the emergency power system in each nuclear power plant unit.

7.3 Spatial Separation

The train-to-train interconnections between emergency power switchgears of neighboring nuclear power plant units shall be either spatially separated or protected from each other such that failure initiating events in one train-to-train interconnection cannot affect any other train-to-train interconnection and that a single plant-internal failure initiating event will not lead to the failure of more than one train-to-train interconnection.

7.4 Activating Interconnections

(1) The interconnections shall normally be activated by manual actions only. The activation of more than one interconnection shall be carried out sequentially one train after another.

(2) Emergency power generation facilities of neighboring nuclear power plant units shall normally not be operated in parallel via interconnections.

(3) A synchronization and short-duration parallel operation of emergency power generators of one nuclear power plant unit with the power feed-in from another nuclear power plant unit is admissible if required to achieve an uninterrupted switchover.

7.5 Disconnecting Interconnections

In case of initiating signals demanding emergency power operation in one train of a nuclear power plant unit, the interconnections from the emergency power switchgear of this train to other nuclear power plant units shall automatically be disconnected.

Appendix A

Examples of Circuit Design Concepts for the Electrical Power Supply of a Nuclear Power Plant

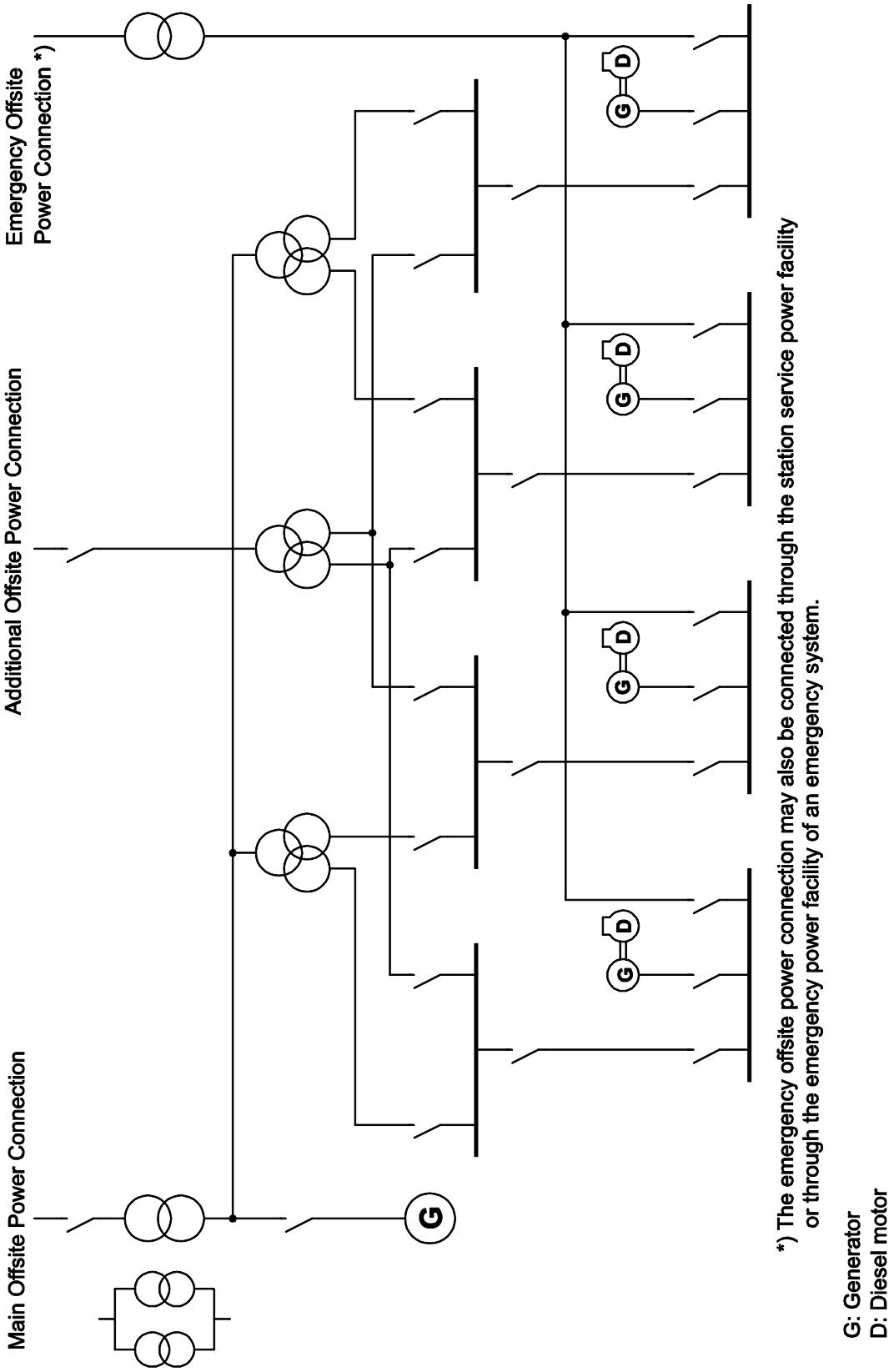


Figure A-1: Example of a circuit design for a nuclear power plant with one main offsite power connection, one additional offsite power connection and one emergency power (grid) connection

