

1-1-2008

Application specific product qualification report for uninterruptible power supplies used in nuclear reactors R1 and R2

Sam Sadeghi
Ryerson University

Follow this and additional works at: <http://digitalcommons.ryerson.ca/dissertations>

 Part of the [Electrical and Computer Engineering Commons](#)

Recommended Citation

Sadeghi, Sam, "Application specific product qualification report for uninterruptible power supplies used in nuclear reactors R1 and R2" (2008). *Theses and dissertations*. Paper 165.

1004576

**APPLICATION SPECIFIC PRODUCT QUALIFICATION REPORT FOR
UNINTERRUPTIBLE POWER SUPPLIES
USED IN NUCLEAR REACTORS R1 AND R2**

by

Sam Sadeghi, B. Eng, Ryerson University, Toronto, Ontario, Canada, March 2008

**Masters of Engineering Project Report
Presented to Ryerson University
in partial fulfillment of the
requirements for the degree of
Masters of Engineering
in the Program of
Electrical and Computer Engineering**

Toronto, Ontario, Canada, 2008

©Sam Sadeghi 2008

**PROPERTY OF
RYERSON UNIVERSITY LIBRARY**

Author's Declaration

I hereby declare that I am the sole author of this report.

Sam Sadeghi

Date

ABSTRACT

Safety is the most important aspect and is considered the overwriting priority in nuclear power plants, which comprise of thousands of systems and components that work systematically together for the purpose of generating electricity in a safe, economical and environmentally friendly manner. As the instrumentation and electrical components advance and become more sophisticated and migrate from analog design to the more complicated and error-prone software-based topology, the task of determining that a programmable electronic system (PES) is capable of meeting its safety-related design objective becomes ever more challenging. The dependence on the PES to accomplish its safety-related objective must be thoroughly studied to assess the safety-related impacts associated with the potential failure modes of the device. Application Specific Product Qualification (ASPQ) is used to provide necessary assurance in the design integrity of a PES and confirms that the product can meet the requirements of a safety-related application.

This report is an application specific product qualification (ASPQ) assessment of WEP 1010-110/120-NEA and WEP 1020-110/120-NEA Uninterruptible Power Supplies manufactured by Gambit Electronic Ltd. Information referenced in this report is based on the data received from Gambit, other nuclear power plants using Gambit products and the site visit paid to Gambit, Country-X in August 2007.

Gambit WEP 1010- and 10XX-XXX/YY NEA UPS systems are used to provide uninterruptible Class II power to a number of safety-related control and instrumentation power distribution panels for R1 and R2 reactors located in X facility. These UPSs are Commercial Off-the-Shelf (COTS) products intended for industrial uninterruptible power supply applications.

An earlier Categorization Assessment Report concluded that UPSs perform Category B safety-related functions and therefore, they must be qualified to meet the safety requirements associated with a Class B Programmable Electronic System (PES) as per IEC 61513. A combination of methods were utilized to demonstrate that the UPS systems were suitable for the target applications, were inherently correct in design, and came with sufficient documentation to allow safe operation by the plant.

The key findings of this report indicate that the aforementioned UPS systems are suitable for use in the target application, have strong evidence of reliability through field experience and various product certifications that support correctness of their design, and come with thorough documentation that support safe operation and suitability assessment.

Two major recommendations made in this report are to establishing a Preventive Maintenance (PM) program by the station to perform replacement of life-limiting components at the minimum frequencies specified by the manufacturer, and to set up an inspection and testing program by the station to perform minimum-monthly testing of the output power quality of the UPS systems to minimize the possibility of partial failure, which is the failure of concern and relates to a situation where the loads are supplied with out-of-specification power, undetected.

Acknowledgements

This report could not have been written without Dr. Richard Cheung's support and continuous advice. The extent of his teaching went well beyond school.

Wally Kalechstein provided me with expertise on the topic of Electro Magnetic Interference assessment and product qualification process. I also would like to thank Atomic Energy of Canada Ltd. for providing me with the funding and topic for this report.

I thank them all.

Dedication

I would like to dedicate this report to my mother, Fereshteh Gitipour who sacrificed uncountable things in her life to provide me with the opportunities that I now have. Without her, I wouldn't be where I am / will be. There are no words to express my gratitude towards her.

I would also like to dedicate this report to my fiancé, Delaram Karimi, who stood my side patiently during the years of graduate school. Obtaining this degree would not have been possible without her support and kind understanding. She gave me the strength I needed from start to finish.

Last but not least, I would like to thank the management of Atomic Energy of Canada Ltd. for providing me the opportunity to do this work as part of my M. Eng project.

TABLE OF CONTENTS

SECTION	PAGE
1.	INTRODUCTION1
1.1	Scope, Objectives and Assumptions1
1.2	Organization of the document.....2
1.3	Terms, Acronyms and Abbreviations3
2.	PRODUCT DESCRIPTION5
2.1	Online UPS Systems - Principle of Operation5
2.2	UPS Skid Structure5
2.3	UPS - Modes of Operation.....7
2.3.1	Normal Operation9
2.3.2	Bypass Operation9
2.3.3	Charger-Only Mode of Operation.....10
2.3.4	Standby Mode of Operation.....11
2.3.5	System Off Mode of Operation.....12
2.3.6	Manual Bypass Mode of Operation13
2.3.6.1	Manual Bypass Mode of Operation for UPS Testing Purposes.....13
2.3.6.2	Manual Bypass Mode of Operation for UPS Repair/Maintenance Purposes.....14
3.	APPLICATION CONTEXT DESCRIPTION.....15
3.1	Identification of the Loads and Their Criticality15
3.2	UPS Modules16
3.2.1	Voltage Quality (VQ)18
3.2.2	Display Measuring Unit (DMU).....19
3.2.3	Inverter Control.....20
3.2.4	DC Voltage Detector.....21
3.2.5	Supply Monitoring & Reset Circuit.....22
3.2.6	Masterlogic23
3.2.7	Main Processor Unit25
4.	FAILURE MODE ASSESSMENT27
4.1	Analysis of UPS Common Cause Failure at Hardware Level27
4.1.1	Main Processor Unit (MPU)29
4.1.2	Display Measuring Unit (DMU).....30
4.1.3	Masterlogic30
4.1.4	Address Decoder.....30
4.1.5	Signal Controller (SC)30
4.1.6	Display Unit (DU).....31
4.1.7	Voltage Quality (VQ)31
4.1.7.1	VQ Mains.....32
4.1.7.2	VQ Bypass33
4.1.7.3	VQ Output.....34

TABLE OF CONTENTS

SECTION	PAGE
4.1.7.4	Combined VQ Failures34
4.2	Analysis of Common Cause Failure at Software Level.....35
4.3	Application Context Failure Mode Assessment36
4.3.1	VQ Mains36
4.3.2	VQ Bypass36
4.3.3	VQ Output.....37
4.3.4	Combined VQ Failures37
4.3.5	Display Measuring Unit (DMU).....37
4.3.6	Inverter Control.....37
4.3.7	DC Voltage Detector.....38
4.3.8	Supply Monitoring & Reset Circuit.....38
4.3.9	Masterlogic38
4.3.10	Main Processor Unit (MPU)38
4.4	Safety-Related Risks and Consequences of System Failure.....39
5.	ASPQ SUITABILITY REQUIREMENTS.....40
5.1	Safety Attributes, Fail Safe or Fail Detected Behaviour.....40
5.2	Functionality40
5.2.1	Normal Mode40
5.2.2	Abnormal Mode40
5.2.3	Emergency Mode41
5.2.4	Maintenance Mode.....41
5.2.5	Return to Normal Operating Conditions.....41
5.3	Performance42
5.3.1	Battery Charger/Rectifier.....45
5.3.2	Inverter46
5.3.3	Batteries46
5.3.4	Static Transfer Switch.....46
5.4	Reliability.....47
5.5	Maintainability47
5.6	Testability47
5.6.1	Battery Charger Tests47
5.6.2	Battery Tests48
5.6.3	Inverter and Transfer Switch Tests48
5.6.4	UPS Test48
5.7	Security48
5.8	Seismic48
5.9	Environmental Tolerance.....49
5.10	Electromagnetic Immunity/Emissions49
6.	ASPQ APPROACH50
6.1	Suitability50
6.2	Adequacy of Documentation50
6.3	Evidence of Correctness51

TABLE OF CONTENTS

SECTION	PAGE
7.	DETAILED FINDINGS FROM THE ASSESSMENT METHODS52
7.1	Suitability Assessment52
7.1.1	Method 4a: “In-Service Maintenance Process Assessment”52
7.1.2	Method 5a: “Environmental Tolerance Assessment”53
7.1.3	Method 5b: “Electromagnetic Immunity and Emissions Assessment”53
7.1.4	Method 5c: “Seismic Tolerance Assessment”59
7.1.5	Method 5d: “Hardware Reliability, Failure Modes and Diagnostic Assessment”59
7.1.6	Method 5e: “Assessment of Hardware Useful Life”62
7.1.7	Method 9c: “Assessment of 3 rd Party Hardware Test Standards Compliance”63
7.1.8	Method 4b: “In-Service Testability Assessment”64
7.2	Documentation for Safety64
7.2.1	Method 2: “Assessment of Product Specifications”64
7.2.2	Method 9a: “Assessment of 3 rd Party Corporate Quality System Certification”66
7.2.3	Method 9b: “Assessment of 3 rd Party Product Safety Certification”66
7.3	Evidence of Correctness68
7.3.1	Method 3c: “Product Design Revision History Assessment”70
7.3.1.1	Firmware Modifications from Package 0 to 171
7.3.1.2	Firmware Modifications from Package 1 to 273
7.3.2	Method 3a: “Operating History Data”75
7.3.3	Method 3b: “Failure Data Assessment”78
7.3.4	Method 3d: “Reference Site Assessments”79
8.	QUALIFICATION CONCLUSIONS82
8.1	Suitability Evaluation82
8.1.1	Safety Attributes, Fails Safe or Fail Detected Behaviour82
8.1.2	Functionality82
8.1.3	Performance83
8.1.4	Reliability90
8.1.5	Maintainability91
8.1.6	Testability91
8.1.7	Security91
8.1.8	Seismic92
8.1.9	Environmental Tolerance92
8.1.10	Electromagnetic Immunity/Emissions93
8.2	Adequacy of Product Documentation93
8.3	Evidence of Correctness93
9.	RECOMMENDED ACTIONS94
9.1	Suitability Evaluation94

TABLE OF CONTENTS

SECTION	PAGE
9.2 Adequacy of User-Documentation-for-Safety	95
9.3 Evidence of Correctness	95
10. REFERENCES	96

TABLES

Table 1-1 Acronyms and Abbreviations	3
Table 3-1 UPS 1 Class II Loads.....	15
Table 3-2 UPS 2 Class II Loads.....	16
Table 4-1 MPU Firmware Task Composition	29
Table 4-2 List of Communications Between MPU and VQ-Mains.....	32
Table 4-3 List of Communications Between MPU and VQ-Bypass	33
Table 4-4 List of Communications Between MPU and VQ-Output.....	34
Table 4-5 Combined VQ Failures and Consequences	35
Table 5-1 Battery Performance Requirements.....	41
Table 5-2 UPS Performance Requirements	42
Table 5-3 Inverter Performance Requirements.....	43
Table 5-4 Rectifier/Battery Charger Performance Requirements.....	44
Table 5-5 Battery Performance Requirements.....	45
Table 5-6 Static Transfer Switch Performance Requirements.....	45
Table 5-7 Environmental Requirements of the UPS.....	49
Table 7-1 Assessment of UPS Compliance with IEC 62020-2:2005 with Respect to Emissions	56
Table 7-2 Assessment of UPS Compliance with IEC 62020-2:2005 with Respect to Immunity.....	57
Table 7-3 UPS 1/2 Main Control Room Alarm Descriptions.....	60
Table 7-4 Gambit UPS Sales / Failure Data As of August 2007	61
Table 7-5 UPS Component Replacement Frequency	62
Table 7-6 MTBF Values of Various Components of Gambit UPS	63
Table 7-7 Conformance of Gambit UPS Systems to Testability Requirement	64
Table 7-8 List of Canadian and International Standards Conformed by Gambit UPS Systems	68
Table 7-9 Software Complexity.....	69
Table 7-10 Minimum Unit-Hours of Operation for Various Classes and Complexity Levels.....	69
Table 7-11 UPS WXX Firmware Revision History	70
Table 7-12 MPU Firmware Modifications from REV01 to REV02.....	71
Table 7-13 VQ Firmware Modifications from REV02 to REV03.....	71
Table 7-14 VQ Firmware Modifications from REV03 to REV04.....	71
Table 7-15 VQ Firmware Modifications from REV04 to REV05.....	72
Table 7-16 Masterlogic Firmware Modifications from REV01 to REV02	72
Table 7-17 MPU Firmware Modifications from REV02 to REV03.....	73

TABLE OF CONTENTS

SECTION	PAGE
Table 7-18 MPU Firmware Modifications from REV03 to REV04	74
Table 7-19 RAR1 Firmware Modifications from REV03 to REV04	74
Table 7-20 Gambit UPS Sales / Failure Data	77
Table 7-21 WXX FW P2 Reliability Data for Period of 01 OCT 2003 to 31 DEC 2004.....	78
Table 7-22 TUV Nord Quantitative Reliability Assessment of WXX Firmware Package 2	79
Table 7-23 Reference Site Questionnaire	81
Table 8-1 Assessment of UPS Conformance to Performance Requirements	83
Table 8-2 Assessment of Inverter Conformance to Performance Requirements.....	84
Table 8-3 Assessment of Rectifier/Battery Charger Conformance to Performance Requirements	86
Table 8-4 Assessment of Battery Conformance to Performance Requirements.....	88
Table 8-5 Static Transfer Switch Performance Requirements.....	89
Table 8-6 Deposition of Non-Conformities to Additional Requirements	90
Table A-1 Interface Complexity Indices and Associated Weights	A-98

TABLE OF CONTENTS

SECTION	PAGE
FIGURES	
Figure 2-1 Basic Online UPS Topology	5
Figure 2-2 Typical Layout of Gambit UPS System.....	6
Figure 2-3 UPS Main Components.....	7
Figure 2-4 UPS Modes of Operation	8
Figure 2-5 Normal Mode of Operation	9
Figure 2-6 Bypass Mode of Operation.....	10
Figure 2-7 Charger-Only Mode of Operation.....	11
Figure 2-8 Standby Mode of Operation	11
Figure 2-9 System Off Mode of Operation.....	12
Figure 2-10 Front Panel of UPS.....	13
Figure 2-11 Manual Bypass Mode of Operation (Test Configuration)	14
Figure 2-12 Manual Bypass Mode of Operation (Bypass Configuration).....	14
Figure 3-1 Block Diagram Representation of UPS.....	17
Figure 3-2 Simplified Block Diagram for a VQ Sensor	18
Figure 3-3 Block Diagram Representation of DMU.....	19
Figure 3-4 Block Diagram Representation of Invert Control	20
Figure 3-5 Block Diagram Representation of DC Voltage Regulator	22
Figure 3-6 Block Diagram Representation of Supply Monitoring & Reset Circuit	23
Figure 3-7 Block Diagram Representation of Masterlogic	24
Figure 3-8 Block Diagram Representation of MPU	25
Figure 4-1 Block Diagram Representation of Gambit UPS Hardware.....	28
Figure 4-2 Display Unit of Gambit UPS.....	31
Figure 7-2 WEP UPS Unit-Years of Operation	77
Figure 8-1 Alarm Indications of UPS Control Panel	82
Figure 8-2 Gambit UPS Front Panel View	92

TABLE OF CONTENTS

SECTION	PAGE
APPENDICES	
Appendix A Appendices	A-98
A.1 Interface Complexity Index	A-98
A.2 Sales Data of Gambit WXX Firmware Package 2 for Period of 01 OCT 2003 to 31 DEC 2004 (AUFSYS Export)	A-100
A.3 Failure Data of Gambit WXX Firmware Package 2 for Period of 01 OCT 2003 to 31 DEC 2004 (IQ-Soft Export).....	A-101
A.3 TUV Nord Certificate of Conformance of Gambit WXX Firmware Package 2 to IEC 60880-2	A-102
A.4 Gambit Declaration of Conformity	A-103
A.5 BVQI Certificate of Conformance of Gambit to ISO 9001:2000.....	A-104
A.6 CANPAC Certificate of Conformance to CSA Z299.2	A-105
A.7 Gambit MTBF and MTTR Calculations for UPS Systems	A-106
A.8 List of Reference Nuclear Power Plants	A-107
A.9 Reference Site Questionnaire Form	A-109
A.9.1 UPS Data.....	A-109
A.9.2 UPS Documentation.....	A-109
A.9.3 UPS Goodness of Design / Reliability.....	A-109
A.9.4 Applicability of the Data.....	A-109
A.9.5 Miscellaneous	A-109
A.10 WEP 1000 Technical Data Sheet.....	A-110
A.11 Batteries Recharge Characteristic Curve	A-114
A.12 Qualification Assessment Plan and Preliminary Assessment Evidence	A-115

1. INTRODUCTION

Safety is the most important aspect in nuclear power plants, which comprise of thousands of systems and components that work systematically together for the purpose of generating electricity in a safe, economical and environmentally friendly manner. As the instrumentation and electrical components become more sophisticated and migrate from analog design to the more complicated and error-prone software-based topology, the task of determining that a programmable electronic system (PES) is capable of meeting its safety-related design objectives becomes ever more challenging. Such devices are vulnerable to random hardware/software failures and when redundancy is used, common cause failure becomes a major concern. The dependence on a PES to accomplish its safety-related objective must be thoroughly studied to assess the safety-related impacts associated with the potential failure modes of the device. From academic perspective, this report demonstrates the complex “qualification” methods used to pinpoint the failure modes associated with a programmable electronic systems and how such failure modes may affect safety in a nuclear power plant. An Application Specific Product Qualification (ASPQ) is used to provide necessary assurance in the design integrity of a PES and confirms that the product can meet the requirements of a safety-related application.

Due to prior confidentiality agreements, and in order to protect the identity of the manufacturer of the UPS systems, specifics such as model numbers, individuals’ names, manufacturer name and location, name and location of the reactors where the UPS are used, name of loads that are directly powered by the UPSs, have been changed through out this report.

Information referenced in this report is based on the data received from Gambit, other nuclear power plants using Gambit products and the site visit paid to Gambit, Country-X in August 2007.

This report sets out the analysis used to determine the Uninterruptible Power Supplies 1 and 2 (UPS 1 and UPS 2) used in R1 and R2 reactors met the minimum application specific qualification evidence as prescribed in AECL procedure: Qualification of Programmable Electronic Systems Products for Use in Nuclear Safety-Related Applications. [3]

The Uninterruptible Power Supply systems (UPS 1 and UPS 2) provide power for a number of important systems, related to the operation of R1 and R2 reactors. Their function is indirectly related to safety as the reactor Safety Load 1 and Safety Load 2 (SL1 and SL2) are among their loads. Although all of the loads are designed to fail-safe when de-energized, the possibility of supply of out-of-specification power (i.e., “dirty power”) in the event of UPS partial failure, needs to be investigated in further detail. UPS Function Categorization Assessment Report [1] provides more details regarding UPS loads and failure impact of UPSs on these loads. In this document terms “UPSs” and “UPS systems” refers to WEP 1010-110/120 NEA and WEP 1020-110/120 NEA uninterruptible power supply systems manufactured by Gambit Electronic Ltd and are used interchangeably. Similarly, term “manufacturer” references to Gambit Electronic Ltd., the manufacturer of these UPS systems.

1.1 Scope, Objectives and Assumptions

The scope of this report is the Application Specific Product Qualification of the Uninterruptible Power Supply systems that provide online power to loads in R1 and R2 reactors. The safety-related function category assigned to UPS 1 and UPS 2 is determined based on the potential risk of radioactivity release to public or exposure to personnel due to UPS failure.

equipment. The company-wide qualification procedure 9999-566.1 [3] requires any programmable electronic equipment that is determined to be Class 1, 2 or 3 to be qualified.

AECL documents 9999-566.1 [3] and 9999-566.1.1 [4] are MMMM-project-specific procedure and guideline for qualification of programmable electronic systems (PES), respectively. The guideline provides details on various methods outlined by the procedure, in order to demonstrate a PES meets certain qualify-ability requirements.

This report presents arguments to support the application specific product qualification (ASPQ) of the UPS systems WEP-1010 and WEP-1020 manufactured by Gambit Electronic Ltd. for use in R1 and R2 reactors. The objective of this qualification report is to demonstrate that the reliance on the UPS systems is clearly understood and the modes of failure are acceptable in the plant design and operating context, with respect to safety, reliability and maintainability.

This qualification report is to provide documented evidence that the UPS systems:

- Are suitable for use in the intended application;
- Come with sufficient user documentation; and
- Are correct in hardware and software design.

This document assumes a basic familiarity with the concepts and terminology of I&C and the theory of operation of continuous UPS systems. Some general knowledge of design concepts for enhanced reliability of products would be advantageous.

1.2 Organization of the document

This document starts with a short introduction and synopsis of the product qualification. Section 2 presents general information on UPS principle of operation, skid structure and the modes of operation associated with Gambit WEP 1010 and 1020 UPS systems.

The loads and their associated criticalities, along with a description of various Gambit UPS modules are presented in Section 3. In Section 4, different failure modes such as common cause failures and application-context failure modes, along with their associated consequences with respect to safety are analyzed. In Section 5 application specific suitability requirements of the UPSs were outlined. Section 6 lists the methods used to demonstrate suitability, documentation and correctness of design of the UPS systems. In the next Section, detailed findings from each assessment method are summarized. Section 8 is the conclusion of the qualification methods applied in the previous Section. Lastly, Section 9 lists the recommended actions and respective rationales to ensure suitability, documentation and correctness-of-design requirements of the UPS systems are met.

1.3

Terms, Acronyms and Abbreviations

Table 1-1
Acronyms and Abbreviations

Term	Definition
AC	Alternating Current
AECL	Atomic Energy of Canada Limited
ASPQ	Application Specific Product Qualification
CANDU	CANada Deuterium Uranium (registered trademark of AECL)
CCF	Common Cause Failure
COTS	Commercial Off the Shelf
DC	Direct Current
DU	Display Unit
DMU	Display Measuring Unit
DR	Design Requirements
EMC	Electromagnetic Compatibility
EMI	1) Electromagnetic Immunity; 2) Electromagnetic Interference
FAT	Factory Acceptance Testing
FMEA	Failure Modes & Effect Analysis
FW	Firmware
GUI	Graphical User Interface
GAL	Gate Array Logic
HAZOP	Hazard and Operability
HMI	Human Machine Interface
HW	Hardware
I&C	Instrumentation and Control
I/O	Input/Output
IEC	International Electro-technical Commission
LED	Light Emitting Diode
LCD	Liquid Crystal Display
MMMM	Name of Project
MTBF	MEAN Time Between Failures
MTTR	MEAN Time To Repair
P2	Package 2
PES	Programmable Electronic Systems
PQR	Product Qualification Report
R1	Reactor 1
R2	Reactor 2
RCCS	Reactor System X

Term	Definition
SC	Signal Controller
SL 1	Safety Load 1
SL 2	Safety Load 2
SRS	Specified Response Spectra
SW	Software
THD	Total Harmonic Distortion
TRS	Test Response Spectra
TS	Technical Specifications
UPS	Uninterruptible Power Supply
VQ	Voltage Quality
PWM	Pulse Width Modulation

2. PRODUCT DESCRIPTION

2.1 Online UPS Systems - Principle of Operation

The basic design topologies for UPS systems are offline (on demand) and online (also known as continuous and true-online). As the names suggest, the first type (offline) provides power only if the utility power is down while the second type is continuously supplying power to the attached loads.

The products under qualification belong to the group of online UPS systems. Their real advantage is the ability to provide a continuous “electronic firewall” between the incoming power and sensitive electronic equipment. While the offline designs normally leave the equipment connected directly to the utility power with minimal surge protection, the online UPS systems provide multiple layers of electronic protection from power problems on a continuous basis.

A simplified online UPS topology is presented in Figure 2-1. First, the incoming AC utility voltage is passed through surge-protected rectifier stage, where it is converted to a direct current (DC), which is heavily filtered by large electrolytic capacitors, to provide low ripple voltage while charging the batteries. The input capacitors also act as an energy storage reservoir, giving the UPS the ability to “ride through” momentary power interruptions without battery drain. As the battery source is also connected to this DC circuitry, it simply takes over as the energy source in the event of a complete utility loss. This makes the transition between utility and battery power seamless, without the typical 4- to 25-millisecond output interruption associated with offline UPS topology.

DC voltage regulation is performed by the SCR bridge rectifiers and a controller. This stage gives the UPS the ability to sustain a constant output even during long deep brownouts or low-line conditions, which would require an offline UPS to go to battery mode.

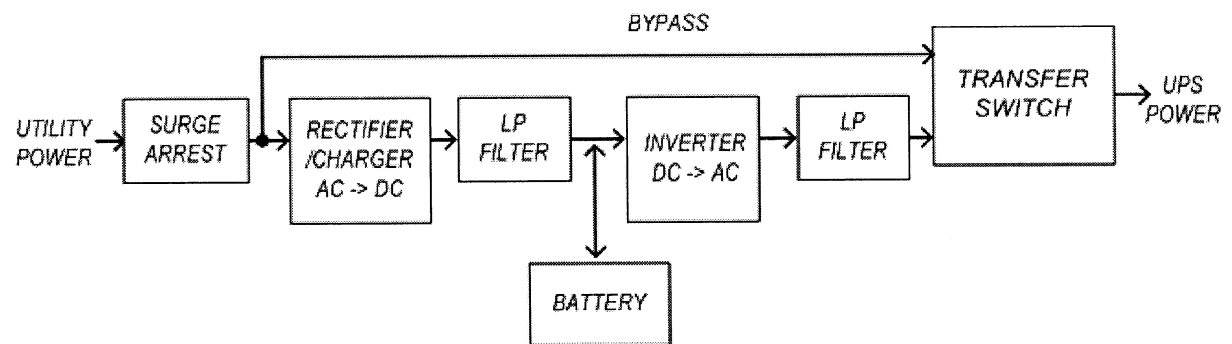


Figure 2-1 Basic Online UPS Topology

The regulated DC voltage is fed to an inverter where a new 60 Hz true AC sine-wave output power is generated. The generated AC is synchronized with the grid, which allows smooth switchover to utility power when needed.

2.2 UPS Skid Structure

A typical structure of a single phase Gambit UPS system is shown in Figure 2-2. It follows a standard online topology as described in the previous Section.

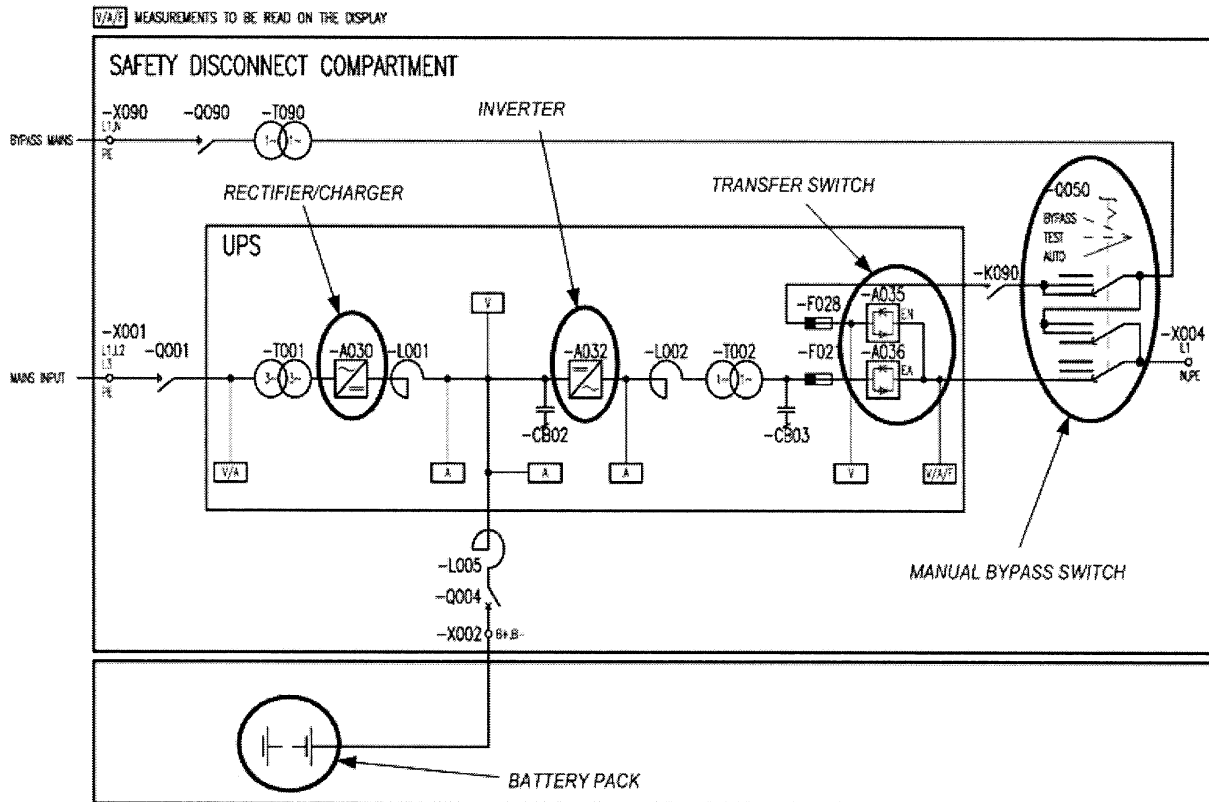


Figure 2-2 Typical Layout of Gambit UPS System

As shown above, the transfer switch is electronic which allows precise control of the switchover instant and eliminates the inherent problems of the mechanical devices. The input and output are electronically separated by transformers T001 and T002 while T090 separates the bypass route. The filters are LC-type and are formed by the inductivity L001 and the capacitor C802 at the output of the rectifier, and L002-C803 at inverter output. Fuses F021 and F028 protect the transfer switch.

Figure 2-3 is a picture of a typical skid structure of a Gambit UPS system. As illustrated below, the main components of the UPS consist of:

- Rectifier Module
- Inverter Module
- Static Switch Module
- Manual Bypass Switch
- Transformers
- Main Controller
- Human Machine Interface (HMI)
- Battery Pack

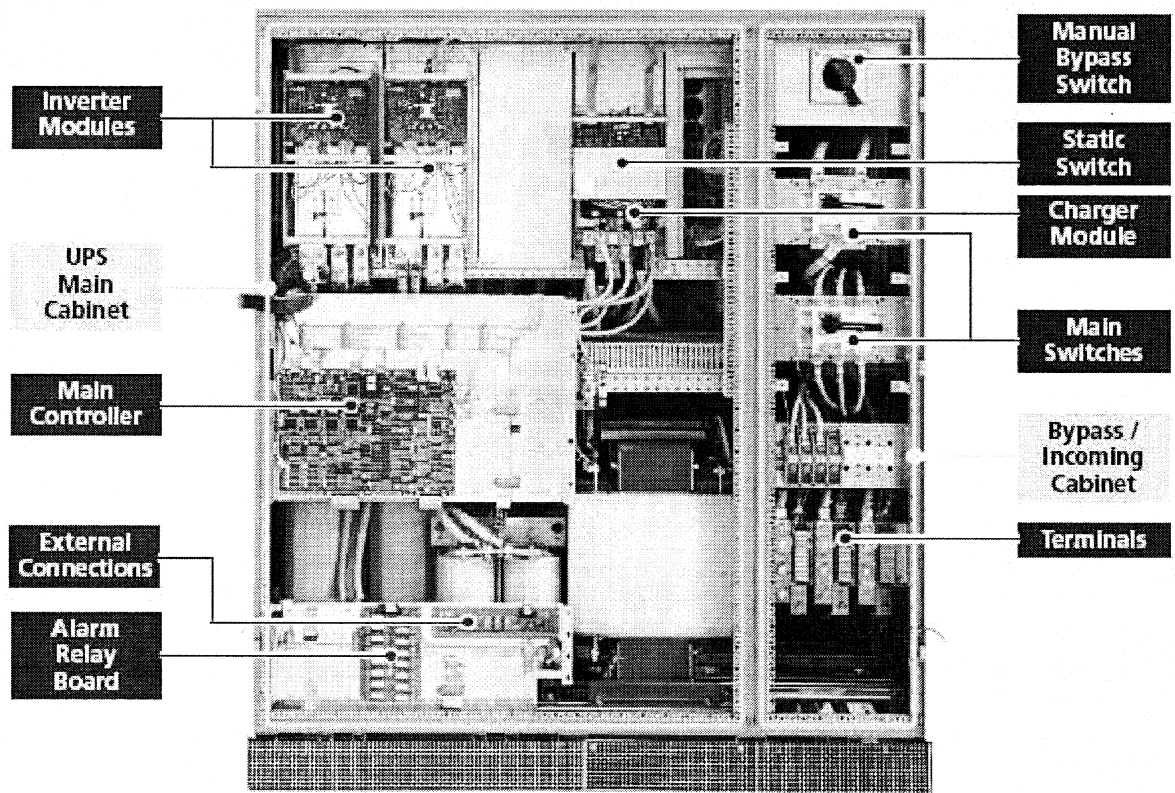


Figure 2-3 UPS Main Components

2.3 UPS - Modes of Operation

In single configuration, there are six modes of operation associated with the UPS system. Depending on the availability of rectifier grid, bypass grid, battery voltage and load, the UPS systems changes from one mode to another. Figure 2-4 depicts the relationship between these modes. It must be noted that since 'Hot Standby' mode of operation is specific to multiple UPS configuration, it is not applicable to the UPS set-up used in R1 and R2. In addition, "Economy Mode" is specific to applications in which efficiency is more important than power quality, and UPS is programmed to treat Bypass as the source with the highest priority, where the loads are powered via Bypass in normal mode of operation. However, this mode of operation is not applicable to the purchased UPS systems and thus not considered.

