System Safety Inc.
Safety Livecycle Services

VERIFICATION REPORT
EN 60601-1-4 + A1

Medical electrical equipment

Part 1: General requirements for safety

Sub-Part 4. Collateral Standard: Programmable electrical medical systems

Report Reference No	20000710
Compiled by (+ signature)	Markus Weber
Reviewed by (+ signature)	
Approved by (+ signature)	
Date of issue	
Verification laboratory	System Safety, Inc.
Address	5150 Corte Playa Catalina
	San Diego, CA 92124-1558
Verification location	
Applicant	
Address	
Standard	EN 60601-1-4:1996 + A1: 2000
Test Report Form No	03092000
Test procedure	MDD Compliance
Procedure deviation	None
Non-standard test method	None
Type of end product	
End product Trademark	
End product Model and/or type reference	
End product Manufacturer	
End product Address	See above
End product Rating(s)	

PEMS/PESS Configuration Information:	No special hardware configuration necessary.
Software Designer (if different than end Product manufacturer).	NA
Address	NA
	NA
Method of Identification of Software:	Revision
Particular Risks Addressed by Software:	As contained in hazard analyses

GENERAL INFORMATION
Particulars: verification item vs. verification requirements As EN 60601-1-4 is a collateral standard to EN 60601-1, this report is to be used in conjunction with Test Report Reference No.: N.N.
Possible verification case verdicts Verification case does not apply to the verification item ---------- : N(ot)/A(pplicable) Verification item is available ---------- : N(oted) Verification item does meet the requirement ---------- : P(ass) Verification item does meet the requirement under the limited scope of this assessment ------- : P(ass) L(imited Scope) Verification item does not meet the requirement ---------- : F(ail) Verification item does not meet the requirement under the limited scope of this assessment -- : F(ail) L(imited Scope) Minor non-compliances are noted in regular case and font Major non-compliances are note in **ALL CAPS** and / or **BOLD**
General remarks
‘’(See enclosure #)" refers to an enclosure appended to this report. "(See appended table)" refers to a table appended to the report. Throughout this report a period is used as the decimal separator. The verification results presented in this report relate only to the item being verified. This verification report shall not be reproduced except in full without the written approval of the verification laboratory.
SUMMARY OF CONTENTS:
The equipment has been evaluated according to standard EN 60601-1-4 (1996) First Edition including Amendment 1 (2000) All applicable verifications according to the above-specified standard(s) have been carried out, however the scope was limited to sub-system evaluation. These verifications fulfil the requirements of standard EN 45001.

Note: As per EN 60601-1-4, determination of compliance is by inspection and audit, the attachments should be documents or parts of documents.

Acronyms and Abbreviations:

COTS	Commercial of the shelf software
DFU	Directions for Use
H&RA	Hazard and Risk Analysis
MDD	European Medical Device Directive
PEMS	Programmable Electronic Medical Devices
RMP	Risk Management Plan
SOP	Standard Operating Procedure
V&V	Verification and Validation

Results and Conclusions:

Clause	Requirement	Result- Remark	Verdict
6	**IDENTIFICATION, MARKING AND DOCUMENTS**		
6.8	**ACCOMPANYING DOCUMENTS**		
6.8.201	All relevant information regarding significant RESIDUAL RISK including descriptions of the HAZARDS and any actions by the OPERATOR or the USER necessary to avoid/mitigate them shall be placed in both the INSTRUCTIONS FOR USE and the RISK MANAGEMENT FILE.		
6.8.202	ACCOMPANYING DOCUMENTS for the PEMS shall identify, as a minimum, the MANUFACTURER and a unique identifier such as revision level and date of release/issue. NOTE – Information pertaining to any specific EQUIPMENT that software is intended to be used in conjunction with, and a means by which the MANUFACTURER can be contacted, can be located on the package or in the INSTRUCTIONS FOR USE so that it is available to the USER independently of the software operation.		
52	**ABNORMAL OPERATION AND FAULT CONDITIONS**		
52.201	**Documentation**		
52.201.1	Documents produced from application of this standard are maintained and are part of the quality records; see figure 201. This should be done in accordance with 6.3 of ISO 9000-3	(See appended table)	
52.201.2	These documents, herein referred to as the RISK MANAGEMENT FILE, are approved, issued and changed in accordance with a formal configuration management system. This should be done in accordance with 6.2 of ISO 9000-3.		
52.201.3	A RISK MANAGEMENT SUMMARY is developed throughout the DEVELOPMENT LIFE-CYCLE as part of the RISK MANAGEMENT FILE. It contains:		
	Identified HAZARDS and their initiating causes;	(See 52.204.3.1.10)	
	Estimation of RISK	(See 52.204.3.2.5)	
	Reference to the SAFETY measures, used to eliminate or control the RISK of the HAZARD	(See 52.204.4.5)	
	Evaluation of effectiveness of RISK control;	(See 52.204.4.6)	
	Reference to VERIFICATION	(See 52.209.3)	
52.202	**RISK management plan**		
52.202.1	The manufacturer has prepared a RISK management plan.		
52.202.2	The plan includes the following:		
	a) Scope of the plan, defining the project or product and the DEVELOPMENT LIFE-CYCLE phases for which the plan is applicable;		
	b) The DEVELOPMENT LIFE-CYCLE to be applied (see 52.203), including a VERIFICATION plan and a VALIDATION plan;		
	c) Management responsibilities in accordance with 4.1 of ISO 9001;		
	d) RISK management process;		
	e) Requirements for reviews.		
52.202.3	If the plan changes during the course of development, a record of the changes is kept.		

Clause	Requirement	Result- Remark	Verdict
52.203	**DEVELOPMENT LIFE-CYCLE**		
52.203.1	A DEVELOPMENT LIFE-CYCLE is defined for the design and development of the PEMS		
52.203.2	The DEVELOPMENT LIFE-CYCLE is divided into phases and tasks, with a well-defined input, output and activity for each.		
52.203.3	The DEVELOPMENT LIFE-CYCLE includes integral processes for RISK management.		
52.203.4	The DEVELOPMENT LIFE-CYCLE includes documentation requirements.		
52.203.5	RISK management activities have been applied throughout the DEVELOPMENT LIFE-CYCLE as appropriate: see 52.204.		
52.203.6	Where appropriate, a defined system for problem resolution within and between all phases and tasks of the DEVELOPMENT LIFE CYCLE shall be developed and maintained as a part of the RISK MANAGEMENT FILE. Depending upon the problem, the system may have the following characteristics:		
	a) Be defined as a part of the DEVELOPMENT LIFE- CYCLE		
	b) Allow the reporting of potential or existing SAFETY problems		
	c) Include an assessment of each problem for associated RISKS		
	d) Identify the criteria (SAFETY and/or performance) that have to be met for the issue to be closed		
	e) Identify the action to be taken to resolve each problem		
	f) Identify VALIDATION methods for each action		
	g) Identify the steps taken for VERIFICATION of continuing compliance		
52.204	**RISK management process**		
52.204.1	A RISK management process is used that has the following elements: RISK analysis; RISK control.		
52.204.2	The process is applied throughout the DEVELOPMENT LIFE-CYCLE		