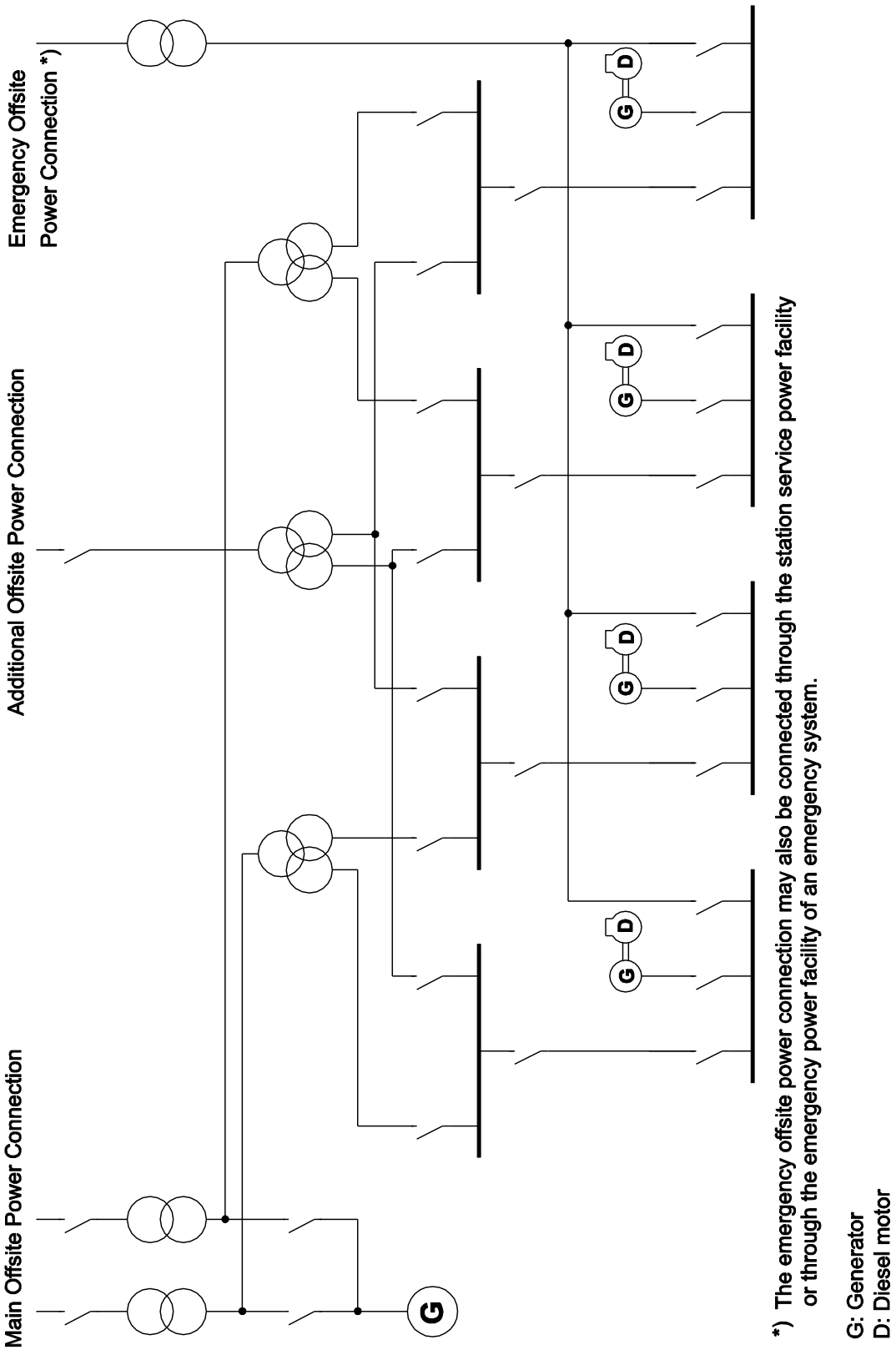


Figure A-2: Example of a circuit design for a nuclear power plant with a two-part main power connection, an additional offsite power connection and one emergency power (grid) connection