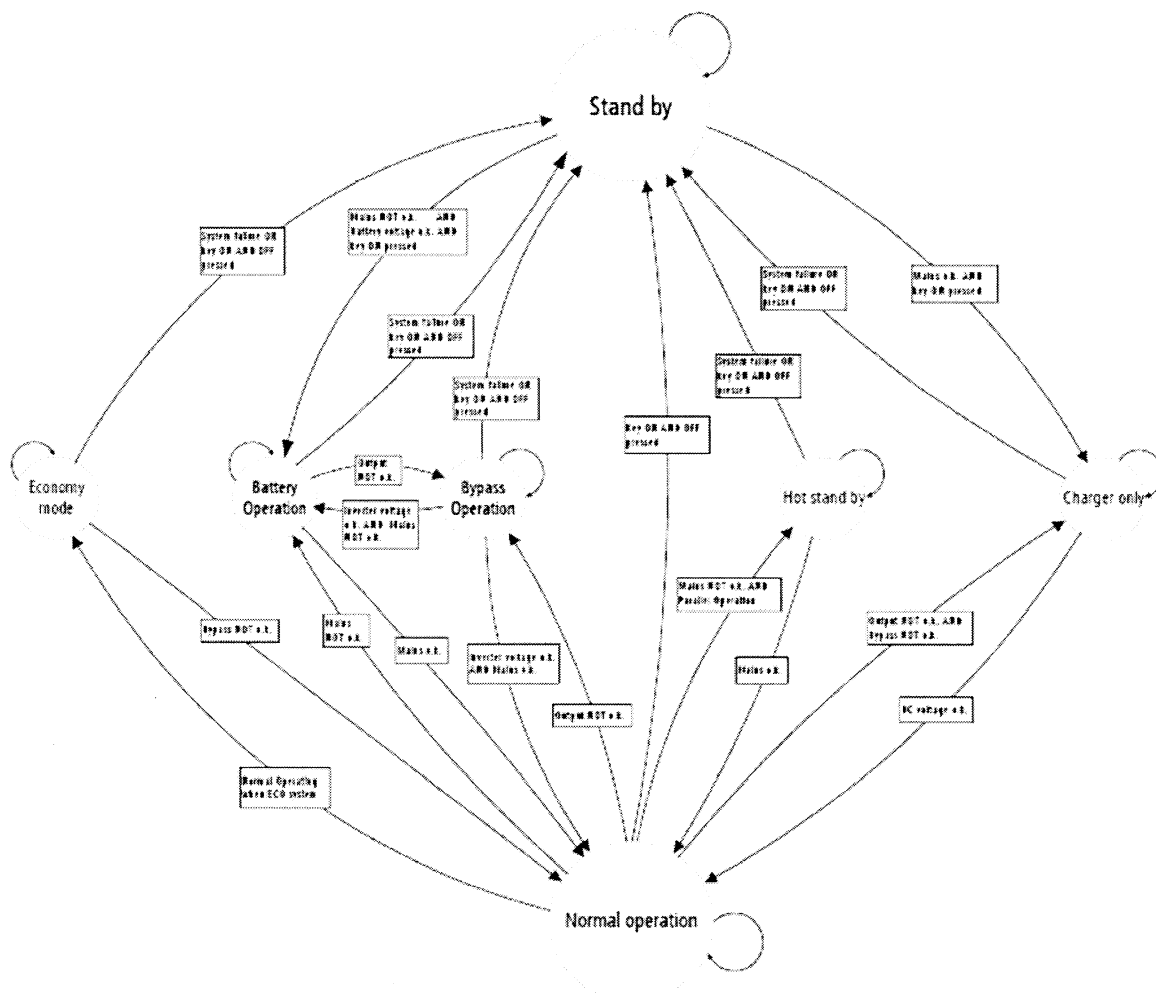


Figure 2-4 UPS Modes of Operation

In a single UPS configuration, the priority of each operation mode is shown below:

1. Normal operation
2. Battery operation
3. Bypass operation
4. Charger only
5. Standby
6. Off

It is noteworthy that for test/maintenance purposes, the UPS is placed in “Manual bypass” mode of operation, by the operator. The following section provides more information on each of these modes.

2.3.1 Normal Operation

This is the normal mode of operation and occurs only during start up of the system as soon as the inverter starts running and the static switch of the inverter (EA) turns on.

The AC input is fed to the phase-angle controlled rectifier via a matching transformer. The rectifier compensates grid voltage fluctuations as well as load deviations and maintains the DC voltage constant.

The rectifier supplies the inverter with the energy needed to keep it charged. The downstream inverter converts the DC voltage by means of optimized sine wave pulse width modulation (PWM) into AC voltage and supplies the connected load via the static switch (EA).

Figure below, shows the flow of energy from grid to the load under this mode of operation.

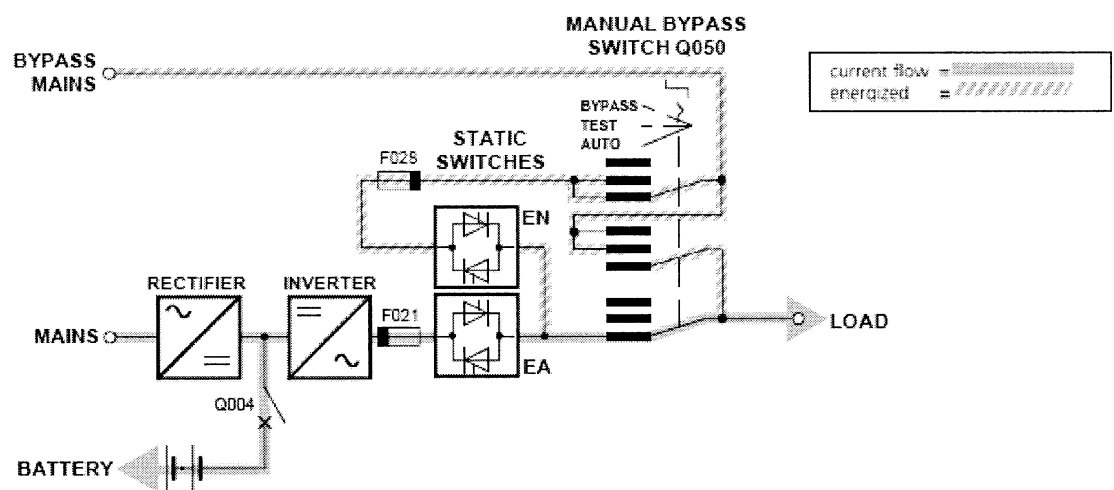


Figure 2-5 Normal Mode of Operation

If the supply of the load from the inverter is not secured due to overload or inverter fault, the UPS will change mode to bypass operation.

2.3.2 Bypass Operation

As illustrated in Figure 2-6, in this mode of operation the load is fed directly by the alternative (bypass) supply through the manual and static switches since rectifier and inverter are no longer supplying the load. This mode is considered as the *emergency* operation mode since loads are no longer backed up and the power quality depends strictly on that of the bypass grid. The changeover from normal to this mode of operation can be initiated automatically, manually or remotely by a control signal. The changeover, whether manual or automatic, is only possible if voltage, frequency and phase characteristics of the UPS systems are synchronized to those of the bypass supply. Automatic changeover of the loads to alternate grid takes place when the power supplied to the inverter is not within the specifications.

A fault at bypass supply causes the system to automatically change to normal mode of operation, if the rectifier mains is available and a prior fault in the inverter is not detected. Otherwise, the UPS system will change over to battery operation, as long as the battery supply is within the tolerance range.

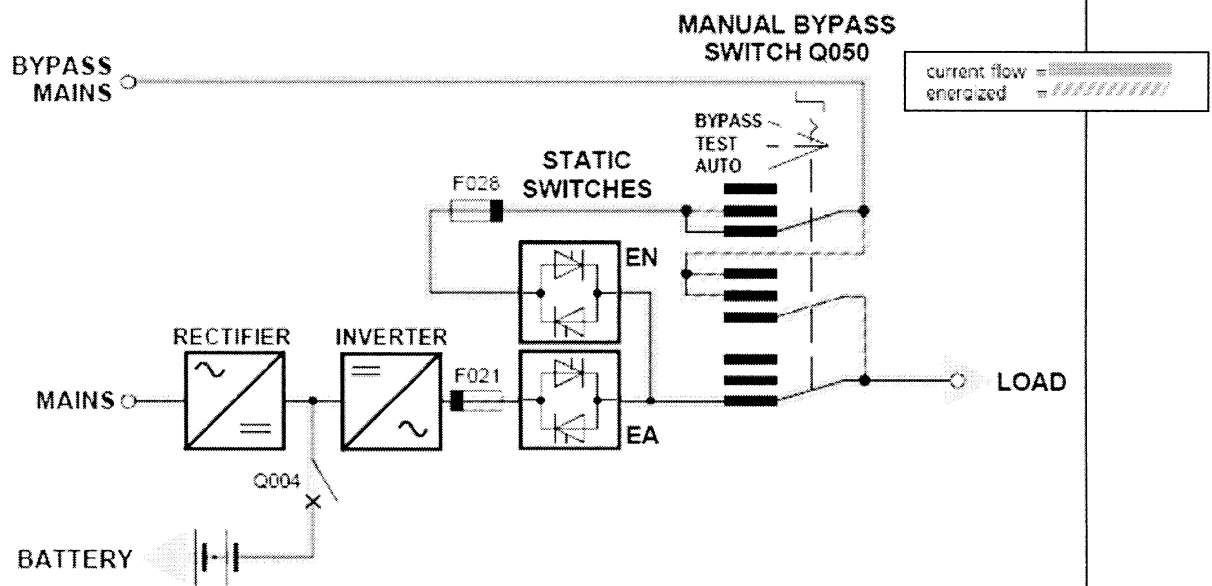


Figure 2-6 Bypass Mode of Operation

2.3.3 Charger-Only Mode of Operation

As illustrated in Figure 2-7, alternating current of the grid is converted to direct current via the rectifier. The DC current is used to charge up the battery. In this mode of operation, the load is not supplied with power and output voltage is zero. The UPS enters this mode of operation when the output is out of specifications (i.e. inverter is either malfunctioning or unavailable) and the alternate supply is either unavailable or out of pre-specified tolerance limits.

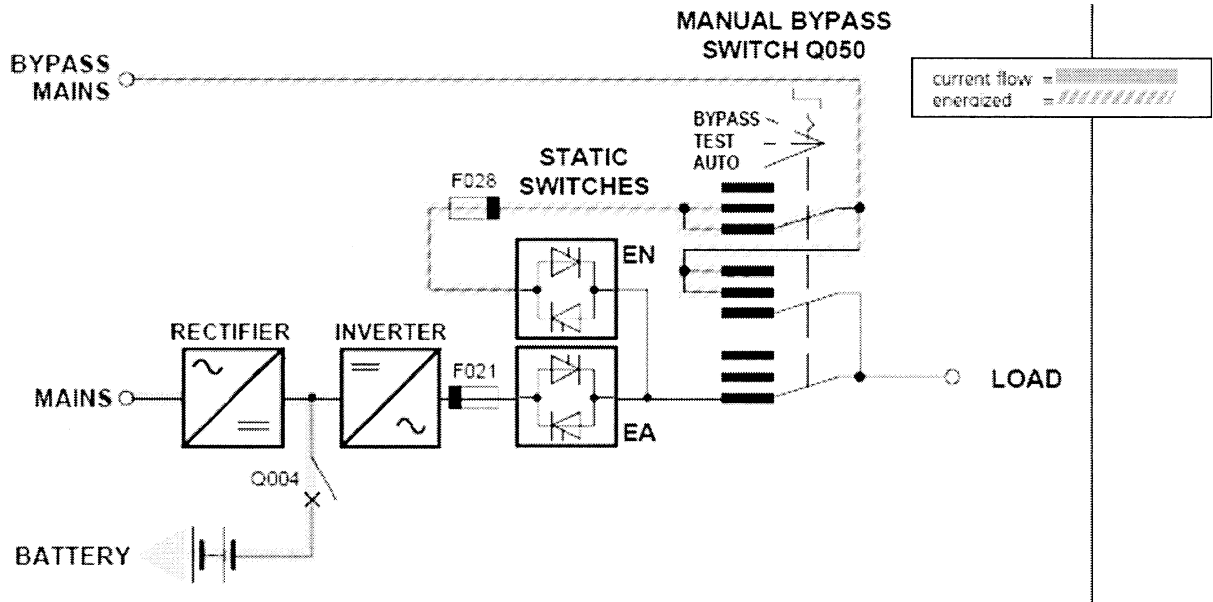


Figure 2-7 Charger-Only Mode of Operation

2.3.4 Standby Mode of Operation

In this mode of operation, the UPS system is ready to be switched on. As illustrated in Figure 2-8, the UPS is de-energized and the load is not supplied. The UPS enters this mode of operation only if at least one of the supplies (i.e., grid or alternate) is available.

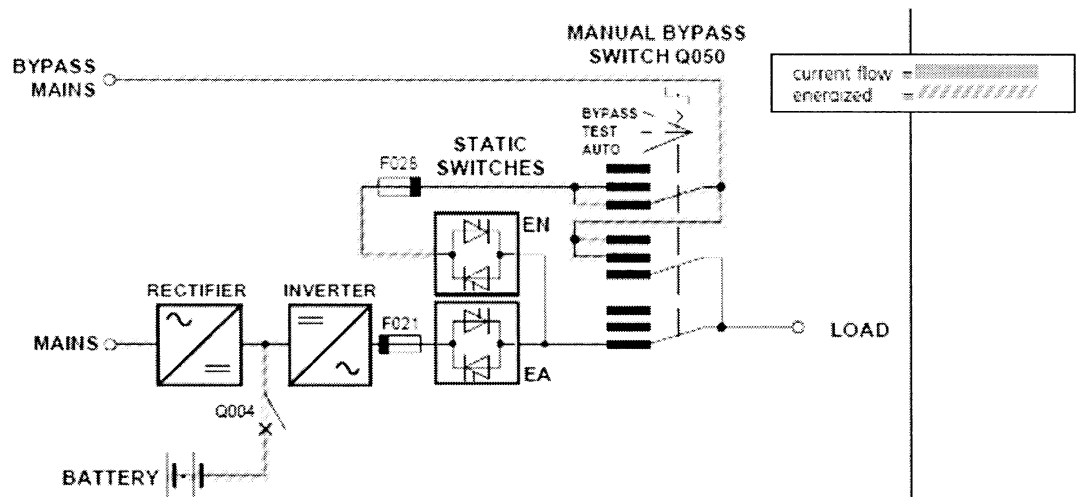


Figure 2-8 Standby Mode of Operation

2.3.5 System Off Mode of Operation

As illustrated below, in this mode of operation, the system is completely de-energized and even the display is dark.

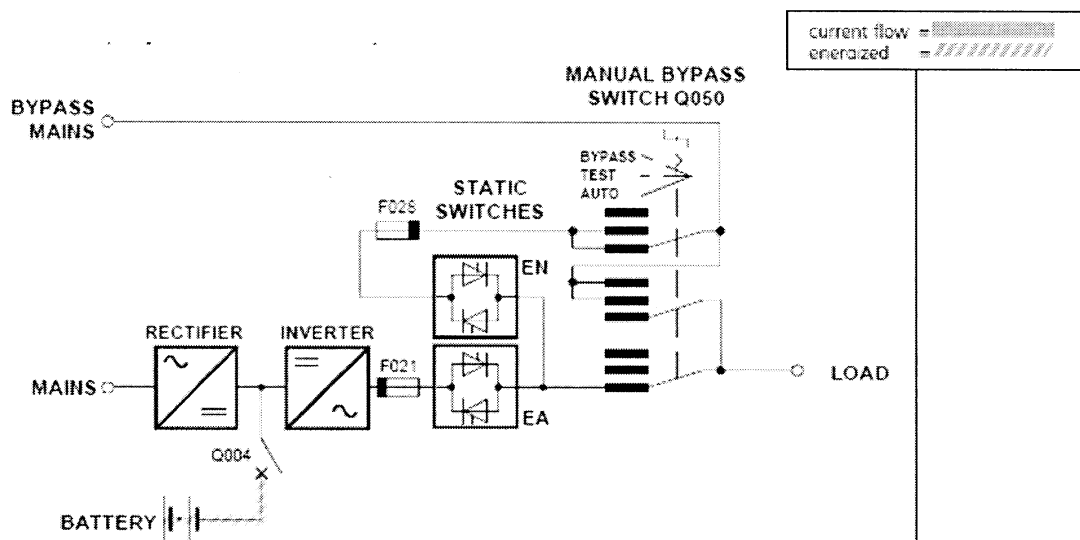


Figure 2-9 System Off Mode of Operation

The UPS enters this mode of operation only if switch 'S2', located on operation panel part of human-machine interface of UPS is manually pressed. Figure 2-10 illustrates the location of switch 'S2'. It must be noted that the batteries are still energized in this mode.

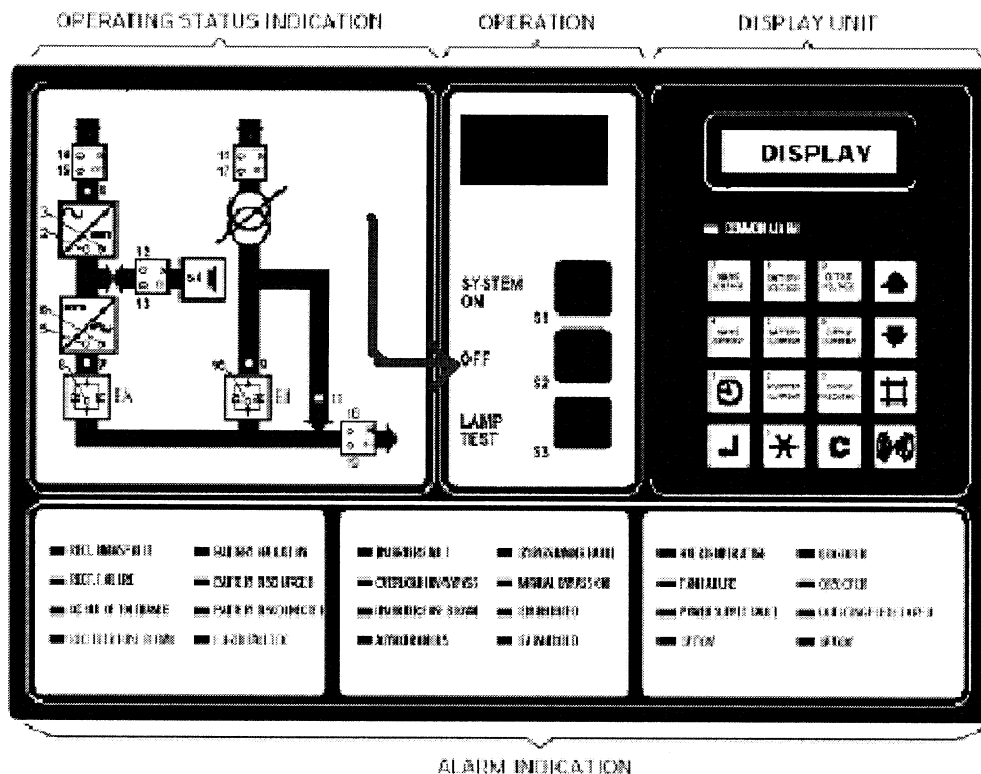


Figure 2-10 Front Panel of UPS

2.3.6 Manual Bypass Mode of Operation

In this mode of operation, the load is directly fed by the alternate supply. The manual bypass switch, Q050 of Figure 2-2, can be placed in three different positions: Bypass, Test and Auto. Each position is described in more details below.

2.3.6.1 Manual Bypass Mode of Operation for UPS Testing Purposes

As the name implies, position “Test” is used for testing purposes. Under this condition, an external mock up load can be connected to the “Test” terminal of the UPS. The test load should not exceed the rated load of the UPS. It noteworthy that the UPS system remains energized during “Test” condition.

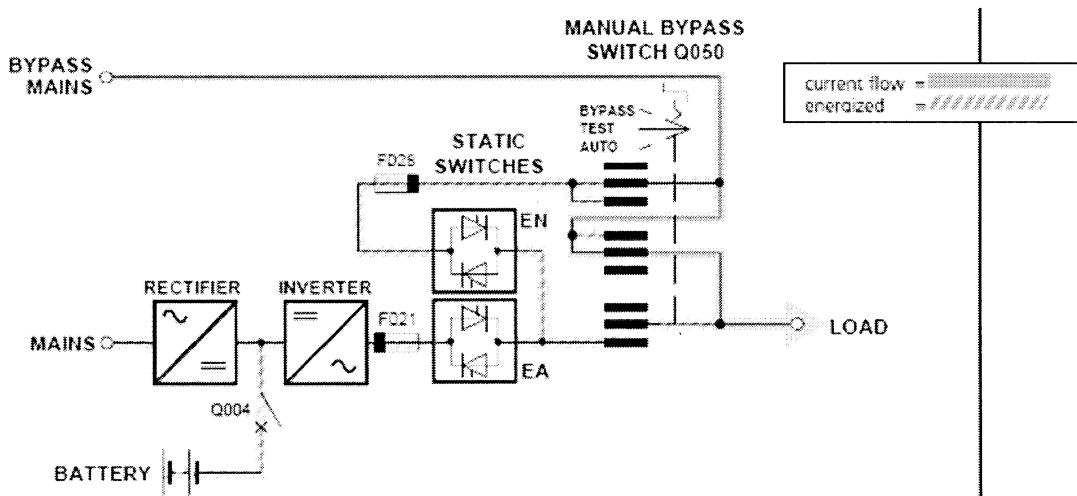


Figure 2-11 Manual Bypass Mode of Operation (Test Configuration)

2.3.6.2 Manual Bypass Mode of Operation for UPS Repair/Maintenance Purposes

For repair or maintenance work on the UPS, switch Q050 is placed on “Bypass” which results the components inside the UPS to become de-energized (Figure 2-12). This allows for safe maintenance/repair of the unit by qualified personnel.

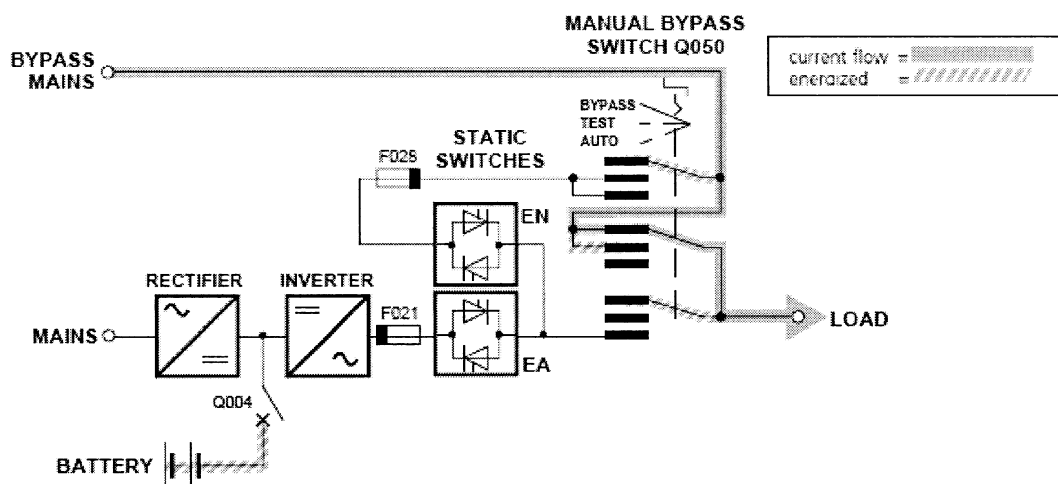


Figure 2-12 Manual Bypass Mode of Operation (Bypass Configuration)

3. APPLICATION CONTEXT DESCRIPTION

3.1 Identification of the Loads and Their Criticality

The criticality of each individual load supplied by UPS 1 and UPS 2 was assessed by Function Categorization Report [1] based on analyzing the failure impact of the UPS loads. Four levels of failure impact type are defined by the categorization procedure: a Type I impact indicates complete loss of the safety-related function of the load system; Type IIa and IIb impacts indicate greater and lesser degrees of impairment, respectively, and a Type III impact indicates no effect on safety. [2] Detailed criteria of the four failure impact types are defined in more details in the categorization procedure guideline [10]. Table 3-1 and Table 3-2 list the loads and the associated failure impact type for UPS 1 and UPS 2 respectively.

Table 3-1
UPS 1 Class II Loads

UPS 1 Load Description	Failure Impact Type
Safety Load 2 - Channel A Safety Load 2 - Channel B Safety Load 2 - Channel C	I
Safety Load 3 Instruments Safety Load 3 Maintenance Station and Reactor Regulation Safety Load 5	I
Control Console	III
Safety Load 7	III
RH Lights Relay Panel	IIb
Confinement Instrumentation	III
HVAC Control	III
Trench Gate	III
RPL & SPL	III

Table 3-2
UPS 2 Class II Loads

UPS 2 Load Description	Failure Impact Type
Safety Load 1 Channel A Safety Load 1 Channel B Safety Load 1 Channel C	I
Safety Load 1 SOR Down Position Sensing Pump	III
Isolation Valve Control Logic	III
RM Main Floor RM Basement	IIa
FPD System	IIa
EAFS & RM Panel	I
Access Control Panel & Access Doors	III
Public Address System	III

As tabulated above, UPS failure was determined to cause complete loss of safety-related function of some of the loads. Consequently, the limiting impact type for both UPS 1 and 2 are of Type I.

3.2 UPS Modules

Figure 3-1 is a block diagram representation of Gambit UPS hardware components.

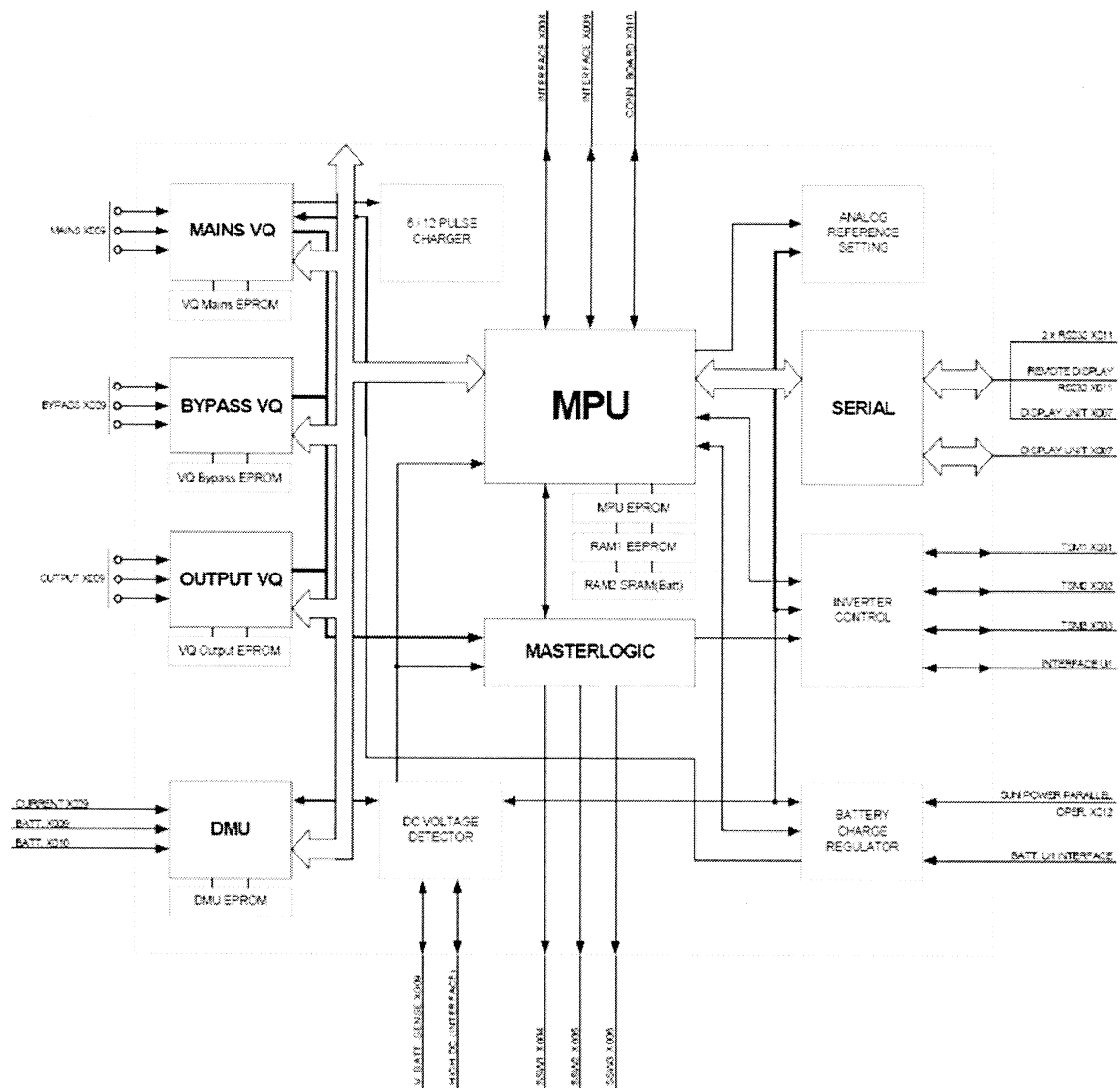


Figure 3-1 Block Diagram Representation of UPS

As illustrated above, the UPS is composed of the following major blocks:

- Voltage Quality (Mains VQ, Bypass VQ and Output VQ)
- Display Measuring Unit (DMU)
- 6/12 Pulse Charger
- DC Voltage Detector
- Main Processor Unit (MPU)
- Masterlogic
- Analog Reference Setting
- Serial I/O
- Inverter Control

- Battery Charge Regulator
- Supply Monitoring & Reset Circuit

However, since block 6/12 Pulse Charger is a subcomponent of Mains VQ, it is described as part of the latter. Similarly, blocks Analog Reference Setting and Serial I/O are described as part of MPU since they are subcomponents of it. Lastly, Battery Charge Regulator is covered as part of Inverter Control.

The function of each of above modules is elucidated in more details below.