Clause	Requirement	Result- Remark	Verdict
52.204.3	**RISK analysis**		
52.204.3.1	**HAZARD analysis**		
52.204.3.1.1	HAZARD identification is carried out as defined in the RISK management plan: see 52.202.		
52.204.3.1.2	HAZARDS are identified for all reasonably foreseeable circumstances including: NORMAL USE; incorrect use.		
52.204.3.1.3	The HAZARDS considered include, as appropriate:		
	a) HAZARDS to PATIENTS		
	b) HAZARDS to OPERATORS		
	c) HAZARDS to service personnel		
	d) HAZARDS to bystanders		
	e) HAZARDS to the environment		
52.204.3.1.4	Reasonably foreseeable sequences of events, which may result in a HAZARD, are considered.		
52.204.3.1.5	Initiating causes considered include, as appropriate:		
	a) Human factors including ergonomic limitations		
	b) Hardware faults		
	c) Software faults		
	d) Integration errors		
	e) Environmental conditions		
52.204.3.1.6	Matters considered include, as appropriate:		
	a) Compatibility of system components, including hardware and software		
	b) User interface, including command language, Warning and error messages		
	c) Accuracy of translation of text used in the user interface and INSTRUCTIONS FOR USE		
	d) Data protection from human intentional or unintentional causes		
	e) RISK /benefit criteria		
	f) Third party software		
52.204.3.1.7	HAZARD identification methods appropriate to the DEVELOPMENT LIFE-CYCLE phase are used.		
52.204.3.1.8	The methods used (e.g. fault tree analysis, failure modes and effects analysis) are documented in the RISK MANAGEMENT FILE		
52.204.3.1.9	The results of the application of the methods are documented in the RISK MANAGEMENT FILE.		
52.204.3.1.10	Each identified HAZARD and its initiating causes are recorded in the RISK MANAGEMENT SUMMARY		
52.204.3.2	**RISK estimation**		
52.204.3.2.1	For each identified HAZARD the RISK is estimated.		
52.204.3.2.2	The estimation of the RISK is based on an estimation of the likelihood of each HAZARD and/or the SEVERITY of the consequences of each HAZARD.		
52.204.3.2.3	Recorded in the RISK MANAGEMENT FILE.		
52.204.3.2.4	The likelihood estimation method is either quantitative or qualitative and is recorded in the RISK MANAGEMENT FILE.		
52.204.3.2.5	The estimated RISK is recorded against each HAZARD in the RISK MANAGEMENT SUMMARY.		

Clause	Requirement	Result- Remark	Verdict
52.204.4	**RISK control**		
52.204.4.1	RISK is controlled so that the estimated RISK of each identified HAZARD is made acceptable.		
52.204.4.2	A RISK is acceptable if the RISK is less than or equal to the MAXIMUM TOLERABLE RISK and the RISK is made as low as reasonably practicable		
52.204.4.3	Methods of risk control reduce the likelihood of the hazard or reduce the severity of the hazard or both. The likelihood that the means for RISK reduction will perform correctly shall be specified quantitatively or qualitatively		
52.204.4.4	Risk control methods are directed at the cause of the hazard (e.g. by reducing its likelihood) or by introducing protective measures which operate when the cause of the hazard is present, or both, using the following priority:		
	a) Inherent safe design		
	b) Protective measures including alarms		
	c) Adequate user information on the residual risk		
52.204.4.5	The requirement(s) to control the RISK is documented in the RISK MANAGEMENT SUMMARY (directly or as a cross-reference).		
52.204.4.6	An evaluation of the effectiveness of the RISK controls is recorded in the RISK MANAGEMENT SUMMARY.		
52.205	**Qualification of personnel**		
	The design and modification of a PEMS is considered as an assigned task in accordance with 4.18 of ISO 9001.		
52.206	**Requirement specification**		
52.206.1	For the PEMS and each of its subsystems (e.g. for a PESS) there is a requirement specification.		
52.206.2	The requirement specification details the functions that are RISK-related. This includes functions that control RISKS arising from:		
	a) Causes arising from environmental conditions;		
	b) Causes elsewhere in the PEMS;		
	c) Possible malfunctions.	(See 52.204.3.1.8)	
52.206.3	The requirement specification shall include the information necessary to assure that RISK control measures satisfactorily reduce the identified RISKS		
52.207	**Architecture**		
52.207.1	The architecture satisfies the requirement specification.		
52.207.2	For the PEMS and each of its subsystems, an architecture is specified.		
52.207.3	Where appropriate, the architecture specification of a PEMS and its subsystems shall address the RISK CONTROL requirements by reducing the corresponding likelihood of the HAZARD or by reducing the SEVERITY of the HAZARD or both		