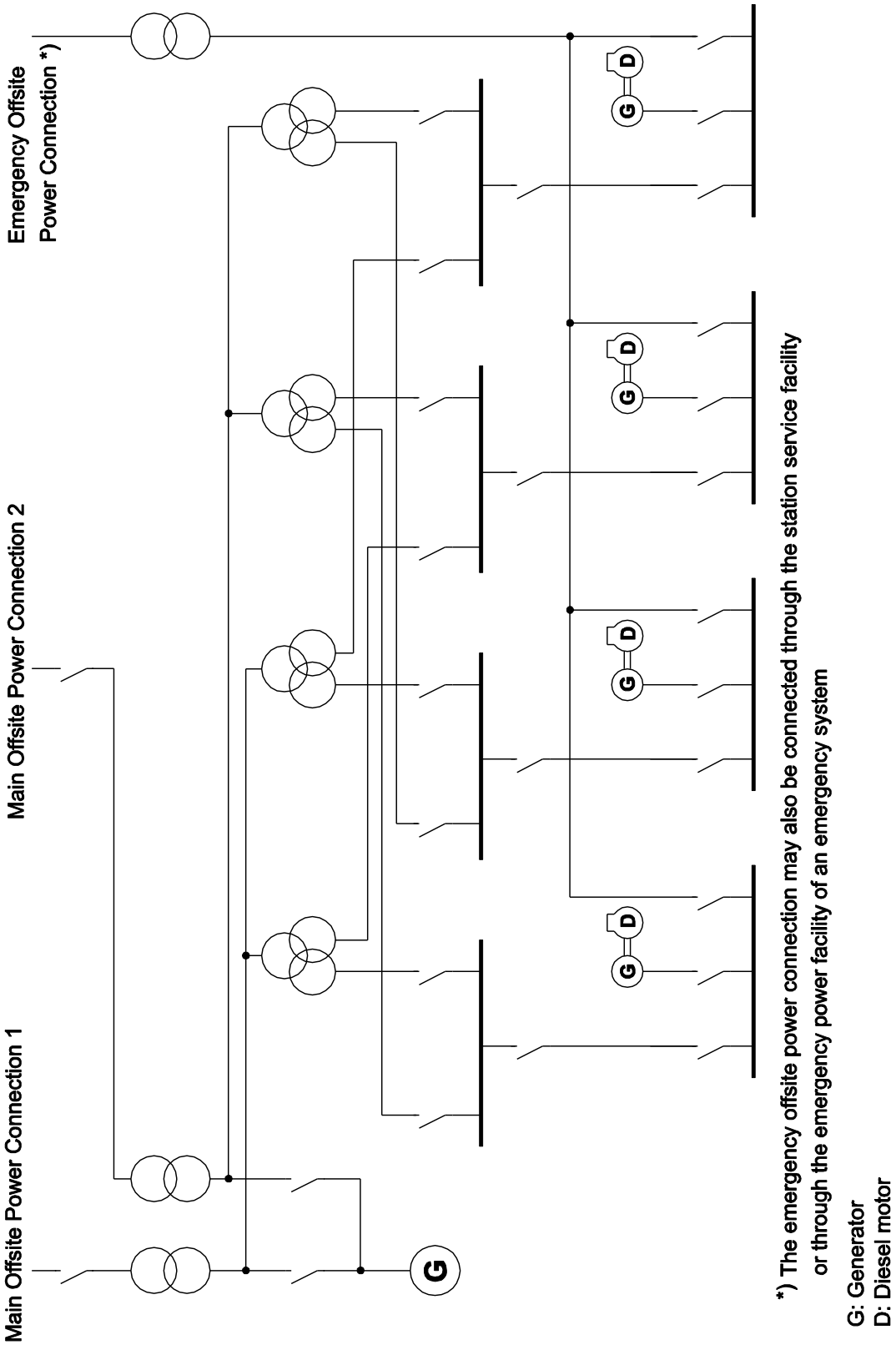
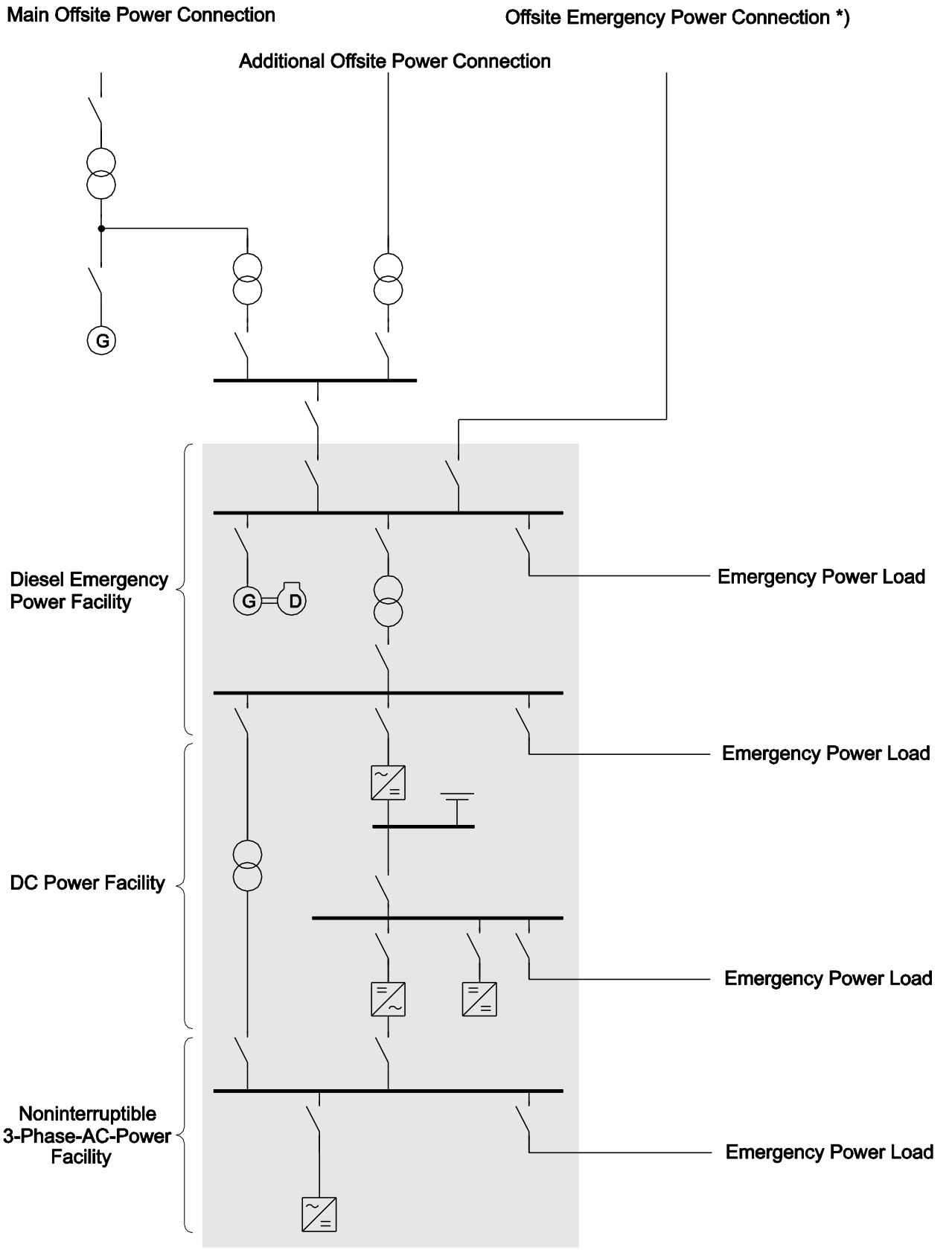


Figure A-3: Example of a circuit design for a nuclear power plant with two main offsite power connections and one emergency power (grid) connection

Appendix B

Boundary Limits of an Emergency Power System



G: Generator
D: Diesel Motor

*) The Offsite Emergency power connection may also be connected through the station service power facility or through the emergency power facility of an emergency system.