3.2.1 Voltage Quality (VQ)

As the names implies, Voltage Quality sensors are responsible to provide information on the line voltage. VQ consists of an Intel processor and external memory. The external memory is an E²PROM type and contains software code and specific calibration values which are programmed during system calibration. Each VQ does the following activities:

- Instantaneous voltage detection of up to 3 phases
- Average voltage detection of 3 phases
- Frequency detection
- Serial Communication (to transmit the data to the MPU)
- Unit-data programming (to adjust tolerances, etc.)

As shown above, the main function of VQ is measurement of voltage and frequency and communicating these data to the MPU. If the voltage or frequency measurements are out of pre-specified tolerance ranges, a hi-speed signal is sent to the Masterlogic, which can change the UPS mode of operation, if necessary.

Figure 3-2, illustrates a simplified block diagram for a VQ sensor.

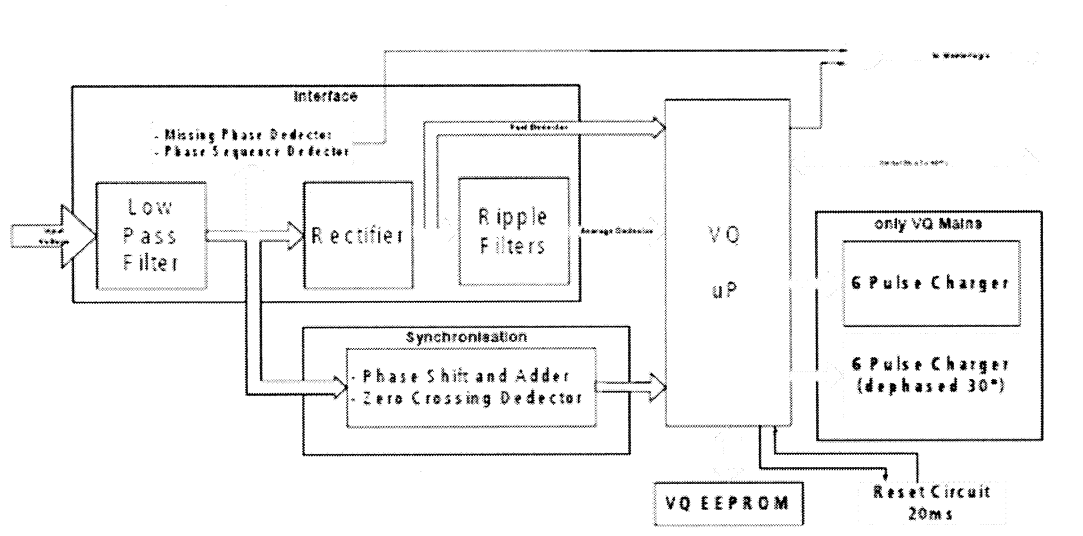


Figure 3-2 Simplified Block Diagram for a Typical VQ Sensor

As illustrated in Figure 3-2 there are three VQs in the UPS system:

- VQ Mains: monitors voltage and frequency of the incoming grid.
- VQ Bypass: monitors voltage and frequency of the bypass grid.
- VQ Output: monitors voltage and frequency quality of UPS output.

3.2.2 Display Measuring Unit (DMU)

The DMU consists of an Intel processor and an external E²PROM memory, which contains software. This module is responsible for activities such as:

- Measurement of incoming grid current (I_{MAINS})
- Measurement of inverter current (I_{INV})
- Measurement of output current (I_{OUT})
- Measurement of battery current ($I_{BATT.SENSE}$)
- Measurement of total DC current
- Measurement of battery voltage ($V_{BATT.SENSE}$)
- Measurement of battery temperature ($T_{BATT.SENSE}$)

Above measurements are taken using various sensors placed throughout the UPS system and are sent to MPU for processing via serial communication. Figure 3-3 illustrates a block diagram representation of DMU.

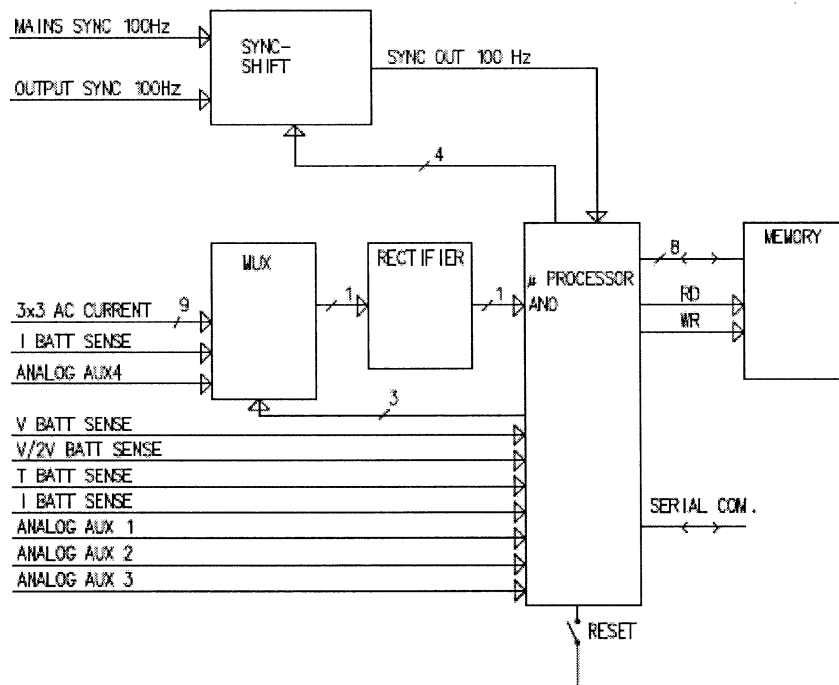


Figure 3-3 Block Diagram Representation of DMU

3.2.3 Inverter Control

This module is responsible for control of the inverter to ensure that the correct sinusoidal output is generated. Figure 3-4 illustrates the different components that Inverter Control is composed of:

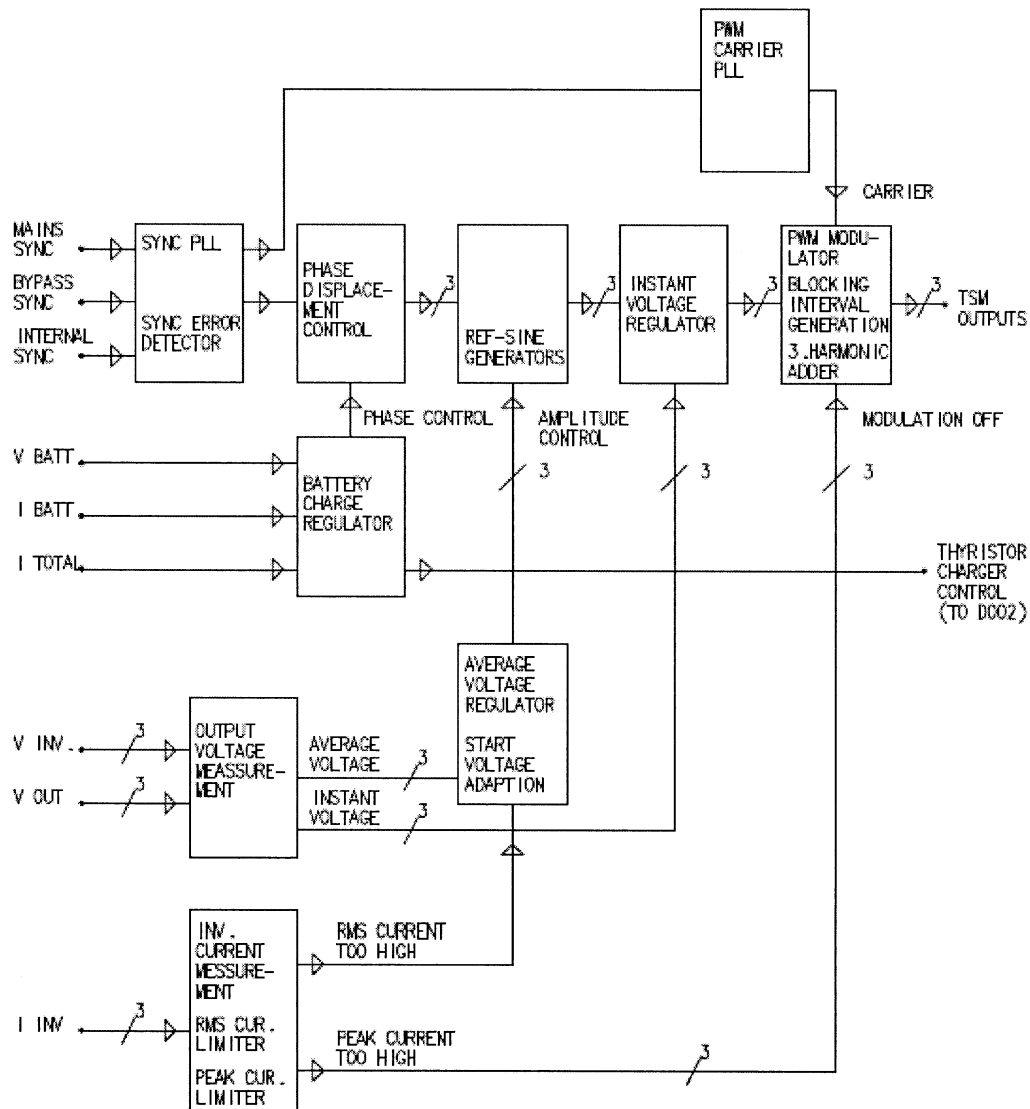


Figure 3-4 Block Diagram Representation of Invert Control

In above figure, module “Sync PLL” controls the three “Ref sine generators” via “Phase displacement control”. The job of the “Ref sine generators” is to generate reference sinusoidal voltages. “Sync PLL” is responsible to synchronize the output voltage with the grid by the means of “Phase displacement control”. Pulse Width Modulation (PWM) technique is used to make the output voltage follow the reference sinusoidal voltages as closely as possible. This is done by comparing the reference voltages with the actual output in “Instant voltage regulator”

and sending the difference to the “PWM modulator”. “PWM modulator” uses triangular carrier signal in the modulation, which is generated by “PWM Carrier PLL”.

“Output voltage measurement” and “Average voltage regulator” measure the output voltage and help keep it constant by changing the amplitude of the reference sine generators. “Inverter current measurement”, “Peak current limiter” and “RMS current limiter” protect the thyristor units against overload by measuring the corresponding currents. If the RMS current is too high, the output voltage of the system is decreased until the peak current is brought down to the acceptable limits. Battery Charge Regulator is responsible for the correct charging voltage and current of the batteries. This is done via changing the start time of the thyristors in the rectifier.

3.2.4 DC Voltage Detector

The purpose of this module is to detect battery voltage to generate any of the following signals, if necessary:

- High DC Warning
- Low DC Warning
- High DC
- Low DC

These errors are forwarded to the Masterlogic and MPU. In the case of the last two warning, the red LED on the UPS display is lit up. Figure 3-5 illustrates a block diagram representation of this module.

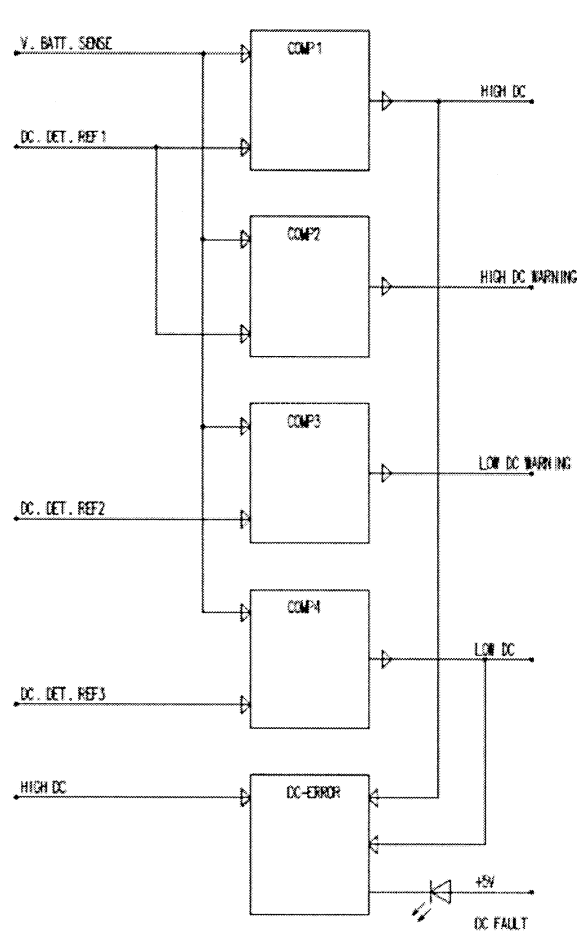


Figure 3-5 Block Diagram Representation of DC Voltage Regulator

3.2.5 Supply Monitoring & Reset Circuit

This module consists of a +12 V, -12V and +5 V monitoring circuits, as well as “mater power up reset”. Figure 3-6 illustrates a block diagram representation of this module. If a fault in one of the supply voltages is detected, “supply OK” will go low, causing the LED to turn off. This causes the microprocessors to reset. When “supply OK” goes high, the reset signals of the microprocessors will go high as well, and after a short time delay “Masterlogic reset” will go high too. This is to make sure that all the control signals to the Masterlogic are correct.

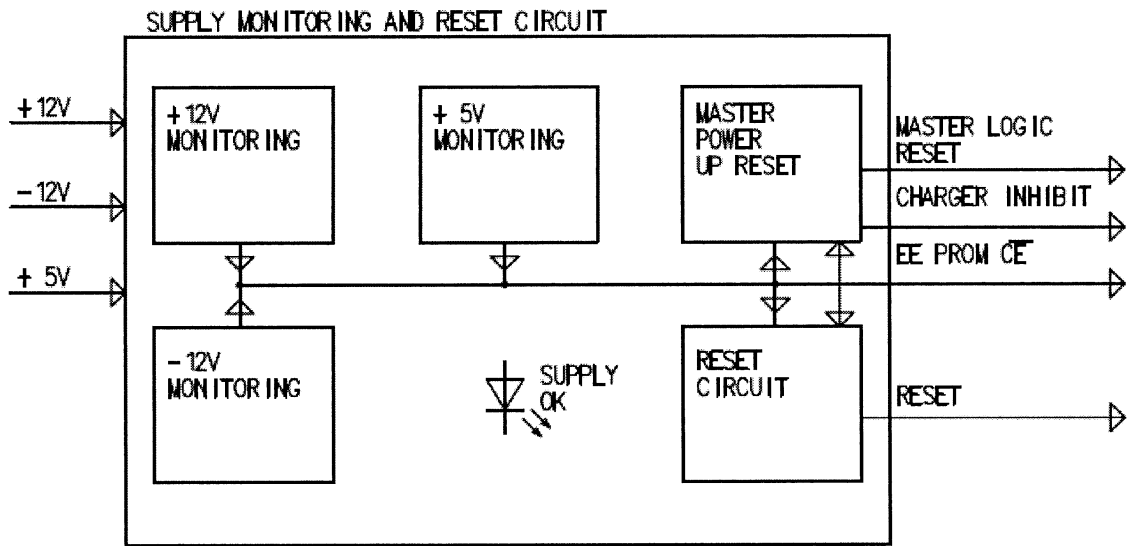


Figure 3-6 Block Diagram Representation of Supply Monitoring & Reset Circuit

3.2.6 Masterlogic

Masterlogic is one of the most important parts of the controller as it is responsible for correct and fast switching of the two static switches, EA and EN. Furthermore, it is in charge of turning the inverter on and off. The purpose of Masterlogic is to rapidly switch between the different operational modes depending on possible faults or requested operational mode. If necessary, Masterlogic can place the UPS in a safe mode (i.e. Bypass as long as it is available and within tolerance limits) without any software action from the MPU. To provide this functionality, every important signal originated by MPU or VQs is connected to one of the two Gate Array Logics (GAL). If any main parts of the UPS fail, Masterlogic reacts immediately by placing the UPS system in a safe state. Figure 3-7 illustrates a block diagram representation of Masterlogic.

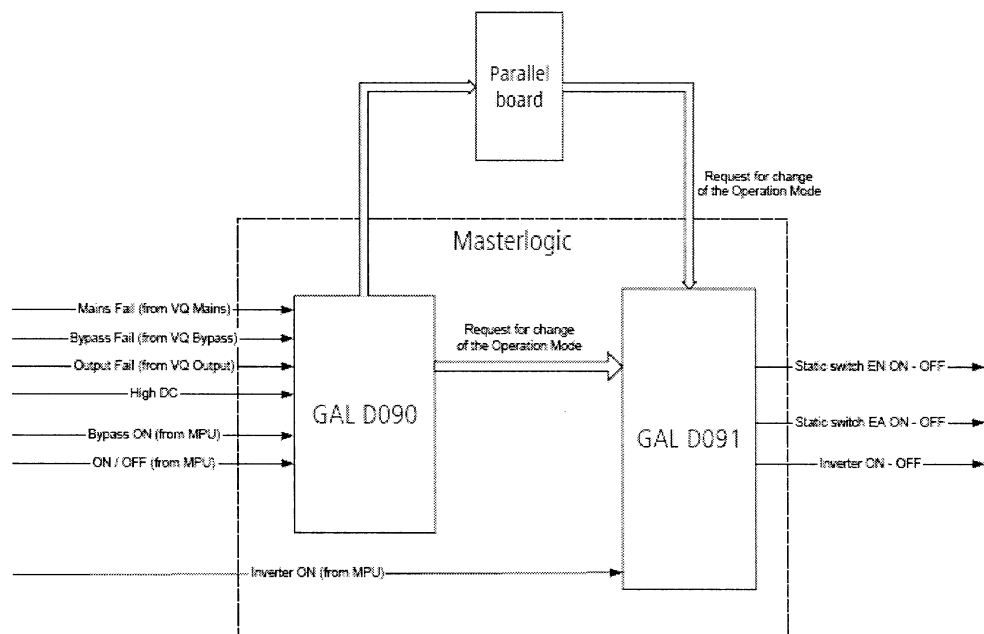


Figure 3-7 Block Diagram Representation of Masterlogic

As illustrated above, Masterlogic is divided into two blocks:

- **GAL D090:** This unit collects and processes the control signals of the UPS system. Based on these signals, decision is made as to whether a change in operational mode is necessary. If the UPS is to change operational mode, a control signal is generated by GAL D090 to GAL D091.
- **GAL D091:** This unit controls the static switches EA and EN and can also generate on/off signals to the inverter. Thus the mode of operation can be changed via GAL D091.

3.2.7 Main Processor Unit

Figure 3-8, illustrates a block diagram representation of the MPU.

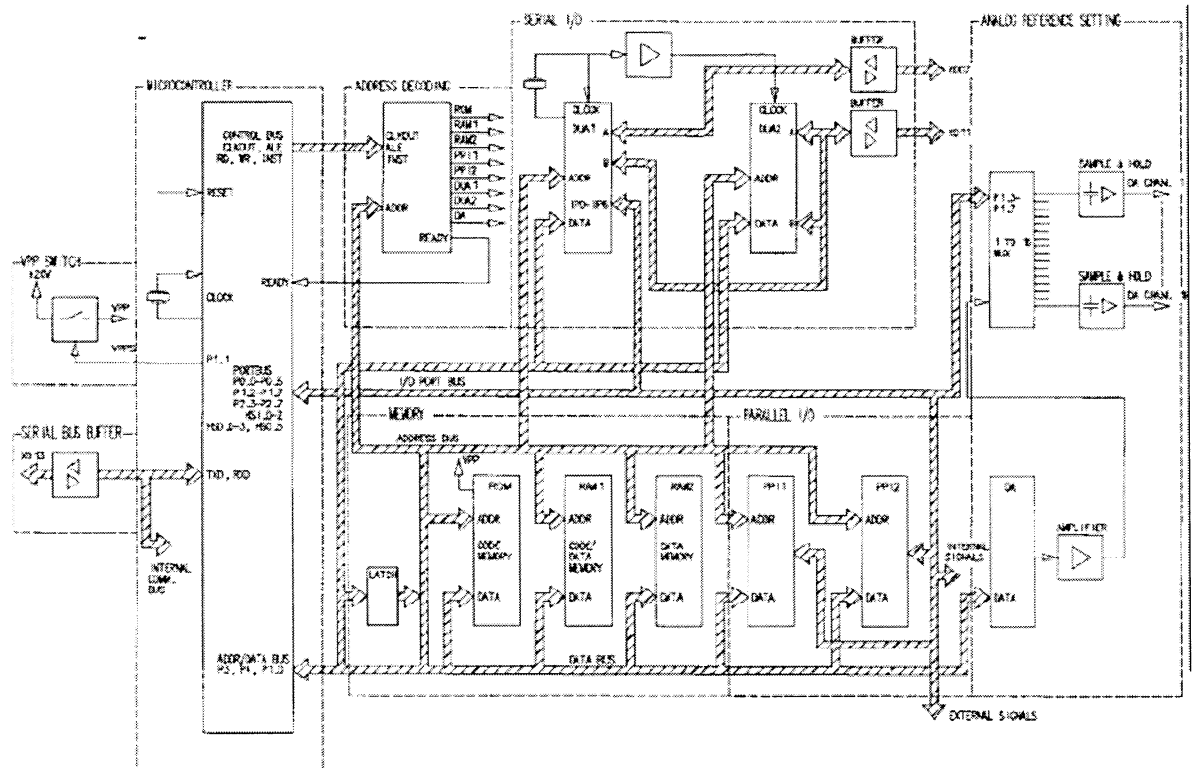


Figure 3-8 Block Diagram Representation of MPU

The microcontroller used in MPU is an Intel with built-in Random Access Memory (RAM), timers, Analog/Digital (A/D) converter, high-speed input/output unit and a serial port. The external memory of MPU is divided into three elements: ROM, RAM1 and RAM2. ROM socket contains the program run by MPU. RAM1 is reserved for constants and field texts for readout on display. RAM2 is used as the UPS systems' external memory and stores the event log stack.

MPU consists of many sub-units, which collect information from the user and from other units on the controller (i.e., VQ units, DMU, inverter, Masterlogic). As illustrated in Figure 3-8, MPU consists of the following sub-units:

- Address decoding
- VPP switch
- Serial bus buffer
- Serial I/O
- Parallel I/O
- Analog reference setting

Collection of information from other units takes place in three different ways:

- Parallel inputs
- Serial data transmission
- Measuring by the means of A/D converter

Similarly, MPU communicates to other devices on the controller in three different ways:

- Parallel outputs
- Serial data transmission
- Setting of voltage reference by means of D/A converter

4. FAILURE MODE ASSESSMENT

For both UPS 1 and UPS 2, the safety related function is to provide electrical power within acceptable limits on voltage amplitude, frequency and harmonics to UPS safety-related loads (Table 3-1 and Table 3-2). [1] These limits are defined in Appendix A of Technical Specifications [5]. Since the UPS loads are designed to fail safe in the event of loss of power, UPSs total failure (i.e., complete loss of power) does not raise a safety concern. The only concern is UPSs partial failure where the loads are supplied with out-of-specification power (i.e., “dirty power”), undetected. Under partial failure, instruments, whether powered directly from the affected UPS, or deriving power from switched mode dc supplies powered from the UPS, continue to receive power, and therefore safety function of systems such as Safety Load systems SL1 and SL2 may be jeopardized since some trip relays may fail to de-energize and open trip contacts, when the measured parameter exceeds the required setpoint. Thus, load system alarms and mitigating features may not operate as required. Relay logic can remain energized under partial power failure, but, in case of low voltage, some relays may drop out, so that correct operation cannot be assured.

Hence, possibility of UPS partial failure and ability of UPSs to detect partial failure is to be examined in more details.

4.1 Analysis of UPS Common Cause Failure at Hardware Level

IEC 60880-2 defines Common Cause Failure (CCF) as a failure, which is the result of one or more events, causing coincident failures of two or more separate channels in a multiple channel system or in multiple systems, leading to system(s) failure.

At system level, a CCF can occur in redundant systems because of the fact that Gambit uses the same kind of firmware for all the UPS systems. Therefore, if a common cause failure potential were to exist, use of redundant UPS systems would not help prevent it due to lack of diversification of firmware (i.e., use of a different firmware in the redundant UPS system). [11] However, this is not a concern since the UPS systems in R1 and R2 reactors are of single configuration.

Figure 4-1 illustrates all the connection between the essential components of a Gambit UPS system:

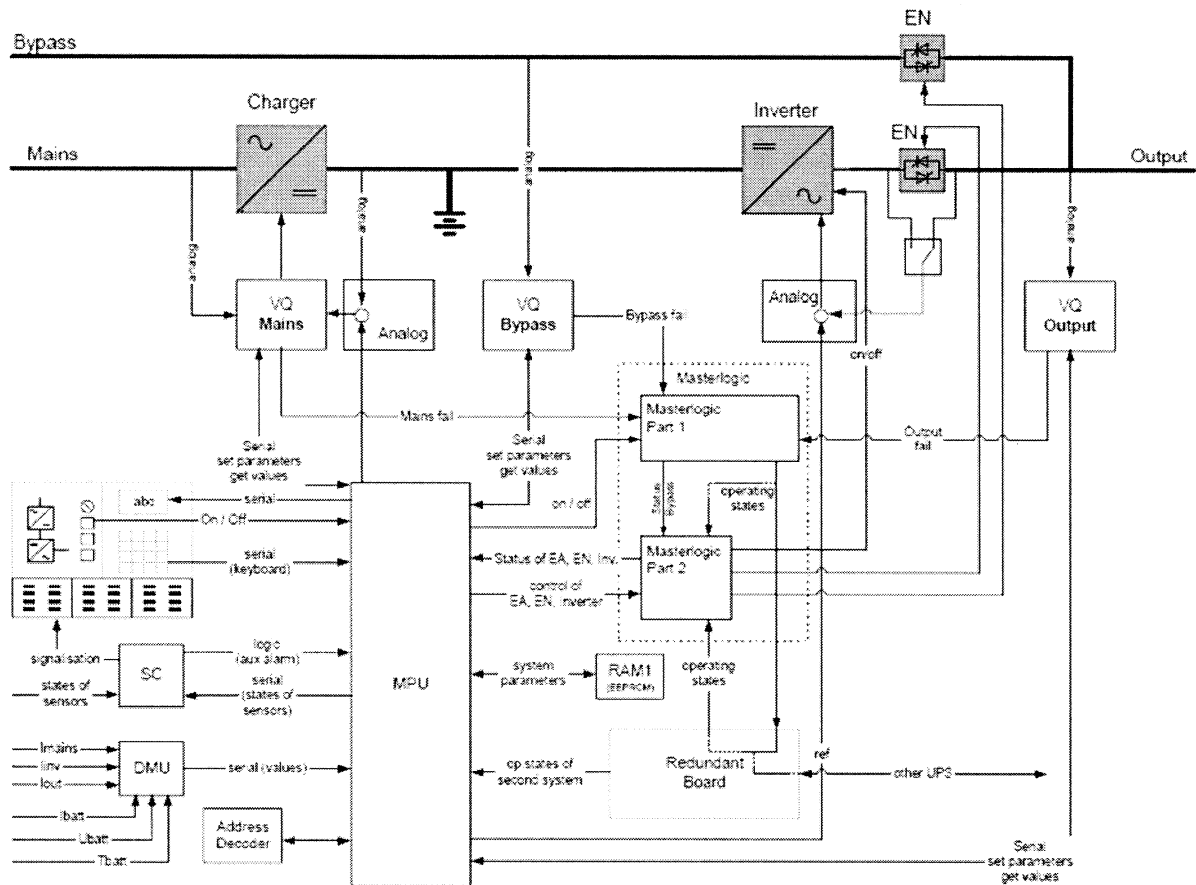


Figure 4-1 Block Diagram Representation of Gambit UPS System

The following parts are identified as potential sources for occurrence of a CCF: [11]

- Main Processor Unit (MPU)
- VQ Mains, VQ Bypass, VQ Output
- Display Measuring Unit (DMU)
- Masterlogic
- Address Decoder
- Signalling Controller,
- Display Unit

“Address Decoder” is not part of Figure 4-1 since it operates simply as chip selector and would complicate the diagram tremendously since it is connected to every chip.

Static inverter switch (EA) and static bypass switch (EN) are directly in charge of the output voltage. If these switches do not work properly, output voltage is no longer guaranteed. The failure impact of each of above potential CCF sources on the safety-related function of the UPS, which is to provide electrical power, within acceptable limits on voltage amplitude, frequency and harmonics to UPS safety-related loads [1], is discussed in more details below.

4.1.1 Main Processor Unit (MPU)

MPU is the brain of the system and controls almost every function of the UPS. Consequently, it is the most critical component with respect to common cause failure. For instance, if one of the firmware modules enters into a never-ending loop, or causes an undefined behaviour of the MPU, the system output may be lost because control of EA and EN will break down.

The program run by MPU consists of the following tasks. Every module is categorized as either safety-related or non-safety-related.

Table 4-1
MPU Firmware Task Composition

	Module	Safety Related	Comments
1	Sync signal to inverter	YES	
2	System control not handled by Masterlogic	YES	
3	Display handling	NO	Only used to control display
4	Serial communication to VQ units and DMU	YES	
5	AC voltage measurement calculations	YES	
6	AC and DC current measurement calculations	YES	
7	Output current limiter function	YES	
8	Adaptive slew rate function	YES	
9	System calibration functions	NO	Only used during system calibration

Since most of above modules are directly or indirectly involved with control on EA and EN, a malfunction in the MPU can affect the output voltage. As noted in above table, modules 3 and 9 are not safety related since they are only used for display control and calibration purposes, respectively. Failure of these modules will in no way affect the UPS output voltage.

The remaining modules perform safety-related activities and their malfunction can result a fatal error of the system such that the output of the UPS may be lost. However, this is not a concern since the loads are designed to fail safe in the event of power interruption. It is concluded that although MPU is a potential source of CCF, its failure cannot affect the safety function of the UPS.

4.1.2 Display Measuring Unit (DMU)

The DMU is responsible for activities such as:

- Measurement of incoming grid current (I_{MAINS})
- Measurement of inverter current (I_{INV})
- Measurement of output current (I_{OUT})
- Measurement of battery current ($I_{BATT.SENSE}$),
- Measurement of total DC current
- Measurement of battery voltage ($V_{BATT.SENSE}$)
- Measurement of battery temperature ($T_{BATT.SENSE}$)

Above measurements are sent to MPU for processing. Since above measurements are critical to the operation of the UPS, a malfunction in DMU can result a fatal error in the UPS system such that the output is lost. However, this is not a concern since the loads are designed to fail safe in the event of power interruption. It is concluded that although DMU is a potential source of CCF, its failure cannot affect the safety function of the UPS.

4.1.3 Masterlogic

Masterlogic is one of the most important parts of the controller as it is responsible for correct and fast switching of the two static switches, EA and EN. Furthermore, it is in charge of turning the inverter on and off. The purpose of Masterlogic is to rapidly switch between the different operational modes depending on possible faults or requested operational mode. However, as illustrated in Figure 3-7, the hardware design of Masterlogic is very simple. Similarly, due to the simplicity of the firmware in Masterlogic, it is assumed to be very reliable and therefore not a source for CCF. This analysis was part of the information that was sent by Gambit to TUV Nord in order to obtain certificate of conformance too IEC 60880-2. [14]

4.1.4 Address Decoder

This chip is responsible for sending chip-select signals to all external devices in memory, serial I/O, parallel I/O and analog reference setting module. It also supplies “READY” signal to the microprocessor to indicate when an external device is available to receive data. Address Decoder is a Gate Array Logic and only contains logical combinations. Similar to Masterlogic, due to simplicity of firmware and hardware design, Address Decoder is assumed to be very reliable and not a source of CCF.

4.1.5 Signal Controller (SC)

The purpose of SC is to extend information on the status of the UPS system to the user in the form of LED's and relays. Signal Controller only receives serial information about errors and/or operational modes from the Controller. It can by no means do any action that will cause a common cause failure in the UPS system. Therefore, SC is not a potential source of CCF.

4.1.6 Display Unit (DU)

As shown in Figure 4-2, the Display Unit is located on the front of the UPS system and consists of a liquid crystal display, an alarm LED, an acoustic alarm and a foil keyboard. DU is used for purposes such as programming the system (i.e., language, time, date, etc.) and manual switch to Bypass mode of operation. DU is only responsible for displaying various values via Human-Machine-Interface. Therefore it is not a potential source of CCF.