Figure B-1: Schematic representation of the boundary limits of an emergency power system (shown for one train)

Appendix C

Additional Testing of Components of the Electrical Power Supply Containing Complex (Programmable or Non-Programmable) Electronic Modules to Demonstrate their Robustness Against Common Cause Failures

C.1 General Requirements

(1) For the theoretical analysis of the prevention of common cause failures at least the documents specified under Sections C.2 through C.4 shall be presented. These documents shall be checked, particularly, regarding their completeness and consistency, and regarding the functional design of the modules.

(2) Testing instructions shall be prepared for the physical tests to be performed. These instructions shall describe the test objectives, the type of tests, the test parameters and their values, the test equipment and the test execution (test sequence and extent of individual test steps). Three test objects shall be made available for the physical tests on the modules.

(3) The theoretical and physical tests performed, and the test results shall be documented in a test report in which the achievement of the test objectives shall be certified.

(4) Instead of following the procedure specified under para. (1), (2) and (3) it is admissible to present comparable certifications.

Note:

Comparable certifications can be based, e.g., on the combination of the SIL 3 qualification in accordance with DIN EN 61508, of the certification of proven performance and additional test certificates based on comparisons with nuclear standards.

C.2 Documents

(1) All module related documents shall contain information on the manufacturer, type and modification state of the modules and information on the respective software. This includes to the documents specified under Section C.3 and C.4.

(2) The extent and level of detail of the documents to be presented shall be coordinated with the proper nuclear authority or its appointed authorized expert (under Sec. 20 AtG),

(3) The following documents shall be presented for the modules:

a) Information for ascertaining the identity of the modules,

b) Description of the function of the modules including the scope of application, task and workings of the modules,

c) Data sheet containing at least the following data – unless this data is contained in the component data sheet:

  ca) electrical characteristics (e.g., over-voltage category, admissible voltage and frequency range),

  cb) input parameters,

  cc) output parameters,

  cd) auxiliary power,

  ce) admissible ambient conditions,

  cf) operating behavior (e.g., behavior upon loss and return of the voltage supply, reaction times)

  cg) interfaces and communication protocols.

d) Operating instructions containing at least the following information – unless this information is contained in the component operating instructions:

  da) installation,

  db) commissioning,

  dc) adjustment settings,

  dd) extra equipment,

  de) servicing,

  df) packaging and storage.

(4) In the case of modules containing discrete components, the circuit diagram shall depict all components of the module and their interconnections.

(5) In the case of modules containing highly integrated components (chips), the connection plan shall depict all electrical and data-technological connections of the module.

(6) The parts list shall list all mechanical and electrical components of the module that are necessary for evaluating the function of the module.

(7) The layout schematic of the components shall depict the arrangement of the components.

(8) The manufacturing quality of the modules shall be documented.

(9) The development process (of the modules) shall be documented.

Note:

These documents shall comprise, e.g.

a) specification of requirements,
b) customer specifications,
c) performance specification,
d) design documents,
e) testing documentation,
f) configuration management,
g) documented modification procedure,
h) documentation of the development and testing tools, and
i) effects analysis (FMEA).

(10) In addition, the following information shall be made available:

a) structure, program sequence and time response of the software,

b) configuration, parameter setting and testing possibilities of the components or modules and the respective software tools,

c) conditions and procedure to observe when configuring and parameterizing,

d) specification of the interface to other modules or components and of the data to be transferred,

e) the qualification test procedure and test results in case of deploying pre-developed software,

f) certification of the qualification tests for the deployed project planning tools and procedures,

g) protective measures against inadmissible manipulation of the software,

h) possibilities for detecting, alarming and documenting manipulations of the software,

i) implemented self-monitoring mechanisms of the hardware and software, and

j) behavior of the modules when the monitoring or the error-handling routines are triggered.

C.3 Determining the Reliability Parameters

(1) The reliability parameters shall be determined by evaluating the operating experience with the components or modules.

Note:

In this context, e.g., experience from the deployment in industrial facilities may be used.

(2) The failure rate evaluation for the hardware needed for determining the reliability parameters shall be performed as follows:

a) In case of newly developed or modified components or modules, the failure rates of comparable components or modules shall be applied, provided, these have accumulated the operating hours required in accordance with the component specific standards. In addition, ten units of these components or modules must have been deployed for at least two years under comparable operating conditions. Components or modules shall be deemed to be comparable, provided,

   aa) comparable electrical component types,

   ab) comparable structural elements,

   ac) similar design principles

   were used and

   ad) similar ambient conditions of the component

   were specified.

b) The following data accumulated over the last two years shall be presented for the comparable components or modules:

   ba) delivered quantities per annum,

   bb) delivered quantities, overall,

   bc) estimated number of components or modules in operation,

   bd) number of repairs per annum in the manufacturing plant,

   be) number of repairs per annum outside of the manufacturing plant, and

   bf) number of failed but not repaired components or modules per annum.

c) The failure effects, failure causes, and the evaluation of the failure causes for the comparable components or modules shall be presented.

(3) In case of insufficient operating experience, the reliability parameters may be determined from the failure rates for the hardware of the modules based on the failure mode and effect analyses (FEMA) as follows:

a) The failure effects considered shall normally be the physical effects that the component failures have on the function of the module.

b) The analysis procedure, its extent and the auxiliary tools applied shall well substantiated.

Note:

The **f**ailure mode and effects analysis (FMEA) is detailed for example in DIN EN 60812.

(4) Failures accountable to software errors shall be documented. In this context, the failure caused, and the failure effects shall be analyzed. The hardware and software versions shall be documented

Note:

Failure causes may be

a) wrong specifications,

b) faulty implementation of the specifications,

c) errors in the application software,

d) firmware failures, or

e) malware.

C.4 Critical Load Analysis

(1) It shall be demonstrated that the static and dynamic loading of the components and their interconnections does not exceed the admissible limit values.

(2) It shall be demonstrated that, considering the tolerances of the components, the function of the modules is ensured. In this context, the effects that component tolerances have on the specified characteristics of the modules shall be analyzed for any function-relevant component combinations.

(3) The demonstration may be carried out analytically or experimentally, or it may be based on operating experience.