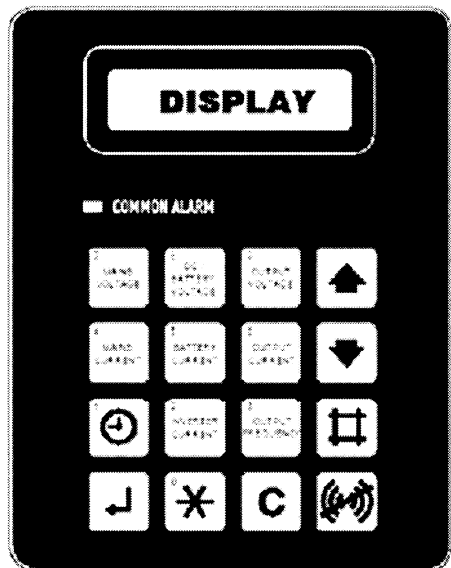


Figure 4-2 Display Unit of Gambit UPS

4.1.7 Voltage Quality (VQ)

As the names implies, Voltage Quality sensors are responsible to provide information on the line voltage. VQ consists of an Intel processor and external memory. The external memory is in as E²PROM and contains software code and specific calibration values which are programmed during system calibration. Each VQ does the following activities:

- Instantaneous voltage detection of up to 3 phases
- Average voltage detection of 3 phases
- Frequency detection
- Serial Communication (to transmit the data to the MPU)
- Unit-data programming (to adjust tolerances, etc.)

If either voltage or frequency is detected to be out of tolerance limits, Masterlogic receives a hi-speed signal and, if necessary, UPSs mode of operation is changed accordingly. As illustrated in Figure 4-1, there are three VQs in the UPS system:

- VQ Mains
- VQ Bypass
- VQ Output

Next, the potential of these VQs to result a CCF is assessed.

4.1.7.1 VQ Mains

This sensor is responsible for voltage and frequency measurement of the incoming grid and hence control of the rectifier. In the event of VQ-Mains failure, grid voltage monitoring is no longer performed and therefore communication with MPU will breakdown. Table 4-2 lists all the possible communications that exist between the MPU and VQ-Mains:

Table 4-2
List of Communications Between MPU and VQ-Mains

MPU → VQ Mains	VQ Mains → MPU
Upper shut down limit for the charger	Average value of Mains voltage
Frequency tolerance for Mains voltage	Fail info: Mains voltage is out of tolerance
Upper limit for Mains voltage average detector	Fail info: Mains frequency is out of tolerance
Lower limit for the Mains voltage average detector	Fail info: Mains detector is not synchronized
Some configuration values to adjust the behaviour of the firmware	Control info: Charger error
	Control info: Charger is on
	Control info: Detection limit of the voltage
	Control info: Programming of the EEPROM in completed

Two consequences can arise due to VQ-Mains failure:

- Rectifier stops working; and / or
- Grid voltage is no longer monitored.

In either case an alarm will be generated and the UPS system will change over to Battery Operation mode. Therefore, it is concluded that a VQ-Main failure cannot affect the output of the system and therefore is not a source for CCF.

4.1.7.2 VQ Bypass

This sensor monitors the bypass voltage. Table 4-3 lists all the possible communications between MPU and VQ-Bypass:

Table 4-3
List of Communications Between MPU and VQ-Bypass

MPU → VQ Bypass	VQ Bypass → MPU
Frequency tolerance for Bypass voltage	Average value of the Bypass voltage
Upper limit for Bypass voltage momentary detector	Fail info: Bypass voltage is out of tolerance
Lower limit for Bypass voltage momentary detector	Fail info: Bypass frequency is out of tolerance
Upper limit for Bypass voltage average detector	Fail info: Bypass detector is not synchronized
Lower limit for Bypass voltage average detector	Control info: Detection limit of the voltage
Some configuration values to adjust the behaviour of the firmware	Control info: Programming of the EEPROM in progress
	Control info: Programming of the EEPROM in completed

In the event of VQ-Bypass failure, the synchronization between grid and bypass voltage will fail and “SYNCH ERROR” alarm signal will be generated. This way MPU is notified of un-synchronized bypass and thus change to Bypass mode of operation will be prohibited, even if both grid and battery become unavailable or go out of tolerance limits. Consequently, in the case of VQ-Bypass failure, and grid and battery unavailability, the output of the UPS will be lost. Hence, it can be conservatively concluded that failure of VQ-Bypass is a source for CCF. However, a failure in VQ-Bypass cannot affect the UPS such that the loads are supplied with out-of-specification power, since VQ-Output is in charge of monitoring system output even when UPS is running in Bypass mode of operation. Therefore, it is concluded that although VQ-Bypass is a potential source of CCF, its failure cannot affect the safety function of the UPS.

4.1.7.3 VQ Output

This sensor is used to monitor the output voltage.

Table 4-4 lists all the possible communications between VQ-Output and MPU:

Table 4-4
List of Communications Between MPU and VQ-Output

MPU → VQ Output	VQ Output → MPU
Frequency tolerance for Output voltage	Average value of the Output voltage
Upper limit for Output voltage momentary detector	Fail info: Output voltage is out of tolerance
Lower limit for Output voltage momentary detector	Fail info: Output frequency is out of tolerance
Upper limit for Output voltage average detector	Fail info: Output detector is not synchronized
Lower limit for Output voltage average detector	Control info: Detection limit of the voltage
Some configuration values to adjust the behaviour of the firmware	Control info: Programming of the EEPROM in progress
	Control info: Programming of the EEPROM in completed

If this VQ fails, the system will automatically switch to Bypass mode of operation. Furthermore, two alarm signals will be generated:

- OUTPUT INST OUT OF TOL
- OUTPUT FREQUENCY OUT OF TOL

It is concluded that since output voltage is not interrupted in the event of VQ-Output failure, it cannot be a source for CCF. However, failure of VQ-Output can potentially impair the affected UPS system's safety function since the loads will be prone to receipt of undetected dirty power. For instance, if the inverter malfunctions such that output voltage and frequency are out of tolerance limits, given that VQ-Output has failed, the loads are open to receive undetected "dirty power". This circumstance is further examined in Section 4.4.

4.1.7.4 Combined VQ Failures

Although all three VQ processors are operated independent from each other, potential for common cause failure of UPS system exists if more than one VQ failure occurs at a time. Table 4-5 lists the possible combinations of VQ failures and the associated consequences:

Table 4-5
Combined VQ Failures and Consequences

Combined VQ Failure	Consequence	Loss of Output
VQ Mains and VQ Bypass	The output of the system would not be affected. The output would be supplied by Battery voltage.	NO
VQ Mains and VQ Output	The output of the system would not be affected; a switch to Bypass mode would be the consequence.	NO
VQ Bypass and VQ Output	The output would get lost, because the system will not switch over to Bypass supply or batteries.	YES
VQ Mains, VQ Bypass and VQ Output	The output would get lost, because the system will not switch over to Bypass supply.	YES

As demonstrated in above table, simultaneous failure of all three VQs, and also, simultaneous failure of VQ-Output and VQ-Bypass would cause loss of output voltage and are therefore sources for common cause failure. However, since the loads are designed to fail-safe in the event of power interruption, these failures do not impair the affected UPS's safety function. As indicated previously, the only failures of concerns are those that include malfunction of VQ-Output. This circumstance is further examined in Section 4.4.

4.2 Analysis of Common Cause Failure at Software Level

The possibility of UPS common cause failure due to firmware malfunction exists simply because some functions are partially called from different routines and the same global variables are used in several software modules. [11]

At software level, concept of diversity would only be applicable to redundant system configuration. Usage of firmware diversity in a UPS system implies development of a completely different firmware for each redundant system to eliminate the possibility of output voltage failure due to firmware malfunction. However, firmware diversity is not applicable since the UPS systems for this project are of single configuration.

The possibility of common cause failure is minimized via UPS self-monitoring features and a highly reliable firmware (see Section 7.3 and appropriate subsections). Gambit UPS system performs various self-monitoring functions which generates alarm(s) in the event of a detected failure.

By the end of year 2004, the firmware used in the purchased Gambit UPS systems, WXX firmware package 2, accumulated a total operating experience of 434 years with zero recorded

fatal failures, which corresponded to failure rate of 2.63560×10^{-7} . [13] This figure in addition to the TUV Nord certification of firmware, demonstrated a high reliability of the firmware and thus a reasonably low possibility of UPS CCF due to firmware. Subsections of Section 7.3 of this report demonstrate that the accumulated operating hours satisfied the minimum requirements associated with a Category-B PES.

4.3 Application Context Failure Mode Assessment

For both UPS 1 and UPS 2, the safety related function is to provide electrical power within acceptable limits on voltage amplitude, frequency and harmonics to UPS safety-related loads (Table 3-1 and Table 3-2). These limits are defined in Appendix A of Technical Specifications [5]. Since the UPS loads are designed to fail safe in the event of loss of power, UPSs total failure (i.e., complete loss of power) is not a concern. The only concern is UPSs partial failure where when the loads are supplied with out-of-specification-power (i.e., “dirty” power). Since it is unknown whether the loads will continue to fail-safe if provided with “dirty” power, ability of UPS’s to detect partial failure is to be examined in more details.

Below, the failure impact of each of UPS components with respect to UPS safety related function is examined. In these examinations, only complete failure of each component is considered as partial failure of components is unlikely and would complicate the assessment significantly.

4.3.1 VQ Mains

This sensor is responsible for voltage measurement of the incoming grid and hence control of the rectifier. In the event of VQ-Mains failure, grid voltage monitoring is no longer performed and therefore communication to the MPU is broken down. Two consequences can arise due to VQ-Mains failure:

- Rectifier stops working; and / or
- Grid voltage and frequency is no longer monitored.

In either case “MAINS FREQUENCY ERROR” alarm will be generated which results the UPS to change mode of operation to Battery. In the event that VQ-Mains fails undetected such that above alarms are not generated, if the incoming grid power quality deteriorates, VQ-Output will generate the appropriate alarm(s) which will cause the UPS to take corrective actions (i.e., change modes of operation, shut down, etc.).

Therefore, it can be concluded that since VQ-Mains failure cannot affect output power quality of the UPS, it is not a source for UPS partial failure and hence it cannot jeopardize the safety function of the UPS.

4.3.2 VQ Bypass

This sensor monitors the bypass voltage and frequency. In the event of VQ-Bypass failure, the synchronization between grid and bypass voltage fails and “SYNCH ERROR” alarm signal is generated. This inhibits the MPU from changing to Bypass mode of operation, in the event of unavailability of grid or battery. In the event that VQ-Bypass fails undetected and the UPS is running in Bypass mode of operation, if bypass grid’s power quality deteriorates, VQ-Output will generate the appropriate alarm(s) which will cause the UPS to take corrective actions (i.e., change modes of operation, shut down, etc.).

Therefore, it can be concluded that since VQ-Bypass failure cannot affect output power quality of the UPS, it is not a source for UPS partial failure and hence it cannot jeopardize the safety function of the UPS.

4.3.3 VQ Output

This sensor is used to monitor the output voltage. If this VQ fails, the system will automatically switch to Bypass mode of operation. Furthermore, two alarm signals will be generated:

- OUTPUT INST OUT OF TOL
- OUTPUT FREQUENCY OUT OF TOL

However, if VQ-Output fails undetected, the possibility of supplying the loads with dirty power in circumstances such as inverter failure exists, since the UPS is no longer monitoring the output power quality (i.e., voltage and frequency). Since the loads are designed to fail safe only in event of complete loss of power, VQ-Output failure jeopardizes the safe operation of the plant as it can negatively impact safety-related loads such as Safety Loads 1 and 2.

Since VQ-Output is the last line of defence against UPS partial failure, it can be concluded that its failure has a direct impact on UPS safety function.

4.3.4 Combined VQ Failures

In the events of VQ output failure in combination with any of the other two VQs, the safety function of the UPS is no longer met since the possibility of undetected output of dirty power to loads exists. Hence, as expected, the limiting factor for combined VQ failures is failure of VQ-Output.

4.3.5 Display Measuring Unit (DMU)

Since this unit is responsible for the measuring the currents in grid, bypass, output and battery as well as the battery voltage and temperature, a malfunction can affect the UPS output in such a way that the mode of operation can mistakenly be changed. For instance, assuming the UPS is operating in Battery mode, if DMU erroneously sends a battery-voltage-out-of-tolerance signal to MPU, the mode of operation will change to Bypass. At the same time, alarm indications will inform the operator of the fault and a technician will be able to diagnose the problem. However, this type of failure cannot affect the UPS's output power quality and is therefore not a concern.

4.3.6 Inverter Control

This module is responsible for correct generation of sinusoidal AC voltage for loads. Malfunction of inverter control can lead to generation of out-of-specification power, which, if undetected, can have a negative impact of the safe operation of the safety-related loads of UPSs. However, a failure in inverter will be detected by VQ-Output in terms of voltage/frequency error. This failure will be reported to the MPU, which will in turn change the mode of operation to either Bypass, if available.

Therefore, although the correct operation of inverter is critical to the UPS, as long as VQ output is functional, failure of inverter/inverter control module does not cause a UPS partial failure, and hence cannot affect the safety function of the UPS.

4.3.7 DC Voltage Detector

This unit is responsible for detecting battery voltage and sending alarm signals to the Masterlogic and MPU in the event that voltage is out of predefined tolerance limits. Failure of DC Voltage Detector will result lack of battery-voltage monitoring. This becomes a critical issue when the UPS is operated in Battery mode of operation since the loads are powered by the battery via the inverter. However, failure of this unit cannot result UPS partial failure since VQ-Output will sense out-of-specification power and will force the UPS to either switch the mode of operation or shut down. In either scenario, safety function of the UPS is not jeopardized and the loads will continue to fail safe, if necessary. Therefore, it is concluded that the failure of this unit will not cause a UPS partial failure.

4.3.8 Supply Monitoring & Reset Circuit

This module consists of a +12 V, -12V and +5 V monitoring circuits, as well as “mater power up reset”. Failure of this component cannot in any way cause a partial failure of the UPS.

4.3.9 Masterlogic

Failure of Masterlogic can result any of the following:

- Failure of static switches EA and EN: which will paralyse the system from switching modes of operation.
- Inverter shutdown: which will result the UPS output be lost in Battery and Normal modes of operation.

In either of above scenarios, the output of the UPS cannot fail partially such that the loads receive “dirty power”. If VQ-Output senses out-specification-power and the UPS is unable to change modes of operation, it will simply shut down. However, since the loads are designed to fail-safe in the event of power disruption, this does not pose a safety threat. Therefore, it is concluded that failure of Masterlogic cannot jeopardize the safe operation of the UPS and the subsequent loads.

4.3.10 Main Processor Unit (MPU)

MPU is the brain the UPS system and processes all the data that is sent to it by all other components within the UPS, as well as the operator (i.e., manual inputs). MPU, with the help of Masterlogic makes the UPS switch to different modes of operation, based on the inputs received from operator and peripheral sensors (i.e., VQs). It is difficult to predict the exact types of failure in the event of MPU malfunction. However, considering that the UPS’s safety function is to supply the loads with “clean power”, the most crucial failure that can arise by failure of MPU is inability of this unit to process VQ-Output’s signal in the event that supply of “dirty power” is detected. Under this circumstance, MPU will fail to switch the mode of UPS operation and loads will continue to receive out-of-specification power. However, as stated before, since UPS’s subcomponents partial failure is not considered in this analysis, failure of MPU is equivalent to failure of the whole UPS system, which results interruption of UPS output, causing the loads to fail-safe. Therefore it is concluded that failure of MPU is not a source of UPS partial failure, as failure of this component results complete failure of the UPS, which is not a safety concern.

4.4 Safety-Related Risks and Consequences of System Failure

Although more than one UPS components were identified as sources for hardware/software Common Cause Failure, VQ-Output is the only unit whose failure could jeopardize UPS's safety function. Similarly, as stated in Section 4.3, VQ-Output is the last line of defence against receipt of "dirty power" by loads. If this component fails, the loads become vulnerable to UPS failure and may not fail-safe. UPS partial failure was considered to have a failure impact type I, where complete loss of safety-related function of the loads (i.e., SL1, SL2, RCCS, etc.) may occur. However, it must be noted that in the event that the UPS is running in Bypass mode of operation while VQ-Output is failed undetected, if Bypass starts to supply out-of-specification power to the UPS, other metering equipment on the Bypass will detect the supply failure, thus the onus is not placed on VQ-Output.

Table 3-1 and Table 3-2 list the failure impact types for all the loads associated with UPS 1 and UPS 2, in the event of UPS partial failure [1].

Considering the possibility of such a partial failure, Category-B classification was assigned to the UPS by the categorization report [1]. In Section 7.3.2 of this report it was demonstrated that the purchased UPS systems met and exceeded the reliability requirements, in terms of unit-hours of operation, associated with a Category-B PES, thus it was concluded that the possibility of a random failure such that the loads are supplied with undetected out-of-specification power, is sufficiently low.

5. ASPQ SUITABILITY REQUIREMENTS

Technical Specifications [5] outlined the minimum requirements associated with UPS 1 and UPS 2 to provide the safety related control and instrumentation loads with 120V single-phase power. Subsequent sections summarize these requirements.

5.1 Safety Attributes, Fail Safe or Fail Detected Behaviour

As a minimum, the UPS Trouble alarm shall be actuated on any of the following conditions:

- Alternate power supply voltage outside tolerance limits.
- Alternate power supply frequency outside tolerance limits.
- Inverter output voltage outside tolerance limits.
- Inverter output frequency outside tolerance limits (free running) or inverter not synchronized.
- Low Battery voltage.

All UPS alarms shall be grouped to provide Form C contacts, having a rating of not less than 1 A at 24 V DC. The grouped alarm contacts shall be wired out to an interface terminal block for remote computer monitoring. As a minimum, the following alarms and status indications shall be provided for remote monitoring:

- UPS Trouble (Indicates any UPS malfunction or failure).
- UPS On Battery (Indicates that the UPS loads are powered from the batteries).
- UPS On Bypass (Indicates that the UPS loads are powered from the alternate source).

The UPS Trouble alarm shall be latched with provision for being reset at the UPS cabinet. Where applicable, test push-buttons shall be provided to facilitate the periodic testing of indicating lamps and alarm devices.

5.2 Functionality

The UPS shall be designed to function in any of the following modes of operation.

5.2.1 Normal Mode

Under normal operating conditions the UPS shall be energized from the AC Class III bus such that the UPS batteries are maintained in a fully charged condition, the inverter output is energizing the Class II safety related loads via distribution panel, and the inverter output is in synchronism with the Class III 120 V single phase alternate power supply.

5.2.2 Abnormal Mode

If there is a malfunction in the inverter, the UPS static transfer switch shall transfer the UPS load to the Class III alternate (bypass) power source. This transfer shall be automatic, if initiated by an inverter malfunction, and shall be accomplished without any loss of power continuity or disturbance at the UPS loads.

5.2.3 Emergency Mode

If Class III normal and alternate (bypass) sources of power fail, and the UPS is being energized from the normal power supply, the UPS batteries shall be capable of energizing the UPS loads at rated full load output for the duration specified in Table 5-1:

Table 5-1
Battery Performance Requirements

UPS	Capacity [kVA]	Power Factor	Duration [min]
R1 UPS 1	20	0.8	30
R1 UPS 2	8	0.8	180
R2 UPS 1	20	0.8	30
R2 UPS 2	8	0.8	180

If the UPS is operating on the alternate mode as a consequence of an inverter malfunction, and the alternate supply fails, the UPS will become unavailable as a source of power to UPS Class II loads. Under these circumstances, operator action will be required to manually restore power to the UPS loads from another on-site power source.

5.2.4 Maintenance Mode

The UPS shall be provided with a manually operated make-before-break bypass switch to enable the Class II bus to be energized from the Class III alternate power supply with the battery charger, inverter and static transfer switch all bypassed. Provision shall be made to ensure that this switch can only be operated provided the alternate power supply is in synchronism with the Class II safety load bus.

The UPS shall be provided with bus terminal connections, via a fused disconnect switch, for load testing. The test terminals shall be located such that an external load bank can be connected to the terminals.

Testing shall only be carried out after transferring the class II load bus to the alternate power supply by closing the maintenance bypass switch without any power interruption at the Class II bus.

5.2.5 Return to Normal Operating Conditions

Provisions shall be made to enable an operator or maintainer to return the UPS from maintenance or abnormal modes of operation, back to normal mode. In addition, provision for automatic transfer back to normal mode of operation shall be made.

When operating in emergency mode, and following restoration of normal Class III power supply, the UPS shall automatically pick up the Class II safety loads and the rectifier/charger shall start to recharge the batteries. In addition, if the normal Class III power supply has been lost for a defined time period between 1 and 6 minutes, an equalizing charge of the batteries shall be automatically initiated.

Following restoration of the normal Class III power supply, the rectifier/charger shall be capable of immediately accepting a load. The inverters shall be self-starting and capable of accepting loads up to their current limit upon restoration of the dc input.

5.3 Performance

The rectifier/battery charger, battery bank, inverter and static transfer switch shall meet or exceed all the technical requirements specified below:

Table 5-2
UPS Performance Requirements

R1 UPS1	20 kVA, 120V ac single phase output at 0.8 lagging Power Factor. Typical loads include switching power supplies and pool lighting (ballast).
R1 UPS2	8 kVA, 120V ac single phase output at 0.8 lagging Power Factor. Typical loads include switching power supplies and 1HP pump motor.
R2 UPS1	20 kVA, 120V ac single phase output at 0.8 lagging Power Factor. Typical loads include switching power supplies and pool lighting (ballast).
R2 UPS2	8 kVA, 120V ac single phase output at 0.8 lagging Power Factor. Typical loads include switching power supplies and 1HP pump motor.
Normal UPS Input Power Supply:	208 V, 3 phase, 3 wire
Normal Power Supply Input Voltage:	208 V \pm 10%
Alternate UPS Power Supply:	120 V, 1 phase, 2 wire
Alternate Power Supply Input Voltage:	120 V \pm 10%
Input Frequency:	60 Hz, \pm 5%
UPS Output:	120 V, 1 phase, 2 wire, 60 Hz.
UPS Load Power Factor:	0.8 to 1.0 lagging
Enclosure:	NEMA 1 with drip shield
Audible Noise Level:	<70 dBA at 1 m.
Normal Ambient Temp:	20°C \pm 5°C
Min. / Max. Ambient Temp:	10°C / 40°C
Relative Humidity:	< 95% at < 200 m above sea level

Table 5-3
Inverter Performance Requirements

Nominal Output Voltage	120 V, 1 phase, 2 wire, 60 Hz.
Output Voltage Regulation	$\pm 5\%$ for any combination of changes to the load (0 to 100% with 1.0 to 0.8 lagging power factor), inverter dc input voltage (up to 110% rated) and ambient temperature (15°C to 40°C).
Voltage Transient Response	$< \pm 10\%$ for a 100% step load change or transfer to the <i>alternate</i> power supply. Recovery to $\pm 3\%$ shall be achieved in $< 100\text{ms}$.
Output Voltage Adjustment	$\pm 5\%$
Output Frequency Stability	$< \pm 0.5$ Hz when operating in free running mode.
Output waveform	Sinusoidal
Harmonic Distortion	$< 5\%$ THD (10 -100% load; 0.8 -1.0 PF); up to 90% Non Linear load. Any single harmonic of the PWM switching frequency shall be less than 0.1 % of the 60 Hz output voltage.
Over -current Capability	125% for 10 minutes and 150% for 30 s., each without the <i>alternate</i> power source.
Slew Rate	< 1.0 Hz/s.
Crest Factor	> 3.0 @ full load

Table 5-4
Rectifier/Battery Charger Performance Requirements

Rated Output Current:	Sufficient to recharge the battery from a fully discharged state to nominal values within 12 hours while simultaneously supporting the continuous UPS Class II full load.
Current limit:	>120% of the rated output current.
Output Ripple Voltage	Sufficiently low to permit the inverter to operate correctly under any load conditions with the battery disconnected, and < 2% with batteries connected.
Harmonics Reflection	<1% harmonics reflected into supply side.
Rectifier	12 Pulse
Nominal Float Voltage	Per Supplier's standard.
Float Voltage Adjustment	± 5 %
Nominal Equalize Voltage	Per Supplier's standard.
Equalize Voltage Adjustment	± 5 %
Output Voltage Regulation	± 1% for any combination of changes to the load (0 to 100%), nominal input voltage (±10%) and ambient temperature (15°C to 40°C).

**Table 5-5
Battery Performance Requirements**

Type:	Lead Acid Sealed, maintenance free
Ampere -Hour Rating:	Sufficient to supply dc to the inverter to provide output to UPS loads.
R1 UPS 1	Battery capacity to be sized to support the Inverter output of 20 kVA at 0.8 Power Factor for 30 minutes.
R1 UPS 2	Battery capacity to be sized to support the Inverter output of 8 kVA at 0.8 Power Factor for 180 minutes
R2 UPS 1	Battery capacity to be sized to support the Inverter output of 20 kVA at 0.8 Power Factor for 30 minutes.
R2 UPS 2	Battery capacity to be sized to support the Inverter output of 8 kVA at 0.8 Power Factor for 180 minutes

**Table 5-6
Static Transfer Switch Performance Requirements**

Type:	Solid State, Single phase
R1 UPS1 Rating	20 kVA
R1 UPS2 Rating	8 kVA
R2 UPS1 Rating	20 kVA
R2 UPS2 Rating	8 kVA
Nominal Voltage	120 V single phase.
Power Factor	0.8 to 1.0 lagging
Switch Operation	Make -before -break
Maximum Transfer Time	< 10 ms
Over -Load Capability	Same as Inverter.

5.3.1 Battery Charger/Rectifier

Each battery charger/rectifier shall be a constant voltage, phase controlled, solid-state type, which meets the performance requirements given in Table 5-4. The battery charger shall maintain the battery charge while providing sufficient power to the inverter to provide rated power output to the UPS loads. The charger capacity shall be sufficient to recharge the batteries from a fully discharged state to full capacity within the time prescribed in 5.2-1, while simultaneously maintaining full rated output at the inverter. The dc output voltage shall be chosen to match the battery voltage.

The battery chargers shall be capable of accepting load immediately after an ac power interruption and restoration.

5.3.2 Inverter

The inverter shall be sinusoidal and sized to supply Class II power at constant voltage and frequency at loads up to the maximum steady -state load specified in Table 5-3. The nominal inverter input voltage shall be coordinated with the characteristics of the battery bank.

The internal oscillator shall operate in synchronism with the alternate power source. If the output deviates by more than ± 1.0 Hz and/or ± 15 volts from the alternate power supply, the inverter shall automatically proceed to operate in a free-running mode. Frequency stability while running in this mode shall be as specified in Table 5-3. The inverter shall have provision for automatically re-synchronizing upon restoration of the alternate power supply.

The inverter shall be capable of operating for extended periods of time at very light loads (e.g., 10% full load).

Harmonic distortion shall not exceed the limit specified in Table 5-3. In addition, the output waveform shall not contain any high-frequency spikes or fast slope changes.

The inverter shall be able to handle high crest factor demand of power supplies and the output voltage shall not result in flat-topping, creating a square wave.

The inverter shall be self-starting and capable of accepting loads up to the current limit on restoration of the dc input.

5.3.3 Batteries

The batteries shall have a long service life and shall be rechargeable, sealed and maintenance free. The batteries shall be fully charged when delivered to the project site such that they are capable of maintaining the full load rated UPS output for the time duration specified in 5.2-1, without any output from the charger/rectifier.

The battery containers shall be made from flame retardant material and shall be shock resistant. Inter-cell connectors and cell terminals shall have fully removable boot type insulation covers.

5.3.4 Static Transfer Switch

A solid state 120 V single-phase, two-way, make-before-break, static transfer switch shall be supplied. The static transfer switch shall be capable of automatically or manually transferring the Class II UPS load from the normal to the alternate power source and shall be capable of being transferred back from alternate to normal power source automatically or by manual initiation. These transfers shall be accomplished without any power interruption to Class II UPS.

The static transfer switch shall automatically transfer from the normal power supply to the alternate power supply in the event of:

- Inverter malfunction,
- Failure of dc input to the inverter from the charger/rectifier or the battery, or
- Inverter overload.

For purposes of static transfer switch control, an inverter malfunction is a condition where monitored inverter parameters are not within tolerance limits. Monitored inverter output parameters shall include output voltage and frequency as a minimum.

Provision shall be made to transfer by manual initiation both from normal to alternate power supplies and visa versa. A self-synchronizing feature shall be provided to enable these transfers.

Following an automatic transfer from normal to alternate power source, the static transfer switch shall automatically transfer back from the alternate to normal power source following restoration and stabilization of the inverter output.

5.4 Reliability

High reliability and easy maintainability under all operating conditions are required over the expected 40-year service life of the facility. The mean time between failures (MTBF) and mean time to repair (MTTR) shall be specified by the supplier and this data shall be backed up by adequate and verifiable supporting information. The Supplier shall provide information on the proportion of partial failures, where power continues to be available, but with degraded voltage, frequency or wave shape.

5.5 Maintainability

High reliability with minimum maintenance is required. Workmanship shall be as per QA standard ISO 9001:2000 and adequate for the reliable operation and service life.

5.6 Testability

The Supplier shall define in a test plan, tests and procedures to demonstrate the performance and operation of the systems as defined in the Technical Specifications [5]. The tests shall clearly demonstrate the correct operation of all control, protective, display and alarm devices. The tests shall also verify the ability to carry the specified load for the specified time duration following failure of normal and alternate power supplies.

The design and the routine test for the complete UPS shall be performed after assembly and interconnection of the functional units, in accordance with IEEE standard 944. The rectifier/charger shall be tested in accordance with NEMA PE5.

5.6.1 Battery Charger Tests

The correct operation of all controls, protective and alarm devices shall be verified and include:

- a) One-minute high potential insulation (dielectric) tests
- b) Range of float charge
- c) Range of equalize charge
- d) Operation of float and equalize charge
- e) Rated current at normal float and equalize settings
- f) Current limit at normal float and equalize settings
- g) Under voltage and over voltage alarms and trips
- h) Interruption and restoration of ac input while on load

5.6.2 Battery Tests

The supplier shall perform the battery acceptance tests including the capacity test. In the case of Valve Regulated Lead Acid Battery, the battery shall be tested as per IEEE standard 1188. The supplier shall number each battery and provide the purchaser with impedance of each battery.

5.6.3 Inverter and Transfer Switch Tests

The correct operation of all controls, protection and alarms shall be verified including:

- a) One -minute high potential insulation (dielectric) tests
- b) Waveform analysis
- c) Rated current
- d) Current limit
- e) Under and over voltage and frequency trips
- f) Automatic transfer (loss of inverter output) and reset
- g) Manual transfer and reset
- h) Interruption and restoration of dc power while on load
- i) Inverter output shall be tested to verify conformance to the harmonic distortion limit requirement of <5% THD using a 90% non -linear load.

5.6.4 UPS Test

Each complete unit including batteries shall be tested to verify the unit's ability to carry the specified load for the specified time following failure of the normal power supply.

5.7 Security

There are no security requirements for the UPS system.

5.8 Seismic

The UPS assembly shall be designed and qualified for being able to start, operate and perform as required, during and after being subjected to a design basis earthquake (DBE). This requirement, defined as a Category B DBE, requires that the UPS assembly shall retain its functional operability during and following the earthquake.

The supplier shall demonstrate the seismic qualification ability of the UPS equipment, including batteries, either by analysis, tests, or by a combination of analysis and testing.

The supplier shall submit a written test procedure to the purchaser and obtain acceptance before conducting the tests. The supplier shall state the method of qualification proposed and reasons for the choice. The name of the company doing the testing shall be indicated.

Where seismic tests are required, the supplier shall follow the requirements of CAN3-N289.4.

The supplier shall provide AECL with frequencies of the equipment, the centre of gravity, the equipment mass, and the maximum loads, which connects to other equipment.

Where calculations are required for the seismic qualification, the supplier shall present a step-by-step analysis in accordance with CAN3-N289.3. Seismic stress analysis requires acceptance by the purchaser. The details for seismic qualifications shall be as per technical specifications [5].