Appendix D

Examples for the Design of Interconnections between Nuclear Power Plant Units

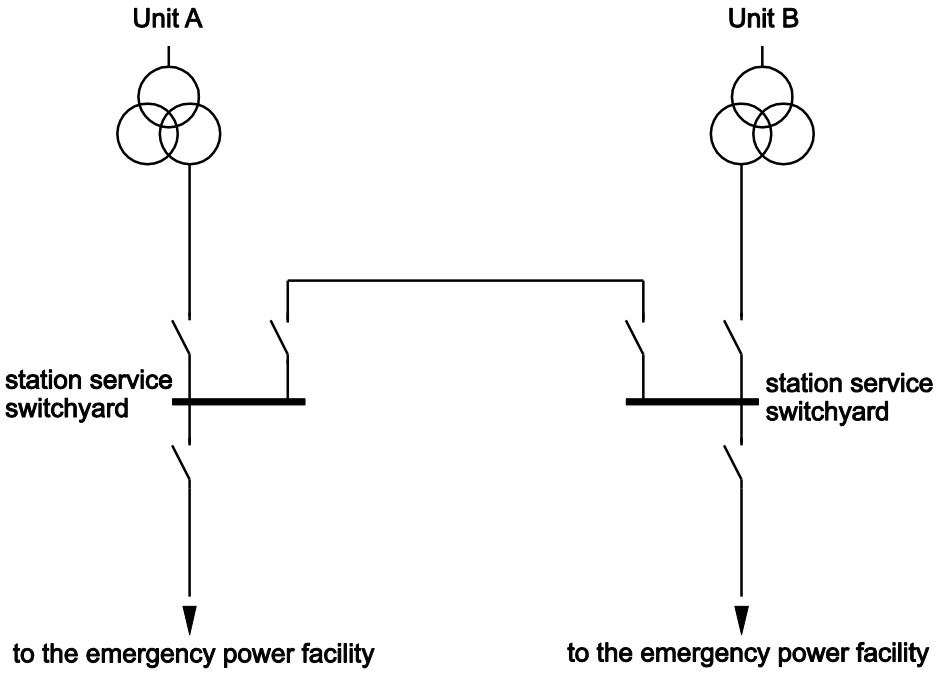


Figure D-1: Example of a power connection between station service switch gear facilities of two nuclear power plant units (schematic for one train)

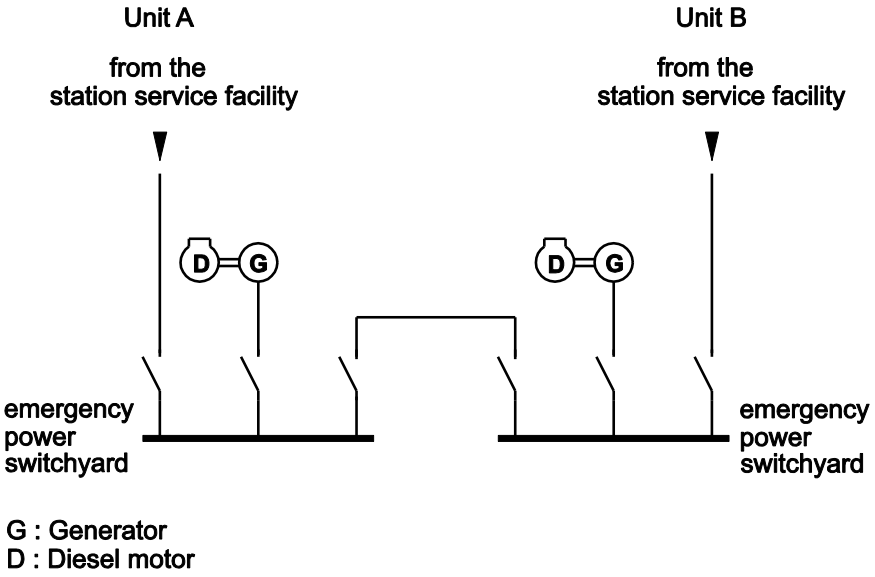


Figure D-2: Example of a power connection between emergency power switch gear facilities of two nuclear power plant units (schematic for one train)