5.9 Environmental Tolerance

There are no special environmental qualification requirements associated with the UPS equipment. The UPS will be located in a heated and air conditioned room having a temperature and humidity profile as detailed in 5-7.

Table 5-7
Environmental Requirements of the UPS

Normal Ambient Temperature	20°C ± 5°C
Minimum Temperature	10°C
Maximum Temperature	40°C
Relative humidity	< 95%
Elevation	< 200 m Above Sea Level

5.10 Electromagnetic Immunity/Emissions

The UPS shall conform to electromagnetic compatibility requirements of Reference [5], i.e., conformance with the standard IEC 62040-2:2005 [6], for UPS of product category C3 operating in the second (industrial) environment, as defined in the standard.

The governing standard IEC 62040-2:2005 [6] lists type tests as the only means for demonstrating compliance and includes discussion of the following aspects of testing:

- UPS operating conditions for testing (input voltage, operating modes, output load)
- Conducted and radiated emission limits and equipment ports to be tested,
- Minimum immunity requirements and equipment ports to be tested,
- Acceptable test methods for conducted and radiated emissions and immunity,
- Minimum parameters to monitor during immunity tests and associated performance levels.

Detailed requirements in the above areas applicable to Reactors 1 and 2 UPSs that are derived by the governing standards are listed in compliance tables of Section 7.1.3.

Additional requirements derived from the qualification procedure [3] and guideline [4] are as listed below:

- Where qualification is established based on type testing of UPS equipment that is similar to, but differs from, UPSs in Reactors 1 and 2, this must be justified. Differences between the tested and supplied equipment must be described and evaluated to demonstrate the equipment supplied is expected to have emissions no greater than, and immunity no lesser than, the tested equipment.
- Where testing required by the standard IEC 62040-2:2005 [6] has not been performed, or does not fully meet all requirements of the standard, this shall be documented and the impact on suitability analyzed. In the case this represents a minor gap in the overall test evidence, and alternative evidence is available to provide reasonable assurance of the required levels of emissions and immunity, the UPS may be deemed compliant with electromagnetic compatibility requirements. Where the UPS is determined to be non-compliant, compensating actions must be defined to provide assurance of electromagnetic compatibility of the UPS with its environment.

6. ASPQ APPROACH

The approach and the strategy used in this qualification have been chosen in accordance with the qualification procedure [3]. The qualification methods were selected in accordance with Table A-1, Recommended ASPQ Methods by System Class, of the qualification procedure. Since the Categorization Report [1] identified the UPS as a Class II PES, the methods applicable to the corresponding system class were utilized to ensure that the UPS system met the requirements for the aforementioned system classification, as set in the procedure. These methods are grouped into three categories:

- **Suitability:** to ensure that Gambit UPS modes WEP 1010-110/120-NEA and WEP-1020-110/120-NEA are suitable for use in the intended application, which is to provide the loads with power within acceptable limits on amplitude, frequency and harmonics, as defined in technical specifications [5]
- **Adequacy of Documentation:** to ensure that the Gambit UPS systems are accompanied with sufficient documentation to allow the operators to safely operate the system.
- **Correctness of Design:** to establish enough evidence to ensure that the Gambit UPS systems are correct in design and will perform as required.

Nevertheless, the findings under certain methods may be used in more than just one type of assessment.

6.1 Suitability

For suitability evaluation, the recommended methods as per Guideline [4] are:

- Method 4a: “In-Service Maintenance Process Assessment”
- Method 5b: “Electromagnetic Immunity and Emissions Assessment”
- Method 5c: “Seismic tolerance Assessment”
- Method 5d: “Hardware Reliability, Failure Modes and Diagnostic Assessment”
- Method 5e: “Assessment of Hardware Useful Life”
- Method 9c: “Assessment of 3rd Party Hardware Test Standards Compliance”
- Method 4b: “In Service Testability Assessment”

Also, the methods used in the following section confirm suitability of the device.

6.2 Adequacy of Documentation

The methods used for establishing the adequacy of safety-related documentation as per the qualification procedure [3] are:

- Method 2: “Assessment of Product Specifications (hardware, software, and tools)”
- Method 9a: “Assessment of 3rd Party Corporate Quality System Certification”
- Method 9b: “Assessment of 3rd Party Product Safety Certifications”

6.3 Evidence of Correctness

As per the qualification procedure [3] adequate evidence to prove correctness of design for a programmable electronic system (i.e., UPS) can be established using the following four approaches:

- Compliance to a recognized safety-related industrial standard
- Proven-in-use arguments
- Complimentary testing; or
- Analysis of the detailed design

If the evidence is generally reasonable but deficient in specific areas, supplemental evidence from any of the remaining approaches, or combination of approaches may be used to compensate and provide the requisite confidence in the correctness of the product design.

The methods used for establishing evidence to support correctness of UPS design are:

- Method 3a: "Operating History Data"
- Method 3b: "Failure Data Assessment"
- Method 3c: "Product Design Revision History Assessment"
- Method 3d: "Reference Site Assessments"

7. DETAILED FINDINGS FROM THE ASSESSMENT METHODS

7.1 Suitability Assessment

The safety function of the UPS is to provide the safety-related control and instrumentation power distribution panels with 120V single-phase power, within the voltage, frequency and harmonics limits specified in Section 5.3 of this report. Since the UPS loads are all designed to fail safe in the event of power failure, the only failure of concern is UPS partial failure, where the loads are supplied with “dirty power”. In addition to supply of uninterruptible power, Gambit UPS systems WEP 1010-110-/120-NEA and WEP 1020-110-/120-NEA are designed to protect the loads against grid disturbances such as voltage, frequency and harmonics fluctuations so that the sensitive loads are not adversely affected. From suitability perspective, it is needed to demonstrate that the choice of UPS is appropriate for the intended application.

7.1.1 Method 4a: “In-Service Maintenance Process Assessment”

The maintenance of the UPS system consists of two parts:

- Maintenance of the hardware; and
- Maintenance of battery pack

There are a number of recommended monthly checks that are to be performed on both the hardware and the battery pack. In addition to monthly tests, the hardware and the battery pack are to be tested annually and semi-annually, respectively [12]. The annual and semi-annual tests are similar to the monthly checks except that they cover more inspections.

Hardware and battery-pack monthly checks are simple and are explained in details in Maintenance Manual. These tests do not require the UPS to be in a configuration such that UPS’s safety function is jeopardized. During maintenance, the UPS mode of operation is manually changed to Bypass where the loads are directly powered via the alternate source of supply. Although this mode of operation restrains the ability of the UPS to supply uninterruptible power, as the loads are directly connected to the alternate Class III bus, this is not a safety concern since the loads are all designed to fail safe in the event of power interruption.

As per Gambit, there are no expected firmware upgrades anticipated for the UPS system, as firmware package 2 is capable of meeting all the requirements set in the technical specification. It was concluded that the difficulty and frequency of the recommended maintenance on the UPS system is acceptable. In addition, from suitability perspective, the in-service maintenance process of the UPS system, including the battery bank, was satisfactory.

7.1.2 Method 5a: “Environmental Tolerance Assessment”

This method assesses the ability of the PES to withstand the worse case in-service operating conditions required over its in-service life and includes: temperature, humidity, shock and vibration, radiation and air-bourn particulates.

The purchased UPS systems will be placed in a heated and air-conditioned room, with temperature and humidity profile of $20^{\circ}\text{C} \pm 5^{\circ}\text{C}$ and $<95\%$, respectively. The ambient temperature range for operating environment of UPS is from -10°C to $+40^{\circ}\text{C}$ with humidity profile of $<95\%$ non-condensing. The UPS will not be exposed to any shock or vibration, as it will be firmly anchored to the floor. For both R1 and R2 reactors, UPS 1 and UPS 2 will be located in rooms 014 and 105, respectively. These rooms are part of Radiological Zone 2, which is normally free of radioactivity, but may be subject to infrequent cross-contamination from higher zones [24]. In addition, there are no air-bourn particulates presents in the room. However, the fans inside the purchased Gambit UPS systems come with “n+1” redundancy and are monitored by the system against failure. In the event that any of the fans stops working due to reasons such as over-time accumulation of air-borne particulates, alarms will be generated.

It was concluded that from suitability perspective, environmental tolerance of the purchased Gambit UPS systems met the applicable requirements.

7.1.3 Method 5b: “Electromagnetic Immunity and Emissions Assessment”

Compliance with electromagnetic emissions and immunity requirements discussed in Section 5.10 of this report is assessed. For the assessment, detailed requirements in regard to emission limits, minimum immunity levels and testing methods applicable to UPS 1 and UPS 2 in Reactors 1 and 2 were extracted from the governing standard [6]. The detailed requirements are listed in the left-most major column in compliance tables below. The assessed level of compliance and reference to supporting information are provided for each requirement in the right-most column.

Compliance with immunity and emissions requirements is assessed on the basis of References [7] and [8] provided by Gambit Electronic Ltd. Reference [8] is a report prepared by Montena EMC SA for Gambit on EMC (emissions and immunity) testing of Gambit product AIS 5000, which is similar to Gambit UPS type WEP 1010-110/120 NEA and WEP 1020-110/120 NEA supplied for R1 and 2 UPS 1 and UPS 2, respectively. Section 2 of Reference [7] highlights and evaluates the differences between the tested and supplied Gambit products. The detail provided on pages 1 and 2 of the aforementioned report is sufficient to support the Gambit conclusion that EMC characteristics of the tested system are representative of the EMC performance of Gambit UPS type WEP 1020-110/120 NEA supplied for R1 and 2 UPS 1. This conclusion is equally applicable to Gambit UPS type WEP 1010-110/120 NEA supplied for R1 and 2 UPS 2 as it is of like type and lower capacity.

Montena EMC SA is accredited by the Swiss Federal Office of Metrology and Accreditation (accreditation number STS 024) as a testing laboratory for EMC, electrical safety and telecommunication in accordance with the standard ISO/IEC 17025 [9] for the competence of testing and calibration laboratories. Montena was contracted by Gambit to perform EMC compliance testing in accordance with the standard IEC 62040-2:2005 (and other standards) over the period 2006 August 7 to 9 and on 2006 December 6. No AECL personnel witnessed the tests as testing was not conducted in connection with any AECL procurement.

References [7] and [8] together provide a basis for conclusion that UPS 1 and UPS 2 comply with emission limits. These documents also provide a basis for conclusion that UPS 1 and UPS 2 comply with immunity requirements, except that the following required tests appear to have been omitted:

1. Test of AC Bypass Mains input for immunity to high-frequency disturbances (fast transient burst, surge, and conducted common-mode disturbances induced by radio-frequency fields), as specified in IEC 62040-2:2005, Clause 7.3.3, Table 6;
2. Test of AC input power port, i.e., AC Mains input and AC Bypass Mains input, for immunity to power line harmonics and inter-harmonics, and phase unbalance, as specified in IEC 62040-2:2005, Clause 7.4 and Annex D.6; and
3. Test of signal and control ports, i.e., alarm relay connections, for immunity to fast transient burst and conducted common-mode disturbances induced by radio-frequency fields, as specified in IEC 62040-2:2005, Clause 7.3.3, Table 6.

In regard to item 1 above, the test report states the AC Bypass Mains input was not tested, as it is not connected to internal circuitry [8]. When asked to explain this statement, Gambit responded that the bypass circuit is always energized at least up to the Bypass switch EN, and there is a connection to internal UPS control circuitry via the Bypass VQ circuit. However, this connection is made in the same manner (using the same type isolation transformer) as the connection of the AC Mains input to the Mains VQ circuit. Further, the Mains VQ and Bypass VQ microprocessors are both located on the main controller board, together with the Masterlogic, MPU and DMU (Figure 3-1), so that the coupling paths for high-frequency disturbances at the AC Mains and AC Bypass Mains to UPS control circuits are similar. Therefore, successful testing of the AC Mains input shows there would be no impact from high-frequency disturbances at the Bypass Mains as well [16]. This supplementary information provides reasonable assurance that the AC Bypass Mains input complies with requirements for immunity to high-frequency disturbances despite the lack of direct test results. The UPS is considered compliant and no compensating actions are required.

In regard to item 2 above, the required tests are new with the 2005 version of the standard. Montena EMC SA was not able to perform the tests, as they did not have the specialized test generator required at the time of testing. It is recommended the lack of test evidence be compensated through the following measures:

- During UPS commissioning, the level of harmonics generation at the AC Mains and AC Bypass Mains inputs should be measured and proper functioning of UPS control circuits confirmed. This will demonstrate immunity at the measured level of harmonics. However, in the absence of harmonics immunity test data, the immunity margin will be unknown.
- During UPS operation, the level of harmonics should be measured at regular intervals defined in the Maintenance Program, so that any increase in harmonics will become apparent.
- Should a rise in harmonics level be detected, corrective measures should be considered.
- Modifications to the electrical system should be designed to minimize any increase in harmonics generation at the AC Mains and AC Bypass Mains inputs.

In regard to item 3 above, alarm relay contacts are not sensitive to continuous or transient conducted disturbances at energy levels involved in the tests. Thus, the lack of testing has no impact, and no compensating measures are required.

Table 7-1
Assessment of UPS Compliance with IEC 62020-2:2005 with Respect to Emissions

Requirements from IEC 62040-2:2005 ¹			Clause	Compliance Assessment & Basis
Aspect	Details			
UPS operating conditions and modes for emissions tests	Input AC voltage: Operating modes: Load:	Rated voltage Normal, emergency Linear load ²	6.2, 6.3	Compliant (Reference [8], Section 5.6)
Documentation of special measures to achieve compliance with emissions limits	Documentation to be provided to purchaser/user		6.3.2	Compliant (Reference [8], Section 4.5 and Reference [7], Section 2, which identifies measures required for category C3)
Limits of conducted emissions at AC input terminals (Mains and Bypass terminals)	Frequency (MHz)	Limit ³ (dBµV) Quasi-peak detector Average detector	6.4.1 Table 2 (<100A, UPS 2; most restrictive requirement)	Compliant (Reference [8], Section 6.1, p15-21)
	0.15 – 0.50	100	90	
	0.50 – 5.0	86	76	
	5.0 – 30.0	90 – 70	80 – 60	
Limits of conducted emissions at AC output terminals	Limits are 14 dB higher than for AC input terminals immediately above		6.4.2 Table 2 (<100A)	Compliant (Reference [8], Section 6.2, p22-30)
Limits of conducted emissions at signal and telecommunication ports	No requirement applicable to UPS 1 or UPS 2		6.4.3	Not applicable
Limits of conducted emissions at DC power ports	No requirement applicable to UPS 1 or UPS 2 as the DC power port is an internal port		6.4.4	Not applicable
Limits of low-frequency conducted emissions (input current harmonics)	No requirement applicable to UPS 1 or UPS 2 (Limits apply to UPS of rated output current ≤16 A only)		6.4.5	Not applicable
Limits of radiated electromagnetic field emissions	Frequency (MHz)	Limit ⁴ (dBµV/m)	6.5.1 Table 3	Compliant (Reference [8], Section 6.3, p31-35)
	30 – 230	130		
	230 – 1,000	125		
Limits of magnetic field emissions	No limits are specified		6.5.2	Not applicable

Note 1: Requirements listed are applicable to UPS of product category C3 operating in the second environment and are applicable to UPS 1 and UPS 2 in Reactors 1 and 2.

Note 2: Load is within the UPS rating and results in the highest emission level, as determined in prior testing.

Note 3: The lower emission limit applies at a transition frequency. Where a range is listed, the emission limit decreases linearly with the logarithm of frequency.

Note 4: Limits are applicable for tests using a quasi-peak detector and test distance of 10 m.

Table 7-2
Assessment of UPS Compliance with IEC 62040-2:2005 with Respect to Immunity

Requirements from IEC 62040-2:2005 ¹				Compliance Assessment & Basis
Aspect	Details		Clause	
UPS operating conditions and modes for immunity tests	Input AC voltage: Operating modes: Load:	Rated voltage Normal Linear load ¹	7.2	Compliant (Reference [8], Section 5.6)
Performance criteria	UPS output voltage variation: UPS mode of operation: Control signals to external devices: Panel indications:	Within ±10 % No change ² No change ² May change only during test	7.2	Compliant (Reference [8], Sections 5.7, 5.8, 5.9s)
Immunity of the enclosure port to high-frequency disturbances	Phenomenon	Test method	7.3.3 Table 6	Compliant (Reference [8], Section 7.1 (ESD), p. 37, 38; Section 7.2 (RFI), p. 39, 40)
	Electrostatic discharge (ESD)	IEC 61000-4-2		
	Radio-frequency electromagnetic field	IEC 61000-4-3 10 V/m 80 – 1000 MHz 80% amplitude modulation (1 kHz)		
Immunity of AC input and output power ports to high-frequency disturbances	Phenomenon	Test method	7.3.3 Table 6	Compliant with respect to AC Mains input and AC output. (Reference [8], Section 7.3, p. 41, 42 (fast transients), Section 7.4, p. 43 – 45 (surge); Section 7.5, p. 46, 47 (conducted common-mode radio-frequency disturbances)) Non-compliant with respect to AC Bypass Mains input. Reference [8] states the Bypass input was not tested as it is not connected to internal circuitry [8].
	Fast transient burst	IEC 61000-4-4		
	Surge (1.2/50 – 8/20 µs)	IEC 61000-4-5 1 kV line-line 2 kV line-earth		
	Conducted common mode disturbances induced by radio-frequency fields	IEC 61000-4-6 10 V _{rms} 0.15 – 0.80 MHz 80% amplitude modulation (1 kHz)		

Note 1: Requirements listed are applicable to UPS of product category C3 operating in the second environment and are applicable to UPS 1 and UPS 2 in Reactors 1 and 2.

Note 2: Change during test is allowed in IEC 62040-2:2005 for certain tests, but was not allowed in testing reported in Reference [8].

Requirements from IEC 62040-2:2005 ¹					Compliance Assessment & Basis
Aspect	Details			Clause	
	Phenomenon	Test method	Test level		
Immunity of DC power port to high-frequency disturbances	Fast transient burst	IEC 61000-4-4	2 kV / 5 kHz using capacitive clamp	7.3.3 Table 6	Compliant (Reference [8], Section 7.3, p. 41, 42)
	Phenomenon	Test method	Test level		
Immunity of signal and control ports to high-frequency disturbances	Fast transient burst	IEC 61000-4-4	1 kV / 5 kHz using capacitive clamp	7.3.3 Table 6	Not compliant The UPS signal and control ports include alarm relay connections that were not tested.
	Conducted common mode disturbances induced by radio-frequency fields	IEC 61000-4-6	3 V _{rms} 0.15 0 80 MHz 80% amplitude modulation (1 kHz)		
	Phenomenon	Test method	Test level		
Immunity of AC input power port to low-frequency conducted disturbances	Power line harmonics and inter-harmonics	IEC 61040-2:2005, Annex D.6.1	10 V _{rms} 140 – 360 Hz	7.4, Annex D.6	Not compliant Neither the AC Mains nor Bypass inputs were tested
	Amplitude and phase unbalance (3-phase input only)	IEC 61040-2:2005, Annex D.6.2	5 V _{rms}		
	Phenomenon	Test method	Test level		
Immunity of the enclosure port to power-frequency magnetic field disturbances	Power-frequency magnetic field	IEC 61040-8	30 A/m	7.5	Compliant (Reference [8], Section 7.6, p. 48, 49. Testing was conducted at a power frequency of 50 Hz.)
	Phenomenon	Test method	Test level		
Immunity to voltage dips, short interruptions and voltage variations	Requirements are covered under functional qualification. There are no specific requirements from IEC 62040-2:2005.			7.6	Not applicable

Note 1: Requirements listed are applicable to UPS of product category C3 operating in the second environment and are applicable to UPS 1 and UPS 2 in Reactors 1 and 2.

7.1.4 Method 5c: “Seismic Tolerance Assessment”

In order to demonstrate seismic tolerance of the purchased UPS systems, Gambit made use of the test results of a similar UPS model (WEP 1020-220/230), which was seismically tested for another client. The tests were performed in Munich by IABG on a UPS system with similar dimensions, which weighed more than those purchased by AECL. The seismic qualification report of the tested unit was submitted by Gambit to AECL and was reviewed by the seismic group. The seismic test response spectra (TRS) of the tested unit was observed to be much more stringent than the specified required spectra (SRS) as indicated in the technical specification. [26] [27] However, some of the components in the tested unit were not the same as those in the purchased UPS systems. Consequently, these components were identified and tested by a third party (Wolfel) in accordance with the same standard used for the main UPS systems.

For batteries, seismic qualification was carried out at AECL by performing detailed engineering calculations. [21] The battery cabinets were deemed to be also seismically qualified due to the construction of their structure which was the same as the UPS cabinets that have already been seismically qualified. [26]

7.1.5 Method 5d: “Hardware Reliability, Failure Modes and Diagnostic Assessment”

Since no FMEA document was available from Gambit, the failure and the associated effects of various components of the UPS were examined in details in Section 4 of this report. The safety function of the UPS is only to provide within-specification power, thus, the only failure of concern is combination of inverter and VQ-Output failure such that “dirty power” is outputted undetected. It should be noted that the failures of these components do not necessarily need to occur simultaneously, as an undetected VQ-Output failure followed by an inverter failure can jeopardize the safety function of the UPS just as well.

As per the categorization report [1], the effect of such failure on safety related loads such as SL1 and SL2 maybe such that trip relays may fail to de-energize and open trip contacts, when the measured parameter exceeds the required setpoint. Thus, load system alarms and mitigating features may not operate as required.

The UPS system conducts multiple self-checks, and in the event of a detected failure, alarm(s) is generated. Below is a list of alarms that can be shown on the UPS display system.

- | | | | |
|-----|---------------------------------------|-----|--|
| 0. | OFF button pushed | 30. | <i>Spare</i> |
| 1. | ON button pushed | 31. | High temp Charger magnetic |
| 2. | FATAL ERR.RAM1 data | 32. | High temp Invert. magnetic |
| 3. | FATAL ERR.RAM1 timeout | 33. | High battery temperature |
| 4. | System set in manual BYPASS | 34. | Inverter voltage error |
| 5. | TSM 1 temp warning | 35. | Inverter fuse blown |
| 6. | TSM 1 temp shutdown | 36. | Low DC warning |
| 7. | TSM 2 temp warning | 37. | Low DC shutdown |
| 8. | TSM 2 temp shutdown | 38. | DC current limit |
| 9. | TSM 3 temp warning | 39. | Mains frequency out of tolerance |
| 10. | TSM 3 temp shutdown | 40. | Mains instantaneous out of tolerance |
| 11. | Battery monitor alarm | 41. | Mains is out of tolerance |
| 12. | Battery symmetry error | 42. | Output frequency out of tolerance |
| 13. | Battery grounding error | 43. | Output instantaneous out of tolerance |
| 14. | Battery monitor warning | 44. | Output is out of tolerance |
| 15. | Battery MCB OFF | 45. | <i>Output switch open (only AIS)</i> |
| 16. | Bypass freq out of tolerance | 46. | <i>Spare</i> |
| 17. | Bypass instantaneous out of tolerance | 47. | SSW2 EN2temp shutdown |
| 18. | Bypass is out of tolerance | 48. | SSW2 EN2temp temp warning |
| 19. | <i>Spare</i> | 49. | SSW2 EN3temp temp shutdown |
| 20. | Charger 0 temp warning | 50. | SSW2 EN3temp temp warning |
| 21. | Charger 0 temp shutdown | 51. | Synchronization error |
| 22. | Charger 30 temp warning | 52. | System lock in operation mode |
| 23. | Charger 30 temp shutdown | 53. | <i>Spare</i> |
| 24. | Current limiter active | 54. | Fan fault |
| 25. | OVERLOAD load is > 100% | 55. | Fault in int power supply |
| 26. | High DC warning | 56. | <i>Rectifier fuse blown (only AIS)</i> |
| 27. | High DC shutdown | 57. | Aux 1 error |
| 28. | High output voltage | 58. | Calibration stack entered |
| 29. | <i>Spare</i> | 59. | <i>Spare</i> |

“UPS Trouble” alarm is generated when any of above alarm conditions are detected by the UPS system. As shown in Table 7-3, the operators of R1/2 reactors are notified of UPS faults and mode of operation via various annunciation windows in the Main Control Room.

Table 7-3
UPS 1/2 Main Control Room Alarm Descriptions

UPS #	Alarm Description	Annunciation Window #
UPS 1	UPS 1 TROUBLE	UPS 1586
	UPS ON BATTERY	UPS 1586
	UPS ON BY PASS	UPS 1586
UPS2	UPS 2 TROUBLE	UPS 1589
	UPS 2 ON BATTERY	UPS 1590
	UPS 2 ON BY PASS	UPS 1591

As per Section 2.7.3 of Reference [11] the following two alarms are generated when VQ-Output fails:

- Output frequency out of tolerance; and
- Output instantaneous out of tolerance

It is noteworthy that above alarms correspond to alarm numbers 42 and 43 of above list. These alarms cause the “Common Alarm LED”, placed above the foil keyboard of the UPS, to be illuminated. An acoustic alarm is also activated and the nature of the alarm is logged and time-stamped by the UPS (up to 250 events). In addition, the operator is immediately notified of UPS trouble and corrective action will be initiated.

Via performing the recommended component replacement program and monthly power quality testing [12], the chances of UPS partial failure is controlled at an acceptably low level such that the reliability requirements associated with a Category B PES is met (Section 7.3.2 of this report). It must be noted that VQ-Output is a highly reliable hardware, as Gambit has never encountered a reported case of its failure. [16]

The initial reliability data provided by Gambit was based on UPS systems with WXX firmware package 2 sold between 10 JAN 2003 and 31 DEC 2004. During this period, a total of 480 units were sold for which zero fatal software or firmware failures were reported. [13]. It is noteworthy that a fatal error is defined by Gambit as a failure that the output of the UPS is interrupted. However, during the site visit to Gambit head quarters in Country-X, an up-to-date copy of hardware reliability data was obtained. Table 7-4 summarizes the findings:

Table 7-4
Gambit UPS Sales / Failure Data As of August 2007

Year	WEP Units Sold	PWX Units Sold	Reported Failures
2004	609	190	3
2005	692	192	1
2006	1179	466	1

The sales data for WXP UPSs are applicable to support hardware reliability of purchased UPS systems, as they have the same hardware configuration and use the same components as WEP family of UPS systems. [16]

As suggested by the Guideline [4] Gambit was asked if they were aware of any software/hardware bugs that existed in the system and whether any software patches were anticipated. Gambit’s response was negative. After reviewing the product documentations and modes of operation, no unacceptable failure modes or dangerous configuration of the UPS system were identified.

In conclusion, it can be said that the purchased Gambit UPS systems are highly reliable. Also, the possibility of double failure of VQ-Output and inverter, considering high reliability of these components in conjunction with performance of recommended frequent testing, and component replacement program, is very low. Section 7.3.2 and 7.3.3 of this report numerically demonstrate reliability of UPSs and their conformance to IEC 60880.

7.1.6 Method 5e: “Assessment of Hardware Useful Life”

This method is of particular interest where in-service replacement, testability, environmental conditions or product age-related degradation mechanisms are a concern. There are no environmental requirements associated with the UPS system as it will be located in a heated and air-conditioned area having a temperature and humidity profile of a normal room. [5]

The service life of the UPS was stated as 40 years in the technical specification [5]. In the bid, Gambit stated that the 40-year life of the UPS system is achievable via performing the recommended component replacement program. In addition, as stated in the bid, Gambit is committed to maintain an inventory of parts and components in case some components and modules become obsolete or replaced with a new design. Also, Gambit provided AECL with a list of recommended spare parts, which will be delivered to Location-X along with the units.

The UPS components with limited lifetimes and their respective replacement frequencies are identified in the table below:

**Table 7-5
UPS Component Replacement Frequency**

UPS Module	Fan	Battery	Backup RAM	DC Capacitor Module	AC Capacitor Module
Replacement Frequency	5 years	20 years	10 years	9 years	9 years

As one of the recommendations made by this report, above components will be added to the station’s preventive maintenance program to ensure high reliability of the UPS systems.

The MTBF and MTTR of the UPS system were calculated by Gambit as 75 years and 4 hours, respectively. As stated by Gambit in the bid, the calculations were made on basis of field experience by Gambit Service Department and customers’ feedback, and are only applicable to UPS systems that were sustained as per manufacturer’s maintenance- and component replacement programs and were operated in non-harsh environmental conditions. The MTBF calculation of the purchased UPS systems is provided in Appendix A.8, and was performed by Gambit. Equation 7-1 demonstrates the relationship between various parameters and MTBF of the whole UPS system.

$$MTBF_{SYSTEM} = \frac{1}{((\lambda_{Mains+EN} \cdot MTTR_{Mains+EN})(\lambda_{UPS} \cdot MTTR_{UPS})(\frac{1}{MTTR_{Mains+EN}} + \frac{1}{MTTR_{UPS}})) + \lambda_C + \lambda_F}$$

Equation 7-1

Description of above parameters and the associated MTBF figures are tabulated in Table 7-6.

Table 7-6
MTBF Values of Various Components of Gambit UPS

Symbol	Description	MTBF (h)
λ_{GR}	Charger Failure Rate	100,000
λ_{BAT}	Battery Failure Rate	100,000
λ_{INV}	Inverter Failure Rate	80,000
λ_{MAINS}	Mains Failure Rate	Depends on Site
λ_{EN}	Static Transfer Switch (EN) Failure Rate	500,000
λ_C	Safebus Failure Rate	5,000,000
λ_F	Feeder Failure Rate ¹	1305483

As shown in Equation 7-1, MTBF of the whole system is function of $\lambda_{Mains+EN}$, which itself is a function of unavailability rate of incoming grid (i.e., MTBF_{MAINS}). In other words, the mean time between failures of a UPS such that output power is lost, is directly proportional to frequency of outages in the grid that supplies the UPS. In order to calculate the MTBF of the UPS systems, the frequency of grid failure at Location-X was conservatively assumed to be one every 1000 hours with MTTR of 0.1 hour. Using these figures, the MTBF of the UPS system was calculated as 43 years [Appendix A.8].

It can be concluded that from suitability perspective the Gambit UPS systems' hardware useful life met the requirements associated with the intended application, as long as the component replacement program is undertaken by the station at maximum frequencies noted in Table 7-3. Also, from documentation perspective, the recommended component replacement program is clearly identified.

7.1.7 Method 9c: "Assessment of 3rd Party Hardware Test Standards Compliance"

Compliance of the UPS with EMC requirements is assessed through demonstrated compliance with the 3rd party hardware test standard IEC 62040-2:2005 [6], which is the international standard governing EMC requirements for UPS systems. This standard specifies the applicable test levels and acceptance criteria, and references standards in the series IEC 61000-4 for details of the test method (Specific standards referenced are listed in compliance tables provided in Section 7.1.3. The EMC test report submitted by Gambit [8] is compliant with IEC 62040-2:2005 [6] and the above standards governing the test method. Thus, compliance with EMC requirements is established on the basis of compliance with 3rd party hardware test standards. See Section 7.1.3 for details of compliance assessment and a listing of gaps in the qualification evidence.

¹ "Feeder Failure Rate" implies the failure rate associated with Bypass switch Q050 and output breaker Q100.

Compliance of the UPS and batteries with seismic requirements is assessed through demonstrated conformity with the technical specification [5]. The suppliers tested an equivalent UPS system in the past in accordance with test standards DIN 40046 and DIN IEC 68, which are equivalent to IEC 68-2-6. The test was more stringent as the loading more severe than the requirements of the technical specification. [5] Seismic conformity of the batteries to CAN3-N289.3 standard was demonstrated via detailed calculations. [21]

7.1.8 Method 4b: “In-Service Testability Assessment”

Table 7-7, summarizes the testability requirements of the Gambit UPS systems as specified in various section of the TS [5].

**Table 7-7
Conformance of Gambit UPS Systems to Testability Requirement**

Item	Description	Compliance
1	UPS shall be provided with bus terminal connections, via a fused disconnect switch to test and external load bank.	Yes
2	Testing shall be carried out after transferring the Class II load bus to the alternate power supply by closing the maintenance bypass switch without power interruption at the Class bus.	Yes
3	Test point shall be provided on battery for adjustment and fault diagnosis.	No
4	Test point shall be provided on inverter for adjustment and fault diagnosis.	No
5	A switch or pushbutton shall be provided to test the static transfer switch from alternate supply to inverter and vice-versa.	No

With respect to items 3 and 4, although there are no physical test points available on battery and inverter for fault diagnosis and adjustments, the requirements are met as these activities can be done directly via the GUI on the front panel. Similarly, for item 5 the test can be conducted via the GUI. Thus, the non-compliances noted for items 3, 4 and 5 were accepted.

7.2 Documentation for Safety

7.2.1 Method 2: “Assessment of Product Specifications”

The data from the product specification were assessed to determine adequacy of UPS documentation in order to allow for safe operation of the UPS.

Multiple documents were provided by Gambit as part of the purchased UPS system and consisted of:

1. General Information of UPS System
2. General System Principle & Description of Components
3. User Manual – Mod-Bus Converter for WEP/DWP & EWW/DWW UPS Systems
4. Installation Manual

5. Operating & Indicating Elements
6. Display & Parameter Settings
7. Packing and Unpacking Manual for Air/ Overseas Transportation
8. Transport of the System without Packing
9. Description of Single/Three Phase Voltage Stabilizer
10. Communication Interface for WEP/DWP UPS Systems
11. UPS Troubleshooting Manual for WXP Systems
12. Start, Switch Over and Stop Instruction Manual
13. Black Start Instruction Manual
14. Safety Regulations
15. Replacement Program of Components & Parts
16. Technical Data of UPS System
17. Qualification of WXX Firmware Package 2 According to IEC 60880
18. Reliability & Operating Experience of Gambit Rectifier, Inverter & UPS Systems According to IEC 60880
19. Common Cause Failure Analysis of Gambit WXX Firmware According to IEC 60880-2
20. Export of AUFSYS
21. Export of IQ-Soft
22. Performance Test Procedure
23. Performance Test Analysis
24. Harmonic Analysis Report
25. Battery Capacity Test Report
26. Seismic Qualification Test Report
27. Bill of Materials
28. Inspection and Test Plan
29. Operation and Maintenance Manual
30. TUV Nord Evaluation Report for Gambit WXX Firmware and SDC Firmware
31. Evidence of Technical Resistance Technical Report
32. Montena Electromagnetic Compatibility Test Report of AIS500
33. Montena Electromagnetic Compatibility Test Report for WEP 1020-110/230-NEA
34. Factory Acceptance Test Report
35. Operation and Maintenance Manual [20]

Above documentation provided sufficient information to support safe operation of the UPS system. Item number 17 is a 100-page document, which provides description on the hardware and software components of the UPS system. Common Cause Failures associated with UPS system were examined at both system level and firmware level in item number 19. Firmware revision analysis, and reported failures were examined in Item #18.

It was concluded that the product specifications were clearly defined in the accompanied documentation.

7.2.2 Method 9a: “Assessment of 3rd Party Corporate Quality System Certification”

Gambit has been an ISO 9001:2000 certificate holder since 16 SEP 1994, which ensures high quality of workmanship. The management system of Gambit was assessed by Bureau Veritas Quality International (BVQI) in 27 APR 2005 in the areas of development, sales, design, manufacture, commissioning, maintenance and repair, and was found compliant to ISO 9001:2000. This certificate is valid until 27 APR 2008. [Appendix A.6]

In addition, Gambit was audited by CANPAC in April 2007 and was assessed to conform to the requirements of CSA Z299.2 [Appendix A.6]

7.2.3 Method 9b: “Assessment of 3rd Party Product Safety Certification”

Gambit UPS system is qualified to numerous international standards. Below is a list of such standards that Gambit UPS conforms to:



General UPS standards		Keywords
IEC 62040-1		Generals and Safety
IEC 62040-2		EMC
IEC 62040-3		Testing and Performance
IEC 60950-1		ITE Safety
IEC 60146-1		Semiconductor converters
IEC 60146-2		Inverters
IEC 60439		Switchgear Assemblies
Nuclear Power Plant specific IEC standards		
IEC 60780		Electric equipment, Qualification
IEC 60880		Software for computers
IEC 60980		Seismic qualification
IEC 61225		Electrical Supplies for Safety



General UPS IEEE standards		
IEEE 944		Application and Type Testing
Nuclear Power Plant specific IEEE standards		
IEEE 323		TE Equipment, Qualification
IEEE 344		Seismic Qualification
IEEE 650		Chargers and Inverters, Qualification



General UPS NEMA standards		
PE 1		Generals and Performance Testing
PE 5		Battery Chargers



General UPS UL standards		
UL 1778		Safety



Nuclear Power Plant GOST standards		
PNAE G-9-027-91		Design, Emergency Power Systems
PNAE G-5-006-87		Design, Seismic Resistance

Conformance of Gambit UPS WXX firmware package 2 to IEC 60880-2 was evaluated by TUV Nord in 2004. Based on the data provided by Gambit at time of certification, TUV assessed that the aforementioned firmware conformed to System Integrity Level 2 (SIL-2) as per IEC 61508 [14]. It is noteworthy that safety integrity level SIL-2 designation means that the PES is capable of performing functions up to Category B [3], which is the function categorization associated with the UPS system [1].

The evaluation was done based on assessing the WXX firmware package 2 against the following criteria:

- Sufficiency of documentation
- Functional safety management
- Common Cause Failure
- Qualification as a pre-developed software according to IEC 61508-3

After reviewing the TUV Nord Evaluation Report, no unacceptable limitations of the firmware were identified. It should also be noted that the application of the WXX firmware package 2 is within the bounds of the certification and thus no additional testing is required.

During the site visit to Gambit, it was realized that the actual firmware used in the UPS systems was WXX firmware package 2.2. Gambit clarified that the source code of package 2.2 is identical to that of package 2, which was certified by TUV Nord. The only difference between the two revisions is that in package 2.2 the compiler is initiated with a parameter as for package 2 no parameter is used for initialization. [23]

As discussed in Section 7.1.6 of this report, Gambit UPS system was certified by Montena EMC CA to meet the requirements of IEC 62040-2 for electromagnetic compatibility. [8]

Gambit UPS system was certified by IABG and Wolfel to meet the requirements of seismic test standards DIN 40046 and DIN IEC 68. [26]

A declaration of conformity was supplied by Gambit and is enclosed in Appendix A.5. The declaration states that Gambit designed, manufactured and tested the supplied UPS systems in accordance with the international and Canadian standards listed in below.

Table 7-8
List of Canadian and International Standards Conformed by Gambit UPS Systems

Standard	Description
CSA C22.2 No. 107.3	Uninterruptible Power Systems
CSA 60950-1	Information Technology Equipment-Safety
CSA C22.2 No. 66	Specialty Transformers
IEC 60076	Power Transformers
C22.1	Canadian Electrical Code, Part 1

It was concluded that the 3rd party product certifications and declaration of conformity that accompanied the UPS system, provided sufficient evidence from suitability, documentation and correctness of design perspectives to support the safe use and operation of supplied UPS systems in Reactors 1 and 2.

7.3 Evidence of Correctness

Proven-in-use arguments are evidences that the in-service operational history provides adequate confidence that there are no unknown systematic faults, and the random hardware failure rate is acceptably low. This method is appropriate because the UPS system has a defined and restricted functionality, and there is adequately documented evidence of usage history in similar applications, during which time failures have been reported.

The following product information is relevant in this context:

- Product unit sales data and operating history, number of units in the field;
- Data on failures in the field;
- Failure modes and effects information for the UPS system.

Section 6.3.1 of the Qualification Guide [5], entitled “Proven-In-Use Assessment”, requires a certain minimum number of operating hours for the UPS, based on sales data, an assumption of

percentage of in-service units, and a subjective “software complexity level”, itself a function of lines of code in the firmware, interface complexity, and number of internal modules within the UPS.

Using the aforementioned parameters, Table 7-9 is used to establish one of the four levels of software complexity. When the evaluated parameters fall into different levels of complexity, the highest is selected. As per the information provided by the manufacturer, there are about 26,650 lines of code used in WXX firmware package 2. Using the directions provided by the Guide, the interface complexity index was calculated to be 12. A copy of the calculation is enclosed in Appendix A.1. It was estimated that the range of number of internal modules in the UPS system is between 20 to 200. Consequently, as illustrated in Table 7-9, the software complexity level of WXX firmware package 2 was determined to be “High”.

Table 7-9
Software Complexity

Level of Complexity	Lines of Code	Interface Complexity Index (ICI)	Internal Modules	Other Considerations
Low	<1000	<5	<20	Low
Medium	1000 – 10,000	5 – 9	20 – 200	Medium
High	<u>10,000 – 100,000</u>	<u>10 – 30</u>	<u>200 – 2000</u>	High
Very High	>100,000	>30	>2000	Very High

As shown below in Table 7-10, as prescribed by the qualification Procedure [3], for a Class 2 system, with high level of software complexity, a minimum of 10 million operating hours need to be demonstrated in order to make use of Proven-In-Use argument.

Table 7-10
Minimum Unit-Hours of Operation for Various Classes and Complexity Levels

Class	Minimum Operating Hours (in millions) Required to Claim Proven-in-Use			
	Low Complexity	Medium Complexity	High Complexity	Very High Complexity
1	5	10	20	Not Recommended
2	2	5	<u>10</u>	20
3	1	2	5	10

Below, methods 3c, 3a, 3b and 3d are used to establish evidences to support correctness of design for Gambit UPS systems WEP-1010-110/120-NEA and WEP-1020-110/120-NEA.

7.3.1 Method 3c: “Product Design Revision History Assessment”

This method involves reviewing the scope and safety significance of the changes that were made between successive versions of the product to determine if/whether any credit can be taken for the operating history of previous versions of the UPS systems. As directed in the Guideline [4], in order to take credit for the operating history of previous versions, all changes to the design must be clearly identified and the impact of each change must be assessed.

Table 7-11 below, summarizes the firmware revisions history and release dates associated with packages 0, 1, 2 and 3. Several improvements were implemented during the life cycle of WXX firmware package 2. The firmware used in the UPS prior to Package 0 was not monitored by Gambit and therefore is not listed in the table below.

**Table 7-11
UPS WXX Firmware Revision History**

Package	Release Date	Main Processor Unit	Voltage Quality	Display Measuring Unit	Master Logic Part 1	Master Logic Part 2	Address Decoding	RAR1 Language	Signaling Controller	Display Unit
0	29.12.98	REV01 29.12.98	REV02 24.01.95 REV03 25.10.96	REV02 01.07.97	REV01 18.05.92	REV01 28.04.94	REV01 18.01.95	REV03 29.12.98	REV01 30.05.95	REV04 11.10.99
1	27.03.03	REV02 27.03.03	REV05 11.03.03	REV02 01.07.97	REV01 18.05.92	REV02 19.03.03	REV01 18.01.95	REV03 29.12.98	REV02 26.02.02	REV04 11.10.99
2	23.07.03	REV04 11.03.03	REV05 11.03.03	REV02 01.07.97	REV01 18.05.92	REV02 19.03.03	REV01 18.01.95	REV04 27.6.02	REV02 26.02.02	REV04 11.10.99
3	08.04.04	REV07 08.04.04	REV05 11.03.03	REV02 01.07.97	REV01 18.05.92	REV03 02.02.04	REV01 18.01.95	REV06 23.03.04	REV02 26.02.02	REV04 11.10.99

The description of the modifications that the firmware underwent from Package 0 to Package 2 is provided below. [12]

7.3.1.1

Firmware Modifications from Package 0 to 1

Table 7-12
MPU Firmware Modifications from REV01 to REV02

Date	Affected source files	Description
17.03.2003	Mpu_al.c	The message “Mains is out of tolerance” (for the alarm- and log stack) is set if the charger control in the VQ mains firmware has a synch error.
17.03.2003	Oper_ups.c, RaR2.c, Commain.c, Mpu.c	Static switch EA is turned ON with a delay, in redundant systems when one UPS changes automatically from Stand by to Normal Operation.
		No uncontrolled turn ON of the static switch EA and inverter in redundant systems when the Mains is turned OFF and ON again (without battery)
		Certain start up of one UPS in redundant systems, when Mains turns ON and then immediately turn Bypass Mains OFF. (Before the system remained in Stand by)

Table 7-13
VQ Firmware Modifications from REV02 to REV03

Date	Affected source files	Description
16.01.1996	Vq.asm, Vq.dec, vqch.ini, vqch.int	Charger function improved, when operating as MAINS VQ, so that the DC voltage is more stabilized.

Table 7-14
VQ Firmware Modifications from REV03 to REV04

Date	Affected source files	Description
20.11.2002	Vq.asm, vq.dec	After a mains failure, the charger is initialized (Variable SAMPCNT is set to 0)

Table 7-15
VQ Firmware Modifications from REV04 to REV05

Date	Affected source files	Description
17.03.2003	Vq.ser	In one routine an AJMP changed to JMP that the code can be extended.
17.03.2003	Vq.asm, Vq.dec, Vq.ser, Vqch.ini, Vqch.int	After a mains failure now in all cases the charger can start up properly. Before in some cases the charger remained OFF after a Mains failure, especially in 60 Hz systems).
		When after a Mains failure the charger is turned OFF for a short time a message is sent to the MPU “Mains is out of tolerance”.
		The allowed synch-symmetry failure (time difference between two half wave of the mains voltage) is improved from 1ms to 2ms. The effect is a better performance of the charger in a MAINS VQ.

Table 7-16
Masterlogic Firmware Modifications from REV01 to REV02

Date	Affected source files	Description
17.03.2003	D091.eqn	If static switch EA is part of the UPS system, then the logic works the same as in R01, otherwise EA does not turn ON until the Inverter is turned ON.

7.3.1.2

Firmware Modifications from Package 1 to 2

Table 7-17
MPU Firmware Modifications from REV02 to REV03

Date	Affected source files	Description
11.06.2003	RaR1.c	Some default values for calibrating changed (UPS specifics instead of Datapower)
11.06.2003	Du_pict.c, Mpu.c, Mpu_al.c, Mpu_cal.c, Mpu_ch_v.c, Mpu_dmu.c, Mpu_du.c, Mpu_du_2.c, Mpu_ser.c, Mpu_str.c, Mpu_vqca.c, Oper_ups.c, RaR1.c, RaR2.c	All code that used only for Datapower is removed.
		The display of the input voltage in the start up display is removed
		New system type (WXW) can be programmed (step 1). If WXW is chosen then automatically step 60 and 61 is set to 0 (charger 0 and 30)
		The value for step 47 is set automatically if step 45 is set ($1.41 * \text{step } 45$)
		The keyed in values for step 34 ... 37 is now shown correctly
		The handling of the system calibration is improved.
		<ul style="list-style-type: none"> - All values can be input without preceding '0's. - Every step has an allocated number of max ciphers (1...4). <p>The value can be confirmed by pushing the '#' key (max ciphers =4).</p> <p>By input of the max number of ciphers the value is automatically accepted. Both cases are confirmed by a short '#' in the display.</p> <ul style="list-style-type: none"> - The decimal part of a value is always only one cipher, and must be confirmed by pushing the '#' key. - The steps can be directly accessed: Push key 'C', and then the step number (2 ciphers are allocated and are automatically accepted) - Entering the calibrating stack will be at the step number, where it was left.

Date	Affected source files	Description
		<p>The following overload profiles are now possible:</p> <ul style="list-style-type: none"> - 150% 1min; 125% 10min; 105% continuous - 150% 1min; 125% 15min; 105% continuous - 150% 1min; 125% 60min; 105% continuous - 150% 1min; 125% 30min; 105% continuous - 150% 1min; 125% 10min; 110% 20min; 105% continuous
		<p>The values that is shown for the blocking time in step 6 is changed: Now: 10us, 30us, 50us Before: 30us, 50us, 70us</p>
		<p>The DC input voltage in a WXW system is always showed positive</p>
		<p>The behavior of a redundant WXW is improved. It depends on the external charger signal.</p>

Table 7-18
MPU Firmware Modifications from REV03 to REV04

Date	Affected source files	Description
21.07.2003	Mpu_ser.c	<p>A failure is repaired. The right value of step 7 is now sent to the charger.</p> <p>In R03 always the default values are sent to the charger (MAINS VQ)</p>

Table 7-19
RAR1 Firmware Modifications from REV03 to REV04

Date	Affected source files	Description
11.06.2003	RaR1.c	Some default values for calibrating changed (UPS specifics instead of Datapower)
11.06.2003	RaR1.c	Some text for the display are changed

As prescribed by the qualification Guideline [4], to take credit for the operating history of previous versions, all changes to the design from the previous versions must be clearly identified and assessed to establish the extent and impact of each change. In particular, it is important to assess whether the safety function associated with the UPS system was affected by any of the revisions. Considering that the UPS safety function is to provide within-specification power, after reviewing the scope and safety significance of the changes to firmware package revisions, it was concluded that the operating history used for both firmware Package 0 and Package 1 can be used to support correctness-of-design arguments for firmware Package 2. Although firmware Package 0 was revised to correct a design issue which caused interruption in UPS output, since there were never any reported incidents of UPS partial failure (i.e., output of “dirty power”) [16], and also due to the fact that VQ revisions did not involve VQ-Output such that UPS’s ability with respect to detection of partial failure is affected, the operating hours of UPS system with firmware Package 0 are applicable. Similarly, the operating hours for UPS systems with firmware Package 1 are applicable since VQ firmware/hardware design was not revised and therefore the UPS ability to detect partial failure was not modified. The nature of the faults that triggered the revision from 0 to 1 is discussed in details in Section 7.3.3 of this report.

In addition to above findings, from documentation perspective it was also concluded that the details of revisions for WXX firmware packages were sufficiently documented.

7.3.2 Method 3a: “Operating History Data”

Proven-in use arguments provide sufficient confidence that there are no unknown systematic faults in the UPS systems and that the rate of random hardware faults is acceptably low. However, as prescribed by the Guide [4], such argument is appropriate provided that the PES has a clearly defined functionality, and is accompanied with sufficient documentation, which officially recorded the failures. The evidence is used to claim that the likelihood of PES failure is low enough that the required integrity of safety function associated with the categorization and class of equipment is achieved (i.e., Category B).

Reliability was measured by Gambit as the capability of the UPS system to provide uninterruptible power [13]. Firmware package 2 was released by Gambit in July 2003 and underwent a supervisory period from 01 OCT 2003 to 31 DEC 2004, before applying for TUV certification to demonstrate compliance to IEC 60880-2. During this period, a total of 480 units were sold. By the time that TUV certification was applied, out of the 480 sold units, 272 were operated for more than a year, while the remaining 208 were operated between half of year to a year, accumulating a total of 3,794,208 operating hours by the end of year 2004 [Appendix A.2, Appendix A.3]. It is unclear how many of the 480 units were of WEP type. In addition, Gambit was unable to provide up-to-date sales and failure data on relevant WEP type UPS systems using WXX firmware package 2. However, since the design of WEP type of UPS is very similar to that of all other kinds of the UPS systems manufactured by Gambit [16], this deficiency in the provided information was overlooked.

In order to be conservative, the following assumption were made when calculating unit-hours of operation for WXX firmware package 2:

1. Only 80% of the units are still in operation.
2. Only 80% of the units were run 24 hours per day

Thus, as demonstrated in Equation 7-2, by September 2007, WXX firmware package 2 accumulated more than 11 million operating hours. Figure 7-1 assists with calculating unit-years of operation.

$$3,794,208 + 0.8 \times 0.8 \times (480 \times (2 + \frac{9}{12})) \times 365 \times 24 = 11,194,656$$

Equation 7-2

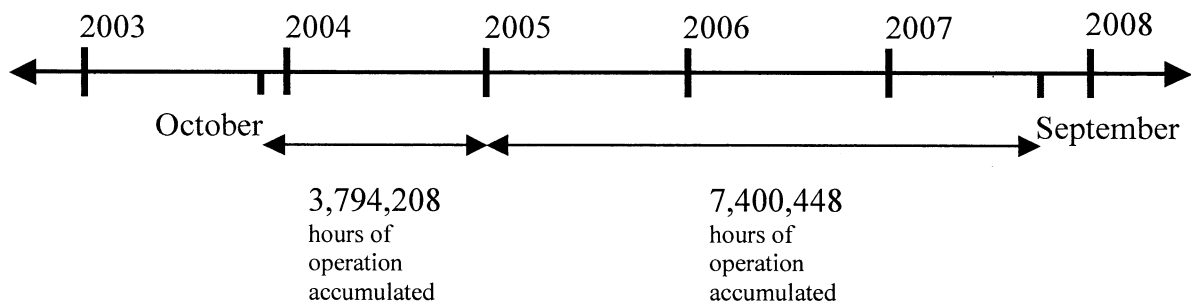


Figure 7-1 WXX Firmware Package 2 Unit-Years of Operation

Although the operating hours of WXX firmware packages 0 and 1 were determined in Section 7.3.1 to be applicable to support correctness-of-design arguments for package 2, they were not used in the calculation since the unit-operation hours of package 2 alone was sufficiently high to meet the minimum 10 million-hour requirement for a Class 2, High complexity PES, as prescribed by the procedure [3].

Hardware reliability of WEP family of UPS systems was established by calculating the unit-hours of operations using the sales data provided by Gambit during the site visit that was conducted during 28 AUG 2007 to 31 AUG 2007. Table 7-20 summarizes the quantity of WEP and WXP types of UPSs sold in years 2004, 2005 and 2006 and the associated number of reported failures. The sales data of aforementioned table were up to the period of 01 SEP 2007 and therefore unit-hours of operation were calculated only up to that date.

Table 7-20
Gambit UPS Sales / Failure Data

Year	WEP Units Sold	WXP Units Sold	Reported Failures
2004	609	190	3
2005	692	192	1
2006	1179	466	1

The following assumptions were made in order to conservatively calculate the unit hours of operation for WEP UPS systems:

1. 50% of the units were sold in the first half of the year and the remaining 50% were sold in the second half.
2. Only 80% of the units are still in operation.
3. Only 80% of the units were run 24 hours per day.

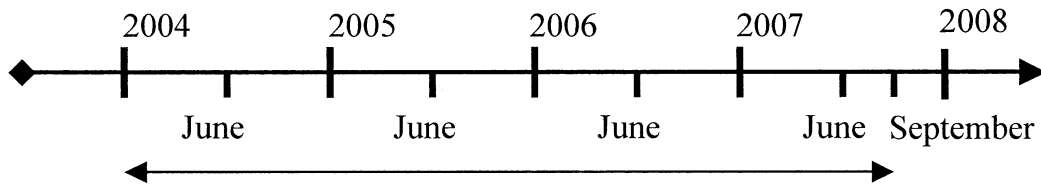


Figure 7-2 WEP UPS Unit-Years of Operation

Based on assumption number 1, the unit-hours of operation for the WEP UPS systems sold in 2004, 2005 and 2006, up to 01 SEP 2007 was calculated as:

$$\left[\frac{609}{2} \times \left(\left(3 + \frac{3}{12} \right) + \left(2 + \frac{9}{12} \right) \right) + \frac{692}{2} \times \left(\left(2 + \frac{3}{12} \right) + \left(1 + \frac{9}{12} \right) \right) + \frac{1179}{2} \times \left(\left(1 + \frac{3}{12} \right) + \frac{9}{12} \right) \right] \times 365 \times 24 = 38,456,400$$

Equation 7-3

As shown in Equation 7-4, utilizing assumptions 2 and 3, unit-hours of operation for WEP family of Gambit UPS systems was conservatively calculated as more than 23.5 million hours.

$$0.8 \times 0.8 \times 38,456,400 = 24,612,096$$

Equation 7-4

Although the operating hours of WXP family of hardware were determined in to be applicable to support correctness-of-design arguments for WEP due the similarity that exists between the design of the two families of UPS, they were not used in the calculation since the unit-operation hours of WEP family alone was sufficiently high to meet the minimum 10 million-hour requirement for a Class 2, High complexity PES, as prescribed by the procedure [3].

Calculated unit-hours of operation for WEP 1020-110/120-NEA and 1010-110/120-NEA with WXX firmware package 2 met and exceeded the minimum unit-hours of operation requirement, thus it was concluded that there are no unknown systematic faults in the UPS systems and that the rate of random hardware faults is acceptably low.

7.3.3 Method 3b: “Failure Data Assessment”

This method is used to establish that the likelihood of any failure of the UPS system due to random and systematic faults is low enough that the required integrity of the safety function for a Class-2 PES is achieved. This method involves review and assessment of Gambit UPS in-service failure data. Gambit makes use of two supervisory systems, AUFSYS and IQ-Soft, to track records of the sold units and reported failures. Former is used to keep track of information such as sales order number, system type, delivery date, customer name and firmware package installed on the sold unit. Latter is used to keep track of information on the customer-reported UPS failures. Data such as failure date, nature of fault and whether the failure was categorized as fatal, are inputted into IQ-Soft for tracking purposes. An export of these two software for the period of 01 OCT 2003 to 31 DEC 2004 were provided by Gambit and are available in Appendix A.2 and A.3 of this report.

As summarized in Table 7-21, during the 2003 – 2004 supervisory period of WXX firmware package 2, a total of 36 errors were reported [Appendix A.3]. However, some of these errors were either encountered during production and system calibration, which is not a concern since they were corrected before leaving manufacturer’s site [13]. The remaining errors were all minor such that the main function of the UPS, which is defined by the manufacturer as to provide uninterruptible power [13], was not jeopardized. In addition, there were no reported incidents of VQ-Output failure, which is the failure of concern as it may contribute to UPS partial failure. [16]

Table 7-21
WXX FW P2 Reliability Data for Period of 01 OCT 2003 to 31 DEC 2004

WXX Firmware Package 2	Minor Errors	Fatal Firmware Errors	Fatal Hardware Errors
> 1 yr	20	0	0
1 yr > 0.5 yr	16	0	0

In a separate supervisory period of 01 NOV 2000 to 31 DEC 2004, Gambit recorded a total of nine fatal firmware failures on UPS systems with firmware WXX package OLD and package 0, where the output of UPS was lost [13]. The descriptions and number of occurrences of these failures are as follows:

1. The charger in VQ-Mains does not detect the mains voltage at any time (7 instances)
2. Equalizing current in a redundant system: if one UPS automatically starts, the output was lost for a short time. (2 instances)

Above failures were rectified by Gambit via upgrading the firmware from Package 0 to Package 1. This was accomplished by making the following modification:

- VQ firmware was upgraded from R03 to R05
- MPU firmware was upgraded from R01 to R02
- Masterlogic firmware was upgraded from R01 to R02.

The description of the modifications that the firmware underwent from Package 0 to Package 2 is provided in Section 7.3.1.

Using the sales and failure data provided by Gambit [Appendix A.2, 3] TUV Nord quantitatively estimated the reliability of WXX firmware package 2 using two different methods [14].

Table 7-22 summarizes TUV Nord's finding.

Table 7-22
TUV Nord Quantitative Reliability Assessment of WXX Firmware Package 2

Estimation Method	Calculated Failure Rate	Corresponding Safety Integrity Level According to IEC 61508
Dual sided confidence limit of 70%	$1.92 \times 10^{-4} / \text{year}$	SIL 2
Single sided lower confidence of 70%	$1.24 \times 10^{-3} / \text{year}$	SIL 2

As shown above, based on the two approaches taken by TUV Nord, calculated failure rates were sufficiently low that they corresponded to SIL 2 category system. It is noteworthy that a SIL 2 classification according to IEC 61508 is equivalent to a Class 2 equipment safety class according to IEC 61513, as prescribed by qualification guide [4].

Based on the assessment performed on the provided failure data, it was concluded that the likelihood of any failure of the UPS system due to random and systematic faults is low enough that the required integrity of the safety function for a Class 2 equipment is achieved.

7.3.4 Method 3d: "Reference Site Assessments"

This method was used to establish credibility of UPS systems operating history. As part of Gambit's bid, an international list of reference nuclear power plants that have purchased Gambit products was provided [Appendix A.9]. In order to obtain relevant operating/failure data, Gambit was later requested to provide a list of contacts who are currently using Gambit UPS systems in nuclear applications. A site questionnaire form consisting of 17 questions was composed and sent to the contacts electronically. The questions were divided into five categories:

- **UPS Data:** The questions in this section were used to establish information such as model number, power rating, firmware package, rating, intended purpose of the UPS, operation environment, etc.
- **UPS Documentation:** To ask the users if any issues were ever encountered due to lack of documentation provided by Gambit (i.e., installation/commissioning/maintenance issues, etc.)
- **UPS Goodness of Design:** Users were asked if they ever encountered any failures, nature of the fault, time to repair, etc.

- **Applicability of Data:** The questions in this section were used to assess applicability of the clients' failure data. Users were asked questions such as whether a preventive maintenance program for the UPS systems existed and what the frequency of the maintenance is.
- **Miscellaneous:** In this section, users were asked about their overall experience with Gambit as a service provider and if the UPS systems met their expectations.

A copy of the questionnaire can be found in the Appendix A.10. By 15 OCT 2007, three of the reference customers responded to the questionnaire. In order to respect the users' privacy, they are referred to User A, User B and User C. Table 7-23 summarizes the users' responses to the questionnaire. The reliability data collected from the reference sites is applicable as the users operated Gambit units in applications and environments similar those that they'll be used in R 1 and R 2. User C who has used Gambit inverter/rectifier systems the longest (between 7 to 17 years) in comparison with User-A and -B, described Gambit products as "highly reliable". Overall, all users indicated satisfaction with Gambit's products and services. The data obtained from the reference sites provided additional support to demonstrate reliability of Gambit UPSs.

Table 7-23
Reference Site Questionnaire

User	UPS Data			UPS Goodness of Design				Applicability of Data		Documentation	Miscellaneous
	Hardware	Firmware	Commissioning Date	Recorded Failure	Cause of Failure	Time to Repair [hr]	Repaired in-house / GAMBIT	Preventive Maintenance (PM) Performed	Frequency of PM		
A	4 sets of DWV inverter systems	WWX Package 2 and SDC Rev 14	May 2005	Yes	Defective Alarm Relay	< 1	In-House	Yes	Service performed every two years. Minor test performed on weekly basis.	Experienced difficulties with setting up the signals from the equipment to the plant due to lack of good documentation.	Overall happy with GAMBIT's service. GAMBIT's products met reliability and safety requirements.
B	2 sets of WEP 1005	WWX firmware Package 3.2	September 2005 October 2005	No	N/A	N/A	N/A	Yes	Service performed every 18 months. Thermography performed every 12 months. System Engineer performs quarterly walkdowns.	No issues encountered due to lack documentation.	Overall happy with the purchased UPS systems.
C	SDU Rectifiers in combination with DWV Inverters	Not known	Units have been in operation between 7-17 years.	Yes	Minor failures (i.e. change of ventilator). Two recorded counts of non-minor failures. The nature of these failures were not discussed. However, client states that the equipment has been highly reliable. No failure has even posed an operational safety threat.	<24	Minor defects (i.e. parts replacement) were done by a local company. Major problems fixed by GAMBIT.	Yes	Performed as per GAMBIT's recommendation (details were not provided)	No problems were ever encountered due to lack of documentation.	GAMBIT's products have met client's expectations.

8. QUALIFICATION CONCLUSIONS

The qualification of Gambit WEP 1010-110/120-NEA and WEP 1020-110/120-NEA UPS systems is based on a comprehensive evaluation of various characteristics related to their application in R1 and R2 reactors, which is to provide Class II electrical power within acceptable limits on voltage, amplitude, frequency and harmonics to safety-related loads. The analysis employs a set of qualification methods, as required by the project specific procedure [3], and leads to the conclusion that the product is suitable for the intended application. The conclusions relevant to the different aspects of application context are detailed below.

8.1 Suitability Evaluation

The subsections here provide details on how the findings under the different methods in Section 7 satisfy the requirements defined in the Technical Specifications [5].

8.1.1 Safety Attributes, Fails Safe or Fail Detected Behaviour

In the event of an inverter failure, the UPS is designed to switch to bypass mode of operation. However, if bypass also becomes unavailable, the UPS is designed to shut down, which does not pose a safety danger to the loads as they are designed to fail-safe in the event of power interruption.