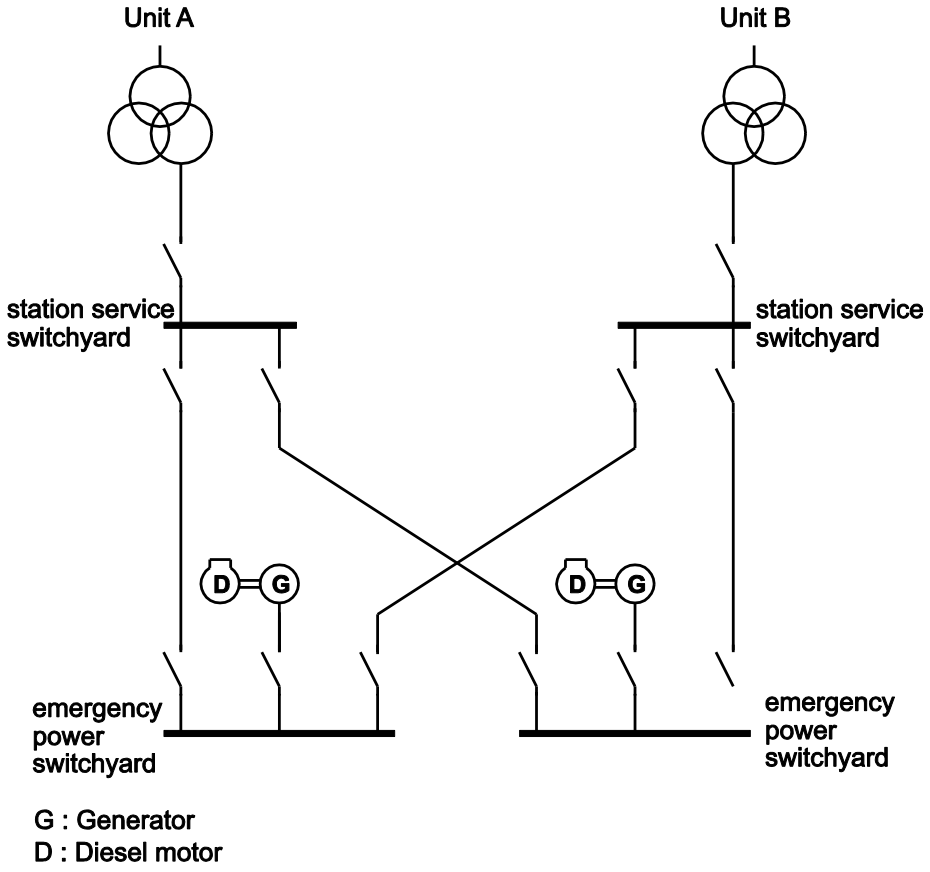


Figure D-3: Example of a power connection between station service switch gear facilities and emergency power switch gear facilities of two nuclear power plant units (schematic for one train)

Appendix E

Regulations Referred to in the Present Safety Standard

(Regulations referred to in the present safety standard are valid only in the versions cited below. Regulations which are referred to within these regulations are valid only in the version that was valid when the latter regulations were established or issued.)

AtG		Act on the peaceful utilization of atomic energy and the protection against its hazards (Atomic Energy Act – AtG) of December 23, 1959, revised version of July 15, 1985 (BGBl. I, p. 1565), most recently changed by Article 5 para. 6 of the Act of February 24, 2012 (BGBl. I, p. 212)
StrlSchV		Ordinance on the protection from damage by ionizing radiation (Radiological Protection Ordinance – StrlSchV) of July 20, 2001 (BGBl. I, p. 1714; 2002 I, p. 1459), most recently changed by Article 5 para. 7 of the Act of February 24, 2012 (BGBl. I, p. 212)
SiAnf	(2012-11)	Safety requirements for nuclear power plants of November 22, 2012 (BAnz of January 24, 2013)
SiAnf-Interpretations	(2013-11)	Interpretations of the safety requirements for nuclear power plants of November 22, 2012, revised version of November 29, 2013 (BAnz of December 10, 2013)
ZPI	(1983-01)	Compilation of the information required in the licensing and supervisory procedure for nuclear power reactors (ZPI) of October 20, 1982 (BAnz 1983, No. 6a, of January 11, 1983)
KTA 1202	(2009-11)	Requirements for the testing manual
KTA 1401	(2013-11)	General requirements regarding quality assurance
KTA 2101.3	(2000-12)	Fire protection in nuclear power plants; Part 3: Fire protection of mechanical and electrical plant components
KTA 2201.4	(2012-11)	Design of nuclear power plants against seismic events; Part 4: Components
KTA 2206	(2009-11)	Design of nuclear power plants against damaging effects from lightning
KTA 3403	(2010-11)	Cable penetrations through the reactor containment vessel
KTA 3501	(1985-06)	Reactor protection system and monitoring equipment of the safety system
KTA 3504	(2006-11)	Electrical drive mechanisms of the safety system in nuclear power plants
KTA 3702	(2014-11)	Emergency power generating facilities with diesel-generator units in nuclear power plants
KTA 3703	(2012-11)	Emergency power facilities with batteries and ac/dc converters in nuclear power plants
KTA 3704	(2013-11)	Emergency power facilities with static and rotary ac/dc converters in nuclear power plants
KTA 3705	(2013-11)	Switchgear, transformers and distribution networks for the electrical power supply of the safety system in nuclear power plants
KTA 3706	(2000-06)	Ensuring the loss-of-coolant-accident resistance of electrical components and of components in the instrumentation and controls of operating nuclear power plants
DIN EN 61508 (VDE 0803)	(2011-02)	Functional safety of electrical/electronic/programmable electronic safety-related systems – all Parts; (IEC 61508-1:2010); German version EN 61508:2010
DIN EN 60812	(2006-11)	Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA) (IEC 60812:2006); German version EN 60812:2006