The UPS system is equipped with sufficient electronics (i.e., VQ-Mains, VQ-Bypass, VQ-Output, DMU) such that failures in incoming grid, bypass, battery and output are detected and appropriate alarms are generated. Below is an illustration of alarm indications on the front control panel of the UPS. An acoustic alarm follows the visual alarms listed below.

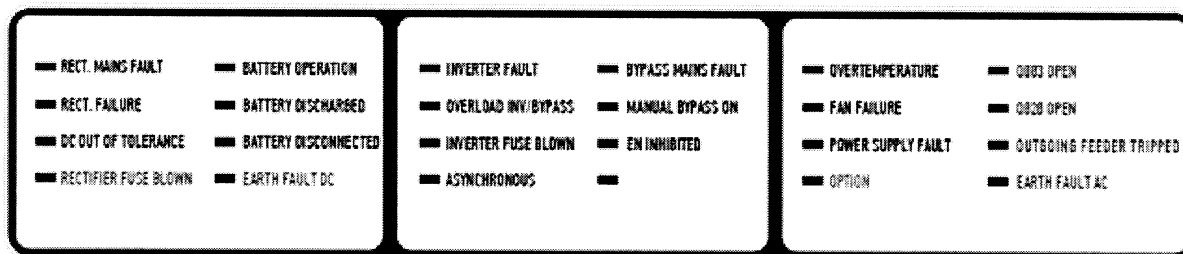


Figure 8-1 Alarm Indications of UPS Control Panel

In addition to above visual and acoustic alarms, plant operator is immediately informed via Main Control Room alarms listed in Table 7-3.

Based on the results of Methods 3b (Failure Data Assessment) and 5d (Hardware Reliability, Failure Modes and Diagnostic Assessment) in respective Sections 7.3.3 and 7.1.5 of this report, from suitability perspective, it was concluded that the purchased UPS systems met the safety attribute requirements, including fail-safe and fail-detected criteria.

8.1.2 Functionality

The conformance of the UPS to the functional requirement under Section 5.2 of this report was evaluated. The UPS modes of operation are in line with the requirements set in TS. The batteries that are supplied with the UPS are capable of energizing the loads for the required

durations as show in Table 5-1. In addition, if the normal Class III power supply has been lost for a defined time period between 1 and 6 minutes, an equalizing charge of the batteries is automatically initiated, as stated in the technical specifications [5].

Product documentation along with the technical evaluation of tenders [15], which was done initially to determine the winning bid indicate functional suitability of Gambit UPS systems for the intended application. Although Gambit's definition of UPS safety function is different than that of the Categorization report [1], considering the un-likelihood of an undetected partial failure as demonstrated by Methods 5d (Hardware Reliability, Failure Modes and Diagnostics), 3a (Operating History Data) and 3b (Failure Data Assessment), the gap was overlooked.

After reviewing the product documentation and considering the results of Methods 2 (Assessment of Product Specification) and 4a (In-Service Maintenance Process Assessment) in respective Sections 7.2.1 7.1.1 of this report, from suitability perspective, it was concluded that the purchased UPS systems met the functional requirements recorded in Sections 5.2.1 to 5.2.5.

8.1.3 Performance

Section 5.3 of this report specified the performance requirements associated with the UPS system, as outlined in the Technical Specifications [5]. Several UPS documentations, such as WEP 1000 Technical Data Sheet [Appendix A.11] and Factory Acceptance Testing [17] were consulted to verify that specified requirements were met. Tables below summarize the performance requirements and UPS systems' compliance to them.

Table 8-1
Assessment of UPS Conformance to Performance Requirements

Performance Requirement	Description	Compliance	Comments
R1 UPS1	20 kVA, 120V ac single phase output at 0.8 lagging Power Factor.	Yes	
R1 UPS2	8 kVA, 120V ac single phase output at 0.8 lagging Power Factor.	Yes	Gambit supplied a 10 kVA, single-phase output at 0.8 lagging power factor. This was accepted by AECL. [18]
R2 UPS1	20 kVA, 120V ac single phase output at 0.8 lagging Power Factor.	Yes	
R2 UPS2	8 kVA, 120V ac single phase output at 0.8 lagging Power Factor.	Yes	Gambit supplied a10 kVA, single-phase output at 0.8

Performance Requirement	Description	Compliance	Comments
			lagging power factor unit. This was accepted by AECL. [18]
Normal UPS Input Power Supply	208 V, 3 phase, 3 wire	Yes	
Normal Power Supply Input Voltage	208 V \pm 10%	Yes	
Alternate UPS Power Supply	120 V, 1 phase, 2 wire	Yes	
Alternate Power Supply Input Voltage	120 V \pm 10%	Yes	
Input Frequency	60 Hz, \pm 5%	Yes	
UPS Output	120 V, 1 phase, 2 wire, 60 Hz.	Yes	
UPS Load Power Factor	0.8 to 1.0 lagging	Yes	Actual allowable power factor is 0.4 lag to 0.9 lead.
Enclosure	NEMA 1 with drip shield	Yes	Gambit supplied IP21 enclosures as per IEC 60529. This was accepted by AECL. [15]
Audible Noise Level	<70 dBA at 1 m.	Yes	
Normal Ambient Temp	20°C \pm 5°C	Yes	
Min. / Max. Ambient Temp	10°C / 40°C	Yes	
Relative Humidity	< 95% at < 200 m above sea level	Yes	

Table 8-2
Assessment of Inverter Conformance to Performance Requirements

Performance Requirement	Description	Compliance	Comments
Nominal Output Voltage	120 V, 1 phase, 2 wire, 60 Hz.	Yes	
Output Voltage Regulation	\pm 5% for any combination of changes to the load (0 to 100% with 1.0 to 0.8 lagging power factor), inverter dc input voltage (up to 110% rated) and	Yes	This was deomstarted in Factory Acceptance Test [17].

Performance Requirement	Description	Compliance	Comments
	ambient temperature (15°C to 40°C).		
Voltage Transient Response	< $\pm 10\%$ for a 100% step load change or transfer to the <i>alternate</i> power supply. Recovery to $\pm 3\%$ shall be achieved in <100ms.	Yes	$\pm 4\%$ in <25 ms
Output Voltage Adjustment	$\pm 5\%$	Yes	Output voltage adjustment is done through the GUI and is password protected.[27]
Output Frequency Stability	< ± 0.5 Hz when operating in free running mode.	Yes	<0.01%
Output waveform	Sinusoidal	Yes	
Harmonic Distortion	A: < 5% THD (10 -100% load; 0.8 -1.0 PF); up to 90% Non Linear load.	Yes	Demonstrated in Harmonic Analysis Report [25]
	B: Any single harmonic of the PWM switching frequency shall be less than 0.1 % of the 60 Hz output voltage.	No	As per Table 11.1 of IEEE 519, the individual distortion associated with UPS systems with rating of 69 kV and lower must be less than 3%. The supplied UPS systems meet the requirements of IEEE 519.
Over-current Capability	125% for 10 minutes and 150% for 30 s., each without the <i>alternate</i> power source.	Yes	
Slew Rate	<1.0 Hz/s.	Yes	The UPS systems are programmed at 1 Hz/Second.
Crest Factor	>3.0 @ full load	Yes	

Table 8-3
Assessment of Rectifier/Battery Charger Conformance to Performance Requirements

Performance Requirement	Description	Compliance	Comments
Rated Output Current	Sufficient to recharge the battery from a fully discharged state to nominal values within 12 hours while simultaneously supporting the continuous UPS Class II full load.	Yes	As per Recharge Characteristic curve provided by manufacturer of batteries, Absolute IIP, at 12 hours, the batteries are 95% charged. [Appendix A.12] The difference of 5% is insignificant and was overlooked.

Performance Requirement	Description	Compliance	Comments
Current limit	< 120% of the rated output current.	Yes	Total rectifier DC current and battery charging current are user adjustable. [Appendix A.11].
Output Ripple Voltage	Sufficiently low to permit the inverter to operate correctly under any load conditions with the battery disconnected, and < 2% with batteries connected.	Yes	Demonstrated in Performance Test Report [17] with the batteries disconnected. No tests were done to measure output voltage ripple with batteries connected, however, since the tolerance limits if the rectifier is 1%, this requirement is met.
Harmonics Reflection	<1% harmonics reflected into supply side.	To be Determined at Time of Commissioning	
Rectifier	12 Pulse	Yes	
Float Voltage Adjustment	$\pm 5 \%$	Yes	Programmable [Appendix A.11]
Equalize Voltage Adjustment	$\pm 5 \%$	Yes	Programmable [Appendix A.11]
Output Voltage Regulation	$\pm 1\%$ for any combination of changes to the load (0 to 100%), nominal input voltage ($\pm 10\%$) and ambient temperature (15°C to 40°C).	Yes	$\pm 1\%$ for static load changes within 0 – 100% load surge. [Appendix A.11]

Table 8-4
Assessment of Battery Conformance to Performance Requirements

Performance Requirement	Description	Compliance	Comments
Type	Lead Acid Sealed, maintenance free.	Yes	
Ampere -Hour Rating:	Sufficient to supply dc to the inverter to provide output to UPS loads.	Yes	
R1 UPS 1	Battery capacity to be sized to support the Inverter output of 20 kVA at 0.8 Power Factor for 30 minutes.	Yes	
R1 UPS 2	Battery capacity to be sized to support the Inverter output of 8 kVA at 0.8 Power Factor for 180 minutes	Yes	
R2 UPS 1	Battery capacity to be sized to support the Inverter output of 20 kVA at 0.8 Power Factor for 30 minutes.	Yes	
R2 UPS 2	Battery capacity to be sized to support the Inverter output of 8 kVA at 0.8 Power Factor for 180 minutes	Yes	

Table 8-5
Static Transfer Switch Performance Requirements

Performance	Description	Compliance	Comments
Type	Solid State, Single phase	Yes	
Switch Operation	Make -before -break	Yes	
Maximum Transfer Time	< 10 ms	Yes	It is < 4ms. [27]
Over -Load Capability	Same as Inverter.	Yes	

With the exception of “Harmonics Reflection” and “Output Voltage Adjustment” requirement in Table 8-2, Gambit complied with all the performance requirements of the UPS systems. Former exception is due to the fact that harmonics reflection of the UPS systems can only be measured after field installation of the system. Previous tests conducted on the existing 6-pulse, 8kVA and 20kVA UPS units demonstrated that the reflect harmonics were 3.3% and 2.1%, respectively. The supply network impedance and X/R ratio remains the same for the new UPS systems. However, since the new UPS systems use 12-pulse rectifiers, which inherently generate fewer harmonic than 6-pulse counter parts, it is expected that measured reflected harmonics will fall close to the required value [19]. Also, another contributing factor to this exception is that the aforementioned test was not part of FAT, which was reviewed and accepted by AECL in advance of testing.

“Output Voltage Adjustment” is not an available option available as systems are calibrated by Gambit at the specified value prior to shipment. [26] This is not a concern since the application for which the UPS systems will be used does not require adjustment of their output voltage.

Conformity of the UPS systems and batteries to the additional requirements specified in Section 5 of this report were investigated and the following non-conformities were identified:

Table 8-6
Deposition of Non-Conformities to Additional Requirements

Section	Requirement	Note
5.3.3	Inter-cell connectors and cell terminals shall have fully removable boot type insulation covers.	No insulation covers are provided. However, access to batteries is protected via Lexam covers.
5.6	The design and the routine test for the complete UPS shall be performed after assembly and interconnection of the functional units, in accordance with IEEE standard 944. The rectifier/charger shall be tested in accordance with NEMA PE5.	IEEE 944 is now obsolete and has been superseded by IEC 62040-3. Gambit tests were done as per IEC 62040-3 standard.
5.6.2	The supplier shall number each battery.	The batteries are not labelled. This is taken care via Recommended Action # 6 in Section 9.1 of this report.
5.6.2	The supplier shall provide the purchaser with impedance of each battery.	The impedance of the batteries is not specified by the supplier. This is not a concern since the faulty battery cells will be identified by the station via the recommended monthly and annual maintenance tests.

Considering the results of Methods 2 (Assessment of Product Specification) and 5d (Hardware Reliability, Failure Modes and Diagnostic Assessment) in respective Sections 7.2.1 and 7.1.5 of this report, from suitability perspective, it was concluded that the purchased UPS systems conformed to the performance requirements.

8.1.4 Reliability

Although no explicit MTBF and MTTR numbers were specified in the TS [5], the calculated figures provided by Gambit [Appendix A.8] are acceptably high. As shown in Equation 7-1, MTBF of the UPS system is a function of failure rate and associated MTBF and MTTR of multiple components that the UPS is composed of (i.e., battery, inverter, etc.). The calculations in Appendix A.8 were done with the following considerations:

- MTTR figures were estimated based on shipping time from manufacturer's site to Location-X.
- The mean time between grid failures in Location-X was conservatively estimated as one every 1000 hours.

The resultant MTBF of 43 years is acceptably high to support reliability of the purchased UPS system.

Considering the results of Methods 3a (Operating History Data), 3b (Failure Data Assessment), 5d (Hardware Reliability, Failure Modes and Diagnostic Assessment), 5e (Assessment of

Hardware Useful Life), 9a (Assessment of 3rd Party Corporate Quality System Certifications) and 9b (Assessment of Product Safety Certification) in respective Sections 7.3.2, 7.3.3, 7.1.5, 7.1.6, 7.2.2 and 7.2.3 of this report, from suitability perspective, it was concluded that the purchased UPS systems met the reliability requirements associated with a Class 2 PES.

8.1.5 Maintainability

As per the Technical Specifications [5] the UPS is required to have "...easy maintainability under all operating conditions...". A copy of the Operations and Maintenance Manual [20] was submitted by Gambit to AECL. Gambit recommended monthly, semi-annually and annual testing of the UPS and monthly and annual checks of the batteries. The description and the scope of the tests are outlined in [20]. A separate P.O. for the recommended spare parts will be issued to ensure component replacement by the station is done at the specified intervals.

Considering the results of Methods 4a (In-Service Maintenance Process Assessment) and Method 3d (Reference Site Assessment) in respective Sections 7.1.1 and 7.3.4 of this report, from suitability perspective, it was concluded that the purchased UPS systems conformed to the maintainability requirements.

8.1.6 Testability

After reviewing Gambit product documentation and considering the results of Method 4b (In-Service Testability Assessment), Methods 4a (In-Service Maintenance Process Assessment) and Method 3d (Reference Site Assessment) in respective Sections 7.1.8, 7.1.1 and 7.3.4 of this report, from suitability perspective, it was concluded that the purchased UPS systems conformed to the testability requirements.

8.1.7 Security

Although no security requirements were mentioned in the TS [5], the UPS system is equipped with multiple security features to prevent non-authorized personnel from changing critical parameters such as set-points and tolerance limits. For instance, in order to perform system calibration, first a pre-defined password needs to be keyed into the system via the keyboard on the front panel (Figure 8-2).

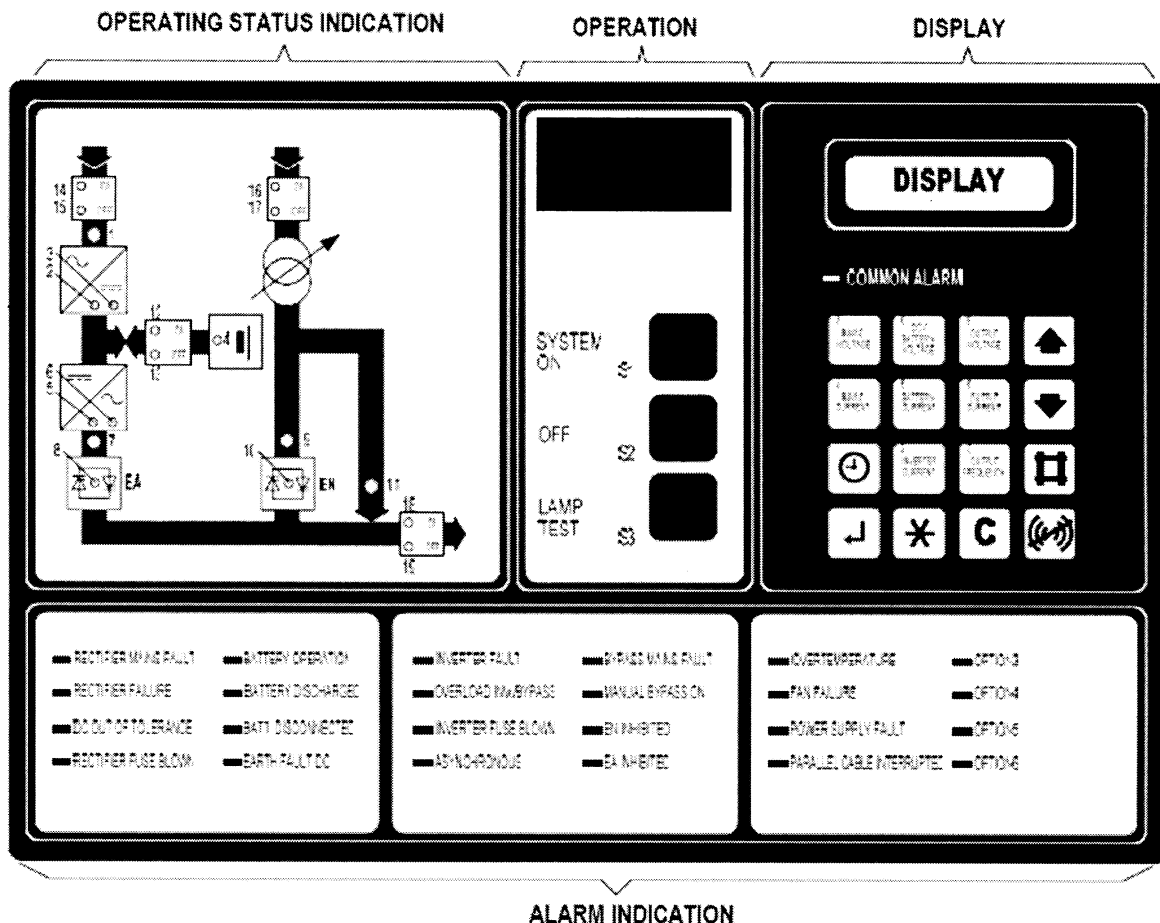


Figure 8-2 Gambit UPS Front Panel View

After reviewing the product documentation, it was concluded that from suitability perspective, the purchased UPS systems came with sufficient security features that protected the UPSs from reconfiguration by unauthorized personnel.

8.1.8 Seismic

The purchased UPS system including the batteries successfully met all the seismic requirements. The base plates required for installation of the batteries was designed by AECL. [21]

Considering the results of Method 5c (Seismic Tolerance Assessment) in Section 7.1.4 of this report, it was concluded that the UPS and batteries supplied by Gambit successfully met the seismic requirements.

8.1.9 Environmental Tolerance

Considering the results of Method 5a (Environmental Tolerance Assessment) in Section 7.1.2 of this report, from suitability perspective, it was concluded that the purchased UPS systems conformed to the environmental tolerance requirements.

8.1.10 Electromagnetic Immunity/Emissions

Considering the results of Method 5b (Electromagnetic Immunity and Emissions Assessment) in Section 7.1.3 of this report, from suitability perspective, it was concluded that the purchased UPS systems conformed to the electromagnetic immunity and emissions requirements, with the exception of a lack of demonstrated immunity of the AC input power port, i.e., AC Mains input and AC Bypass Mains input, to power line harmonics and inter-harmonics, and phase unbalance, as specified in IEC 62040-2:2005, Clause 7.4 and Annex D.6.

Recommended actions to compensate for the above gap in qualification evidence have been defined to provide assurance of electromagnetic compatibility of the UPS with its electromagnetic environment, in conformance with requirements identified in Section 5.10.

8.2 Adequacy of Product Documentation

In general, the documentations provided with the purchased UPS systems were found to be detailed, complete and sufficient to determine the suitability and correctness of design. The list of all the documentation submitted by Gambit is available in Section 7.2.1 of this report. These documents clearly defined the product specifications and provided sufficient information to support safe operation of the UPS system.

Considering the results of Methods 2 (Assessment of Product Specification), 3d (Reference Site Assessment) and 9b (Assessment of 3rd Party Product Certification) in Sections 7.2.1, 7.3.4 and 7.2.3 of this report, it was concluded that the purchased UPS systems came with sufficient documentation that assisted with assessing the suitability of the purchased UPS systems in the target application and supported their safe operation. In addition, requirements for periodic inspections and replacement of life-limiting components were provided in the product-documentation made available by Gambit.

8.3 Evidence of Correctness

The two approaches used to establish evidence of correctness of the purchased UPS systems were:

- Compliance to appropriate recognized safety-related standards
- Reliability data gathered from field experiences

Results of Methods 3a (Proven in Use Argument, Section 7.3.2), 3b (Operating History Data, Section 7.3.3), 3c (Product Design Revision History Assessment, Section 7.3.1), 3d (Reference Site Assessment, Section 7.3.4), 5d (Hardware Reliability, Failure Modes and Diagnostics Assessment,), 9a (Assessment of 3rd Party Corporate Quality System Certification, Section 7.2.2), 9b (Assessment of 3rd Party Product Safety Certification, Section 7.2.3) and 9c (Assessment of 3rd Party Hardware Test Standards Compliance, Section 7.1.7), provided sufficient evidence that the purchased UPS systems are correct in design and can be used safely in R1 and R2 plants for the intended application.

9. RECOMMENDED ACTIONS

9.1 Suitability Evaluation

After reviewing the findings under methods outlined in Section 6.1, which were used to establish suitability of the purchased UPS systems in the target application, the following recommendations were made:

1. A Preventive Maintenance program should be implemented by the station to perform component replacement on the UPS systems as suggested by Gambit.

Rationale: in order for the UPS systems to achieve the required 40-year life and manufacturer-calculated MTBF and MTTR figures, the station at the specified frequencies should carry out replacement of life-limiting components identified in Section 7.1.6 of this report.

2. Monthly, semi-annual and annual maintenance testing and inspection of the UPS systems, along with monthly and annual testing of the batteries should be carried out by the station as indicated in the Gambit's Operation and Maintenance Manual [20]. The frequencies of the tests, at bare minimum, must match or preferably exceed those suggested by the [20].

Rationale: Class-2 category was assigned to the UPS systems contingent on monthly maintenance checks [1]. Also, maintenance test and inspection of the UPSs are designed to monitor system health and ensure longevity of the systems.

3. A calibrated, external power monitor should be used on minimum monthly intervals to examine the quality of the output voltage, frequency and harmonics of the UPS systems.

Rationale: As per the Categorization Report [1], monthly maintenance testing is relied upon to reveal out-of-specification output-power-harmonics, which is a condition not revealed by the alarm functions. In addition, monthly maintenance testing is considered to provide back-up detection capability against undetected partial power failure. These reasons constitute the need for an external power quality monitor to minimize the possibility of UPS partial failure.

4. In the event that any of the following two alarms are generated:

- a) OUTPUT INST OUT OF TOL; and
- b) OUTPUT FREQUENCY IS OUT OF TOLERANCE

It is recommended to shut down the affected UPS system and manually power the loads via the alternate supply, while diagnostics tests are performed

Rationale: Above alarms may be generated due to VQ-Output failure, which makes the loads of the affected UPS system prone to receipt of out-of-specification power. In order to prevent this scenario, it is recommended that the loads be supplied directly via alternate supply while the systems is diagnosed.

5. The following actions should be implemented to compensate for the lack of demonstrated immunity of the AC input power port, i.e., AC Mains input and AC Bypass Mains input, to power line harmonics and inter-harmonics, and phase unbalance, as specified in IEC 62040-2:2005, Clause 7.4 and Annex D.6:

- During UPS commissioning, the level of harmonics generation at the AC Mains and AC Bypass Mains inputs should be measured and proper functioning of UPS control circuits confirmed.

- During UPS operation, the level of harmonics should be measured at regular intervals defined in the Maintenance Program, so that any increase in harmonics will become apparent.
- Should a rise in harmonics level be detected, corrective measures should be considered.
- Modifications to the electrical system should be designed to minimize any increase in harmonics generation at the AC Mains and AC Bypass Mains inputs.

Rationale: In the absence of power line harmonics and inter-harmonics, and phase unbalance immunity test data, immunity margin is unknown. It is therefore necessary to monitor power line harmonics and inter-harmonics, and phase unbalance for any deterioration, as this poses an EMI threat. Corrective measures to restore power line harmonics and inter-harmonics, and phase unbalance to levels no higher than the baseline established during commissioning are needed to ensure electromagnetic compatibility.

6. The set of cell numerals and system polarity labels, which are supplied with the batteries should be applied after receiving the shipment.

Rationale: The TS required the supplier to label each battery cell prior to shipment. However, this requirement was not met as the supplier expects the purchaser (i.e., AECL) to affix the numbers. Numbering of cells helps with performing diagnosis/maintenance of individual cells, should the need arise. The manufacturer of the batteries, Absolyte IIP, recommends applying the labels on the positive terminal of each cell [20].

9.2 Adequacy of User-Documentation-for-Safety

1. The Graphical User Interface (GUI) on the front panel of Gambit UPS systems is password protected. It is recommended that the passwords be only accessible to the authorized personnel who are trained on the systems.

Rationale: Some safety parameters, set-points and calibration values of the UPS systems can be changed via the GUI. In order to ensure that only the trained authorized personnel perform change of such parameters, it is recommended to control access to the documents that contain such information.

9.3 Evidence of Correctness

There are no recommendations made under this section as the evidences of correctness gathered through application of various methods in Section 7 demonstrated sufficient reliability in correctness of design of the purchased UPS systems.

10. REFERENCES

- [1] R1 and R2 Function Categorization Assessment, 9999-65500-ASD-018, Rev. 1, 2007 October.
- [2] Categorization of Functions for the Classification of Programmable Electronic Systems (PES) in Nuclear Safety Related Applications, 00-567.1 Rev. 0, 2004 March.
- [3] Qualification of Programmable electronic Systems (PES) Products for use in Nuclear Safety-Related Applications, 9999-566.1 Rev-0, 2006 Sept, (project specific procedure).
- [4] Guide for the Application of the "Procedure for Qualification of Programmable electronic Systems (PES) Products for use in Nuclear Safety-Related Applications", 9999-566.1.1, Rev. 0, 2006 Sept.
- [5] Technical Specification Uninterruptible Power Supply, 9999-52300-TS-010, Rev. 1, 2006 September.
- [6] IEC 62040-2:2005, Uninterruptible power systems (UPS) – Part 2: Electromagnetic compatibility (EMC) requirements), International Electrotechnical Commission, 2005 October.
- [7] Evidence of EMC Resistance/ Gambit EMC Type Test Program, Gambit Technical Report #1070050003/4, Rev. 01, 2007 May 15, AECL document number 9999-55000-371-000-0001.
- [8] Electromagnetic Compatibility, Montena EMC SA Test Report No. 14'662, 2006 Dec 12, AECL document number 9999-55000-371-000-0002.
- [9] ISO/IEC 17025:2005, General requirements for the competence of testing and calibration laboratories, International Organization for Standardization, 2005 May.
- [10] Guideline for the Application of the Procedure for Categorization of Function for the Classification of PES in Nuclear Safety-Related Applications, 00-567.1.1 Rev 0, 2004 March.
- [11] Common Cause Failure Analysis of Gambit WXX and SDC Firmware According to IEC 60880-2, Clause 4.1. Gambit Document Q 320.108GB, 2005 June, AECL document number 9999-55000-371-000-0003.
- [12] Qualification of WXX Firmware Package 2 According to IEC 60880. Gambit Document Q 320.106GB, 2005 June, AECL document number 9999-55000-371-000-0004.
- [13] Reliability & Operating Experience of Gambit Rectifier-, Inverter- and UPS-Systems According to IEC 60880. Gambit Document Q320.109GB, 2005 June, AECL document number 9999-55000-371-000-0005.
- [14] TUV Nord SysTec GmbH & Co. KG, Evaluation Report for Gambit WXX Firmware and SDC Firmware. Document Number, M. SEE.02.022.04, 2005 March, AECL document number 9999-55000-371-000-0006.
- [15] Technical Evaluation of Tenders for Replacement of R1 & 2 UPS 1 & 2, 9999-55000-313-014, Rev. 0, 2007 February.

- [16] Minutes of Meeting between AECL and Gambit Electronic Ltd. Date: August 29th, 30th, September 3rd, 4th and 5th, 2007, AECL document number 9999-55000-320-000-0009.
- [17] Performance Test Report, 9999-55000-371-9003, Rev. 1, 2007 December.
- [18] Deviation Disposition Request, 9999-55000-014-DDR-001 Rev. 0, 2007 September.
- [19] E-mail from Chet Raghu to Wally Kalechstein, 23 OCT 2007, 11:53 AM, AECL document number 9999-55000-200-000-0040.
- [20] Operation and Maintenance Manual, 9999-55000-MM-9001, Rev. 0.
- [21] Seismic Qualification of R1 and 2 UPS Batteries, 9999-55000-220-001, Rev. 0, 2007 October.
- [22] Seismic Test Report / Analysis of AC-UPS, 9999-55000-371-9004, 2007 July.
- [23] E-mail from Gambit on 31 AUG 2007, 10:31 AM, AECL document number 9999-55000-320-000-0010.
- [24] Radiological Areas and Zones, AECL RC-2000-633-1, Rev. 0, 1996 July.
- [25] Harmonic Analysis Report, 9999-55000-371-9001 Rev. 0, 2007 September.
- [26] Performance Test Procedure, 9999-55000-9001 Rev. 0, 2007 July.
- [27] Email from Gambit on 10 DEC 2007, 2:01 PM, AECL document number 9999-55000-320-000-0011.

Appendix A

Appendices

A.1 Interface Complexity Index

The Interface Complexity Index (ICI) is a measure used to indicate the relative software design complexity of a PES due to the number and complexity of its interfaces and is calculated using the following simple formula:

$$ICI = \sum \text{Complexity Index Rating of Each Interface}$$

Equation 10-1

The Qualification Guide [4] suggests the typical types and complexity values for internal and external interfaces. These values are summarized in the table below.

Table A-1
Interface Complexity Indices and Associated Weights

Interface Description	Maximum Associated Weight
Serial or Parallel Ports	2
Hardwired I/O Signal Interface	1
LAN Communication Interface	7
Standard Keyboard Interface	4
Text Display Interface	2
Advanced Graphics Display Interface	10
Inter-Process Communication	5
Shared Area or Common Memory Data Interchange	3
Other Consideration	Use Judgement

Using the values provided in table above, interface complexity index of the purchased UPS systems was calculated as 12 using the Equation 10-2:

$$ICI = 0 + 1 + 0 + 2 + 1 + 4 + 2 + 2 + 0 = 12$$

Equation 10-2

A.2

Sales Data of Gambit WXX Firmware Package 2 for Period of 01 OCT 2003 to 31 DEC 2004 (AUFSYS Export)

Sum of No. of Controller Installed Software	Total
SDC old	944
SDC Rev14	2417
SDC Rev14 (<1Y)	475
SDC Rev14 (>1Y)	1942
XXW old	346
XXW P0	2091
XXW P1	190
XXW P2	480
XXW P2 (>1Y)	208
XXW P2 (0.5...1Y)	272
XXW P3	402
other system than SDC,XXW	207
Grand Total	7077

Sum of operating time [year] Installed Software	Total
SDC old	5073
SDC Rev14	5383
SDC Rev14 (<1Y)	250
SDC Rev14 (>1Y)	5132
XXW old	2216
XXW P0	7658
XXW P1	274
XXW P2	433
XXW P2 (>1Y)	228
XXW P2 (0.5...1Y)	206
XXW P3	123
other system than SDC,XXW	930
Grand Total	22090

Sum of operating time [h] Installed Software	Total
SDC old	44'435'640
SDC Rev14	47'154'048
SDC Rev14 (<1Y)	2'194'080
SDC Rev14 (>1Y)	44'959'968
XXW old	19'409'832
XXW P0	67'081'368
XXW P1	2'403'192
XXW P2	3'794'208
XXW P2 (>1Y)	1'993'320
XXW P2 (0.5...1Y)	1'800'888
XXW P3	1'081'272
other system than SDC,XXW	8'147'328
Grand Total	193'508'888

	operating time [h]	Fatal FW errors	Failure rate
SDC old	44'435'640	0	2.25045E-08
SDC Rev14	47'154'048	0	2.12071E-08
SDC Rev14 (<1Y)	2'194'080	0	4.55772E-07
SDC Rev14 (>1Y)	44'959'968	0	2.2242E-08
Total	91'589'688	0	1.09183E-08

	operating time [h]	Fatal FW errors	Failure rate
XXW old	19'409'832	2	1.03041E-07
XXW P0	67'081'368	7	1.04351E-07
XXW P1	2'403'192	0	4.16113E-07
XXW P2	3'794'208	0	2.6356E-07
XXW P2 (>1Y)	1'993'320	0	5.01676E-07
XXW P2 (0.5...1Y)	1'800'888	0	5.55282E-07
XXW P3	1'081'272	0	9.24837E-07
Total	97'564'080	9	9.22471E-08

A.3

Failure Data of Gambit WXX Firmware Package 2 for Period of 01 OCT 2003 to 31 DEC 2004 (IQ-Soft Export)

Count of IQ-Soft No. (Only for Information)	
installed SW	Total
SDC old	47
SDC Rev14	104
SDC Rev14 (>1Y)	92
SDC Rev14 (<1Y)	12
XXW old	43
XXW P0	186
XXW P1	21
XXW P2	36
XXW P2 (>1Y)	20
XXW P2 (0.5...1Y)	16
XXW P3	17
error in production	5757
other system than SDC XXW	129
System not supervised <1998	101
Grand Total	6441

Sum of Error fatal	
installed SW	Total
SDC old	3
SDC Rev14	1
SDC Rev14 (>1Y)	1
SDC Rev14 (<1Y)	0
XXW old	4
XXW P0	24
XXW P1	0
XXW P2	0
XXW P2 (>1Y)	0
XXW P2 (0.5...1Y)	0
XXW P3	0
error in production	0
other system than SDC XXW	1
System not supervised <1998	7
Grand Total	40

Sum of SW related fatal Error	
installed SW	Total
SDC old	0
SDC Rev14	0
SDC Rev14 (>1Y)	0
SDC Rev14 (<1Y)	0
XXW old	2
XXW P0	7
XXW P1	0
XXW P2	0
XXW P2 (>1Y)	0
XXW P2 (0.5...1Y)	0
XXW P3	0
error in production	0
other system than SDC XXW	0
System not supervised <1998	0
Grand Total	9

TUV Nord Certificate of Conformance of Gambit WXX Firmware Package 2 to IEC 60880-2



CERTIFICATE

Registered No.:

Reference of Applicant:

not applicable

Date of Application:

2007-02-13

File Reference:

CER

Test Report No.:

Bearer of Certificate:

Electronic Ltd

The bearer of certificate fulfils the requirements of the standard for the product, both named below. The specified documents have been presented to the certification body. The descriptions contained in these documents are corresponding with the product.

Product and Version:

Firmware Package 2

Tested in Accordance with:

IEC 60880-2

Software for computers important to safety for nuclear power plants – Software aspects of defence against common cause failure, use of software tools and of pre-developed software

- 4.1 Defences against common cause failure due to software
- 4.3 Qualification of pre-developed software

Validity of Certificate:

2010-03-31

2007-04-12

Dr.-Ing. G. Glöe

Town

Dated

Head of Certification Body

SEECERT Software & Electronics Certification Body

TÜV NORD SysTec GmbH & Co. KG, Grosse Bahnstrasse 31, 22525 Hamburg, Germany
 ☎ +49 40 8557 2583, ✉ +49 40 8557 2429, □ <http://www.tuv-nord.de/1238.asp>

Registration No. of Certification Body: DAT-ZE 012/00-10

Hints: This certificate is valid only for the above named bearer and the product indicated. Any modification intended or already made must be announced to the certification body.

Gambit Declaration of Conformity

DECLARATION OF CONFORMITY

We hereby declare that the equipment described below conforms to the relevant requirements of the applicable CSA standard(s).

This declaration shall cease to be valid if modifications are made to the equipment without our approval.

Product: **Uninterruptible Power Supply (UPS)**

Type: **[REDACTED]**

Serial number(s): **[REDACTED]**

We confirm that the equipment was designed, manufactured and tested according to the following International and Canadian standard(s) :

Uninterruptible Power Systems :	CSA C22.2 No. 107.3
Information Technology Equipment - Safety :	CSA 60950-1
Specialty Transformers :	CSA C22.2 No. 66
Power transformers :	IEC 60076


and conforms with the following requirements and specifications :

suitable for use with C22.1, Canadian Electrical Code Part I

Appendixes :

- Technical Report -
- CoC Power Transformers -

Electronic Ltd.


Gert Andersen
Quality Assurance


M. Dreier
Technology Manager

The signatories act on behalf of company management and with full power of attorney.



Certificate
for

Electronic Ltd

Bureau Veritas Quality International (BVQI)
hereby confirms that the management system of the above-mentioned
organisation has been assessed and complies with the requirements set out in the
following standards / regulations.

Standards/Regulations

SN EN ISO 9001 : 2000

The management system comprises:

**DEVELOPMENT, SALES, DESIGN, MANUFACTURE,
COMMISSIONING, MAINTENANCE AND REPAIR OF
UNINTERRUPTIBLE POWER SUPPLY SYSTEMS**

Date of initial certification: **16.09.1994 (BSI)**

The requirements of the standards / regulations must be complied with throughout the period of validity of this certificate.
This will be ensured through regular monitoring by BVQI.

Date of certification: **27.04.2005**

Valid until: **27.04.2008**

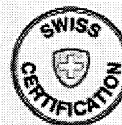
BVQI will provide information on the validity of this certificate on request at any time.

Additional information on the management system and the area of applicability should be obtained from the organisation itself.

Date: **03.05.2005**

Certificate number:

A handwritten signature in black ink, appearing to be 'J. L.', is written over a horizontal line.

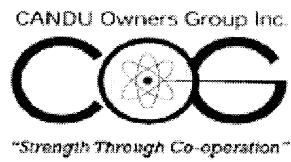


SCIS 003

Bureau Veritas Quality International (Switzerland) AG/SA
Vor Ort 25, CH-8104 Weiningen/Zürich

A.7

CANPAC Certificate of Conformance to CSA Z299.2



CANPAC

**Corrective Action Follow-up and Closure to
Audit # 7-041**

Electronics Ltd.

**This package contains:
7-041-C1**

Single UPS with Static Bypass

Mains MTBF

1000 Hours

$MTBF = \frac{1}{\lambda} \text{ h}$
Mean time between failures

$MTTR = \frac{1}{\mu} \text{ h}$
Mean time to repair

λ_i
Failure rate for a systempart

Component		$\lambda \text{ (h}^{-1}\text{)}$	MTBF (h)	MTTR (h)
Charger	λ_{GR}	1.00E-05	100000	51
Battery	λ_{BAT}	1.00E-05	100000	52
Inverter	λ_{INV}	1.25E-05	80000	52
Mains	λ_M	1.00E-03	1000	0.1
Static Transfer Switch EN	λ_{EN}	2.00E-06	500000	50
Common failure on safebus	λ_C	2.00E-07	5000000	49
Feeder	λ_F	7.66E-07	1305483	49

$MTBF_{UPS} = \frac{1}{\lambda_{GR} + \lambda_{BAT} + \lambda_{INV}}$

MTBF for UPS (Charger, Battery and Inverter)

30769 Hour

$MTTR_{UPS} = \frac{(\lambda_{GR} \cdot MTTR_{GR}) + (\lambda_{BAT} \cdot MTTR_{BAT}) + (\lambda_{INV} \cdot MTTR_{INV})}{\lambda_{GR} + \lambda_{BAT} + \lambda_{INV}}$

MTTR for UPS (Charger, Battery, Inverter and EA)

51.69 Hour

(Including 48 hours for shipping)

$MTBF_{Mains+EN} = \frac{1}{\lambda_{Mains} + \lambda_{EN}}$

MTBF for Bypass (Mains and EN)

998 Hour

$MTTR_{Mains+EN} = \frac{(\lambda_{Mains} \cdot MTTR_{Mains}) + (\lambda_{EN} \cdot MTTR_{EN})}{\lambda_{Mains} + \lambda_{EN}}$

MTTR for Bypass (Mains and EN)

0.20 Hour

$MTBF_{SYSTEM} = \frac{1}{((\lambda_{Mains+EN} \cdot MTTR_{Mains+EN})(\lambda_{UPS} \cdot MTTR_{UPS})(\frac{1}{MTTR_{Mains+EN}} + \frac{1}{MTTR_{UPS}})) + \lambda_C + \lambda_F}$

MTBF for System

43 Year

376526 Hours

Mains

Bypass

λ_{UPS}

λ_{M+EN}

λ_C

λ_F

Output

A.9**List of Reference Nuclear Power Plants**

Year	Project Name	End User Country
1992	Temelin	Czech Republic
1992	Beznau	Switzerland
1992	Muehleberg	Switzerland
1993	Temelin	Czech Republic
1995	Nuclear Design	China
1998	Dukovany	Czech Republic
1999	Kozloduy	Bulgaria
1999	Beznau	Switzerland
1999	FRM-II	Germany
2000	Heysham	United Kingdom
2000	Gosgen	Switzerland
2000	Ringhals	Sweden
2000	Qinghua	China
2000	Hifar	Australia
2000	Qinshan	China
2001	Qinshan	China
2001	Lianyungang / Tianwan	China
2002	Qinshan	China
2002	South Ukraine	Ukraine
2002	Beznau	Switzerland
2002	Rheinsberg	Germany
2002	Bruce Power Units 5 - 8	Canada
2003	Tarapur 3 & 4	India
2003	Bruce Power Units 3 & 4	Canada
2003	Gosgen	Switzerland
2003	Zaparozhe	Ukraine
2003	Rowno	Ukraine
2003	South Ukraine	Ukraine
2003	Lianyungang /Tianwan	China

Year	Project Name	End User Country
2003	MMIR Maple	Canada
2003	Heysham	United Kingdom
2003	Ignalina	Lithuania
2004	CEFR	China
2004	Torness	United Kingdom
2004	Kozloduy	Bulgaria
2004	Qinshan	China
2004	Gosgen	Switzerland
2004	CARR	China
2004	Callaway NPP	US
2004	Kudankulam	India
2004	Oskarshamn, BAMS	Sweden
2004	Cernavoda Unit 2	Romania
2005	DOE/Hanford Nuclear Waste	US
2005	Lungmen Nuclear	Taiwan
2005	Zaporozhe	Ukraine
2006	Chashma Unit 2	Pakistan
2006	Heysham	United Kingdom
2006	USEC Paducah	US
2006	USEC Portsmouth	US
2006	Zaporozhje	Ukraine
2006	Qinshan Phase II, Units 3&4	China
2006	Bruce Power Units 1 & 2	Canada
2006	Embalse	Argentina
2006	Forsmark Units 1-3	Sweden
2006	DOE / Hanford RPP/WPP	US
2006	Dungeness B	UK
2006	Qinshan Phase III	China
2006	Forsmark Unit 3	Sweden
2006	Zaporozhe	Ukraine
2006	Ringhals Unit 1	Sweden
2007	Kudankulam	India
2007	Point Lepreau Refurbishment	Canada
2007	MMIR Maple	Canada
2007	Leibstadt	Switzerland

A.10 Reference Site Questionnaire Form

A.10.1 UPS Data

1. What model of Gambit UPS system are you currently using?
2. What is the power rating of the UPS system?
3. What is the approximate total power consumption rating of the connected loads?
4. What is the software version of the UPS system (i.e., WXX firmware package 1, package 2, etc.)?
5. What is the intended purpose of the UPS system (i.e., provide uninterruptible power to loads, provide isolation between grid and load, etc.)?
6. Is the UPS system located in a harsh environment (i.e., high temperature, high humidity, radiation, etc.)?
7. How long have you been using the Gambit UPS system?

A.10.2 UPS Documentation

1. Were any issues ever encountered due to lack of the documentation provided by Gambit as part of the UPS system (i.e., maintenance issues, commissioning issues, installation issues, etc.)?

A.10.3 UPS Goodness of Design / Reliability

Have any failures ever been recorded for the UPS system? If yes,

1. What was the cause of the failure?
2. How long did it take to have it repaired?
3. Was the repair performed by a Gambit representative or was it done in-house?
4. Can you please provide an approximate history of the failures encountered by the UPS?

A.10.4 Applicability of the Data

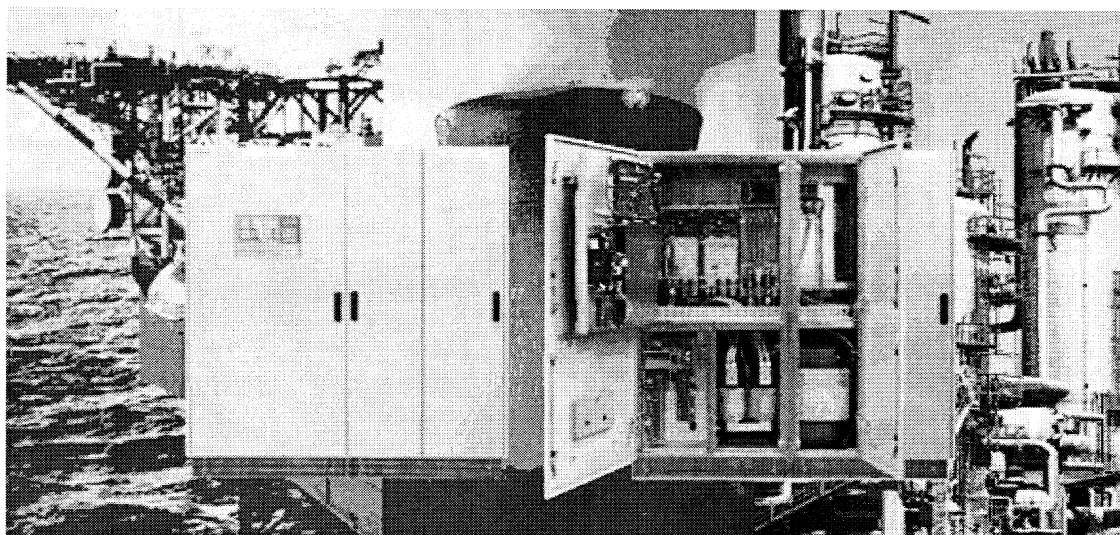
1. Is there a preventive maintenance program in place for the UPS system?
2. How often is the UPS system tested to detect any failures (i.e., monthly, annually, etc.)?
3. Were you requested by Gambit to report all failures / issues with the UPS?

A.10.5 Miscellaneous

1. Has Gambit ever been contacted regarding any after-sale issues (i.e., spare parts, maintenance issues, etc.)? If yes, how would you rate their service?
2. Overall, does Gambit UPS system meet the expected requirements in terms of reliability and user-safety?

A.11

WEP 1000 Technical Data Sheet



TECHNICAL DATA SHEET

AC UPS System [REDACTED] 5 - 200 kVA Single Phase

TECHNICAL DATA

UPS Input

Rectifier input voltage	3x380/400/415V
Tolerance	
- DC in tolerance	+/-10%
- for function	+10/-15%
Bypass input voltage	1x220/230/240V +/-10%
Frequency	50/60Hz +/-6%
Inrush current	<10x I _N (input current)

Intermediate DC Circuit

Voltage	110/125/220/400VDC
Rectifier voltage tolerance	+/-1% IU characteristic
Float voltage range at +/-10% mains	100 - 115% programmable
Boost voltage range at nominal mains	100 - 125% programmable
Boost charge time	1 - 24h programmable
Charging current limitation	depending on battery, programmable
Inverter input range	
- with output tolerance +/-1%	+20/-15%
Inverter maximum input range	
- with output tolerance +/-10%	typical +/-25%

UPS Output

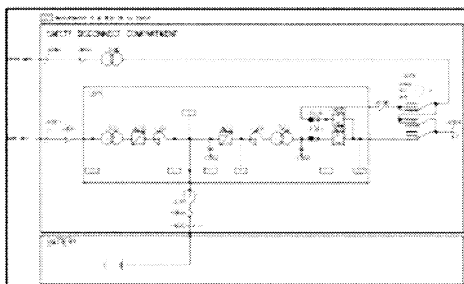
Nominal UPS rating	kVA at PF 0.8 lag
Voltage	1x220/230/240V
Voltage tolerance:	
- static within 0-100% load	+/-1%
- dynamic at 100% load surge	+/-4%
- regulation time	<25 ms
Overload	
- Inverter 1 min	150%
- Inverter 10 min	125%
- Bypass 100 ms	1000%
Short-circuit inverter 50 - 100ms	200%
Frequency	50/60 Hz
Frequency stability free running	<0.01%
Synchronization range	0.5%/2%/4%/6% programmable
Slewrate single unit	0.25/0.5%/2/4 Hz/s programmable
Slewrate redundant system	1.0 Hz/s
Wave form	sinusoidal
Output crest factor admissible	unlimited
Distortion factor:	
- Linear load	= <3%
- Non linear load according to IEC 62040-3	= <5%
Allowable power factor	0.4lag - 0.9 lead
Fault clearing capability	30% of UPS nom. current rated gG fuse (IEC 60269) within 10 ms and bypass available

General Data

Ambient temperature range for storage	from -20 to +70 °C
Ambient temperature range for operating	from -10 to +40 °C (100% nominal load)
Altitude above sea level	1000 m without load derating
Allowable air humidity	<95% (non condensing)
Noise level standard n=1 fan system	60 - 70 dBA depending on type
Noise level 100% redundant fans	65 - 75 dBA depending on type
Degree of protection	IP20 according to IEC 60529
Painting	pebble grey, RAL 7032 structured
Safety	IEC / EN 62040-1-2
EMC	IEC 62040-2, EN 50091-2
Performance	IEC / EN 62040-3
UPS Classification	VFI - S5 - 111 acc. to IEC 62040-3 (TUV approved)
Conformity	CE-Label
Efficiency	76-93% depending on type range
Cooling	forced ventilation with redundant n=1 monitored fans

Data subject to changes

Typical Single-Line Drawing



Battery Voltage & UPS Ratings

Voltage (VDC)	110	125	220	400
UPS Rating (kVA)	5	5	5	-
	10	10	10	-
	15	15	15	-
	20	20	20	-
	30	30	30	-
	40	40	40	-
	-	-	50	-
	-	-	60	-
	-	-	80	-
	-	-	100	-
	-	-	-	120
	-	-	-	150
-	-	-	200	

Higher ratings and other voltages on request

Standards

Single UPS

UPS output voltage 1x230V
 Rectifier input voltage 3x400V +10V-10%
 Bypass input voltage 1x230V +10V-10%
 Frequency 50Hz \pm 5%
 6 - pulse Rectifier with Isolation Transformer
 Rectifier standard size, for UPS A/C load
 - PFC 0.8 and up to 1h Battery autonomy
 Rectifier input switch
 Fixed charging voltage IU characteristic
 Power - Module for nominal rating
 Static switch EN (mainly side) with additional backfeed protection
 System front panel with additional LED's for direct alarm display
 LCD display unit with keyboard
 Alarm relays
 - Battery operation NC/NC
 - Common alarm 2x NC/NC
 Battery capacity test (full discharge with actual load)
 Bottom cable entry
 Earth terminal
 N+1 monitored two-speed fans
 Ambient temperature range from -10 to +40 °C
 Protection IP20
 Painting pebble grey, RAL 7032 structured

Options

Parallel redundant configuration
Other input voltages
Frequency 60Hz $\pm 1\%$
12-pulse Rectifier with Isolation Transformer
Larger Rectifier $-1 \text{ step} / -2 \text{ steps}$

- Rectifier fuse
- Bypass input switch
- Bypass input MOCB
- Rectifier input MOCB
- Sensor for temperature dependent battery charging voltage, recommended for sealed VRLA batteries and wide temperature range
- Battery temperature alarm
- Serial diode (for parallel Rectifiers)
- Diode for reverse polarity protection
- Rectifier output isolator
- Rectifier output circuit breaker
- Battery fuse in UPS
- Battery fuse box
- Battery MOCB in UPS
- Battery MOCB box
- Inverter input Isolator
- Inverter input circuit breaker
- Larger Inverter Power Module - 1 step* 1 - 2 steps*
- Static Switch EA (Inverter side)
- Manual Bypass 3 pos in UPS
- Battery Monitor (programmable battery data)
- Battery asymmetry supervision
- DC earth fault alarm
- AC earth fault alarm
- RS 232 Interface (event log download)
- RS 485 Interface
- RJ 45 Ethernet port for WEB browser based monitoring
- RS 485 MODBUS Protocol (slave)
- External time synchronisation
- Top cable entry
- Top & bottom cable entry
- Space heaters
- Ventilation 100% redundant
- Panel lighting
- Ambient temperature maximum +55 °C
- Allowable altitude < 4000 m above sea level
- Protection up to IP52
- Air filters at air inlet
- Other colours
- Bypass isolation transformer
- Bypass stabilizer with isolation transformer
- * within type range

Additional analogue meters 96x96 cl. 1.5

- Set with VM DC, AM Bat & output FM, VM & AM
- Set with input VM & AM with select switch
- kW of output
- Power factor

Relay board A077, 16 failsafe NO/NC contacts:

- Rectifier mains fault
- DC out of tolerance
- Rectifier fuse blown
- Battery discharged
- Earth fault DC
- 6x options
- Inverter fuse blown
- Bypass mains fault
- Overtemperature
- Fan failure
- Power supply unit fault

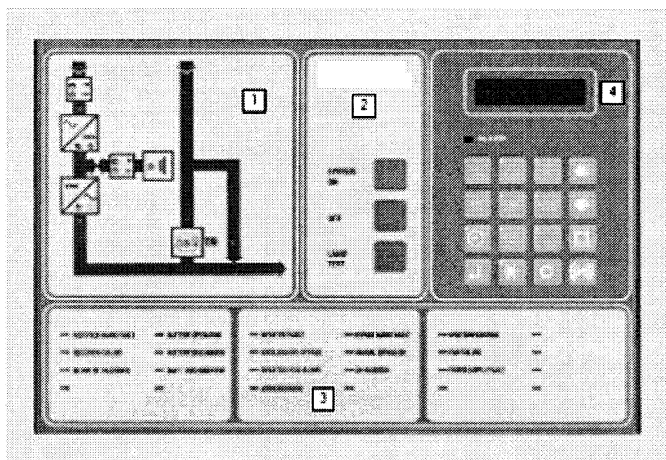
Relay board A078, 16 failsafe NO/NC contacts:

- EA inhibited
- EN inhibited
- Manual Bypass ON
- Asynchronous
- Overload Inverter / Bypass
- Inverter fault
- Battery disconnected
- Battery operation
- Rectifier failure
- EN ON
- EA ON
- Inverter ON
- Boost charge
- Rectifier ON
- External horn

Additional options are available on request

MAN-MACHINE INTERFACE (FRONT PANEL)

The front panel which is identical for both AC and DC Systems facilitates a comprehensive and flexible man-machine interface. It is divided into four sections:



- 1.) The system panel shows the system's current operation status, meaning which system part is supplying the load at the moment and which is in stand-by mode. LED's also indicate possible faults.
- 2.) Operations for turning on and off the system and a lamp test button for checking if all LED indications function properly.
- 3.) On the alarm indication panel the respective LED lights up, after an alarm has occurred.
- 4.) The display unit consist of a LC display, an alarm LED, an acoustic alarm and a key-pad. With this the user can set following operational parameters, obtain a list of measurement data, and get access to the event and alarm log.

Operational parameters

- Selectable second display language
- Autostart
- Bypass operation
- Boost charge
- Auto boost (charge)
- Battery capacity test
- Battery monitor test (optional)
- Set date / time

Measurements

- Load in % of nominal kVA rating
- AC rectifier mains 1 voltage and current
- AC bypass mains 2 voltage
- DC total current, battery voltage and current
- Battery temperature (with optional sensor)
- AC inverter current
- AC output voltage, current and frequency
- AC output peak current
- Time left in battery operation with actual load (optional with programmed battery data)
- Event log with date and time (change in operating mode and alarm)

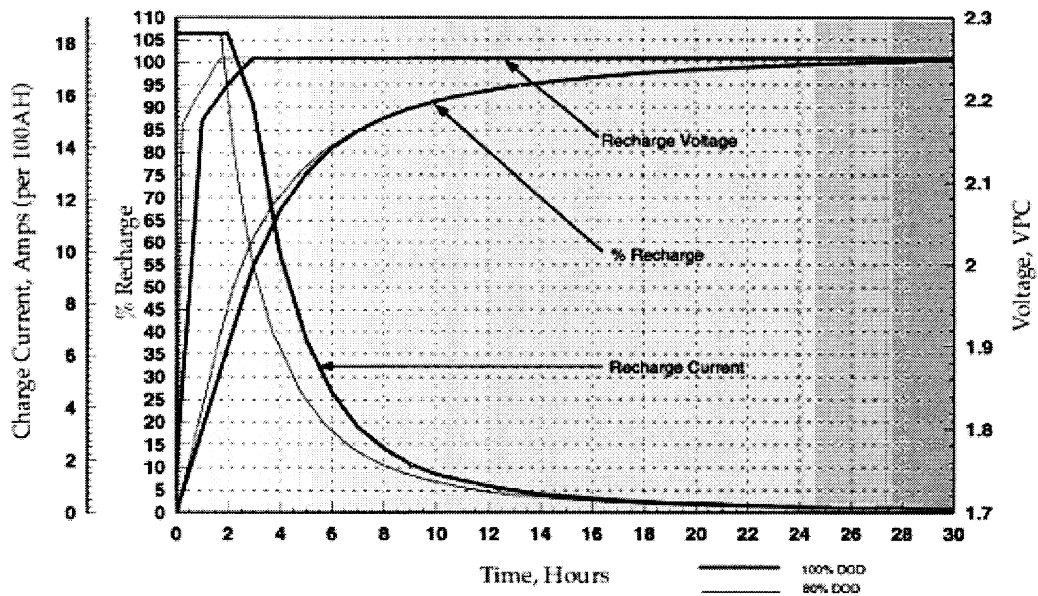
A.12

Batteries Recharge Characteristic Curve

Page 17

Recharge Characteristics @25°C (77°F)

50A/90A/100A Series 2.25 Volts Per Cell Float



A.13 Qualification Assessment Plan and Preliminary Assessment Evidence

Application Specific Qualification Method	Method Recommended for Class 2 / Category B	Quality Objectives							Applicable	Notes
		Safety	Functionality	Performance	Reliability	Maintainability	Testability	Security		
Method 1: Qualification Feasibility Assessment	R	✓	✓	✓	✓	✓	✓	✓	No	An initial qualification feasibility assessment was done in bid evaluation document [15]
Method 2: Assessment of Product Specifications (hardware and software tools)	R	✓	✓	✓	✓	✓	✓	✓	Yes	
Method 3: Proven in Use Assessment										
a) Operating History Data	R	✓	✓	✓	✓				Yes	
b) Failure Data Assessment	R	✓	✓	✓	✓				Yes	
c) Product Design Revision History Assessment	AA			✓	✓	✓			Yes	
d) Reference Site Assessments	AA	✓	✓	✓	✓	✓		✓	Yes	
Method 4: Maintenance Assessment										
a) In-Service Maintenance Process Assessment	R	✓	✓			✓	✓	✓	Yes	

Application Specific Qualification Method	Method Recommended for Class 2 / Category B	Quality Objectives							Applicable	Notes
		Safety	Functionality	Performance	Reliability	Maintainability	Testability	Security		
b) In-Service Testability Assessment	AA	✓	✓	✓	✓	✓	✓	✓	Yes	
Method 5: Hardware Design Assessment										
a) Environmental Tolerance Assessment	R			✓	✓				Yes	
b) Electromagnetic Immunity and Emission Assessment	R			✓	✓				Yes	
c) Seismic Tolerance Assessment	AA			✓	✓				Yes	
d) Hardware Reliability, Failure Modes and Diagnostic Assessment	R	✓	✓	✓	✓				Yes	
e) Assessment of Hardware Useful Life	R			✓	✓	✓			Yes	
Method 6: Hardware Development Process Assessment										
a) Assessment of Hardware Testing Techniques	AA	✓	✓	✓	✓		✓	✓	No	Vendor is registered to ISO 9001 standards. In addition, Gambit submitted a copy of Inspection and Test Plan (ITP) and Factory Acceptance Testing to AECL, prior to commencement of hardware testing.

Application Specific Qualification Method	Method Recommended for Class 2 / Category B	Quality Objectives							Applicable	Notes
		Safety	Functionality	Performance	Reliability	Maintainability	Testability	Security		
b) Hardware Design Process Assessment	AA	✓	✓		✓	✓		✓	No	Vendor is registered to ISO 9001 standards.
c) Product Manufacturing Process Methods and QA Assessment	AA				✓				No	Vendor is registered to ISO 9001 standards.
Method 7: Software Design Assessment										
a) Software Safety Impact Assessment	R	✓	✓					✓	No	The intent of this method was met via TUV Nord assessment and subsequent certification of Gambit WXX Firmware Package 2 to IEC 60880-2. [14] In addition, Gambit is registered to ISO 9001:2000 standard.
b) Assessment of Software Diagnostics and Self-Check Capability	R	✓	✓	✓	✓		✓		No	The intent of this method was met via TUV Nord assessment and subsequent certification of Gambit WXX Firmware Package 2 to IEC 60880-2. [14] In addition, Gambit is registered to ISO 9001:2000 standard.
c) Assessment of Software Goodness of Design	AA	✓			✓	✓		✓	No	The intent of this method was met via TUV Nord assessment and subsequent certification of Gambit WXX Firmware Package 2 to IEC 60880-2. [14] In addition, Gambit is registered to ISO 9001:2000 standard.
d) Software HAZOP	AA	✓	✓		✓	✓			No	The intent of this method was met via TUV Nord assessment and subsequent certification of Gambit WXX Firmware Package 2 to IEC 60880-2. [14] In addition, Gambit is registered to ISO 9001:2000 standard.
Method 8: Software Development Process Assessment										
a) Assessment of Software Design-Implementation Processes	AA	✓		✓	✓	✓		✓	No	The intent of this method was met via TUV Nord assessment and subsequent certification of Gambit WXX Firmware Package 2 to IEC 60880-2. [14] In addition, Gambit is registered to ISO 9001:2000 standard.
b) Assessment of Software Testing Techniques	AA	✓	✓	✓	✓	✓	✓	✓	No	The intent of this method was met via TUV Nord assessment and subsequent

Application Specific Qualification Method	Quality Objectives							Notes
	Method Recommended for Class 2 / Category B							
	Applicable							
	Safety	Functionality	Performance	Reliability	Maintainability	Testability	Security	
				✓	✓			
				✓				
						✓		
c) Assessment of Software Configuration Management Process			R				The intent of this method was met via TUV Nord assessment and subsequent certification of Gambit WXX Firmware Package 2 to IEC 60880-2. [14] In addition, Gambit is registered to ISO 9001:2000 standard.	
d) Software Support and Support-life Assessment			R				The intent of this method was met via TUV Nord assessment and subsequent certification of Gambit WXX Firmware Package 2 to IEC 60880-2. [14] In addition, Gambit is registered to ISO 9001:2000 standard.	

Application Specific Qualification Method	Method Recommended for Class 2 / Category B	Quality Objectives							Applicable	Notes		
		Safety	Functionality	Performance	Reliability	Maintainability	Testability	Security				
		Method 9: Evidence from 3rd Party Certifications and Assessments										
		a) Assessment of 3rd Party Corporate Quality System Certifications	AA				✓	✓	✓			Yes
		b) Assessment of 3rd Party Product Safety Certifications	R	✓	✓		✓	✓	✓		Yes	
		c) Assessment of 3rd Party Hardware Test Standards Compliance	R			✓	✓		✓		Yes	
		d) Assessment of 3rd Party Software Development Process Certifications	AA	✓			✓				Yes	
		Method 10: Limited Product Modifications	AA	✓	✓	✓	✓	✓	✓		No	No modifications will be done to the UPSs.
		Method 11: Complementary Testing	AA	✓	✓	✓	✓	✓	✓		No	Through application of other methods, correctness of design purchased Gambit UPS systems was demonstrated and thus no complimentary testing required.