Clause	Requirement	Result- Remark	Verdict
	Allocation Of RISK control measures to subsystems and components of the PEMS-,		
	a) Redundancy;		
	b) Diversity;		
	c) Failure rates and modes of components;	(See 52.204.3.1.8)	
	d) Diagnostic coverage:		
	e) Common cause failures:		
	f) Systematic failures:		
	g) Test interval and duration;		
	h) Maintainability;		
	i) Protection from human intentional or unintentional causes.		
52.207.4	Where appropriate, to reduce the likelihood of the HAZARD, the architecture specification shall make use of		
	a) Highly reliable components		
	b) Fail-safe functions		
	c) Redundancy		
	d) Diversity		
	e) Defensive design		
	f) Limits on potentially hazardous effects, for example by restricting the available output power and/or by introducing means to limit the travel of actuators		
52.207.5	The architecture specification shall take into consideration		
	a) Allocation of risk control measures to subsystems and components of the PEMS NOTE – Subsystems and components include sensors, actuators, PESS and interfaces.		
	b) Failure modes of components and their effects		
	c) Common cause failures		
	d) Systematic failures		
	e) Test interval, test duration and diagnostic coverage		
	f) Maintainability		
	g) Protection from human intentional or unintentional causes		

Clause	Requirement	Result- Remark	Verdict
52.208	**Design and implementation**		
52.208.1	Where appropriate, the design is decomposed into subsys-tems, each having a design and test specification.		
52.208.2	Requirements for the design environment shall be included in the risk management file		
	a) Software development methods;		
	b) Electronic hardware;		
	c) Computer aided software engineering (CASE) tools		
	d) Sensors		
	e) Actuators;		
	f) Human-PEMS interface;		
	g) Energy sources;		
	h) Environmental conditions;		
	i) Programming language.		
	j) Third party software.		
52.209	**VERIFICATION**		
52.209.1	VERIFICATION of the implementation of SAFETY require-ments is carried out.		
52.209.2	A VERIFICATION plan shall be produced to show how the SAFETY requirements at each DEVELOPMENT LIFE-CYCLE NOTE – Examples of methods and techniques are: • Walkthroughs and inspections; • Static/dynamic analyses; • White/black box testing.		
	a) The selection and documentation of VERIFICATION strate-gies, activities and techniques		
	b) The selection and utilization of verification tools		
	c) Coverage criteria for verification		
52.209.3	The verification shall be performed according to the verifica-tion plan. The results of the verification activities shall be doc-umented, analysed and assessed		
52.209.4	A reference to the methods, techniques and results of the veri-fication shall be included in the risk management summary		
52.210	**VALIDATION**		
52.210.1	Validation of the safety of PEMS under the conditions of the intended use shall be carried out		
52.210.2	A VALIDATION plan is produced to show that correct SAFETY requirements have been implemented.		
52.210.3	The VALIDATION shall be performed according to the VALIDATION plan. The results of VALIDATION activities shall be documented, analysed and assessed		
52.210.4	The leader of the team carrying out the VALIDATION is inde-pendent of the design team.		
52.210.5	All professional relationships of the members of the VALIDATION team with members of the design team are doc-umented in the RISK MANAGEMENT FILE.		
52.210.6	The design team shall not solely be responsible for the VALIDATION.		
52.210.7	A reference to the methods and results of the VALIDATION is included in the RISK MANAGEMENT FILE		

Clause	Requirement	Result- Remark	Verdict
52.211	**Modification**		
52.211.1	If any or all of a design results from a modification of an earlier design then either all of this standard applies as if it were a new design or the continued validity of any previous design documentation is assessed under a modification/change procedure.		
52.211.2	All relevant documents in the DEVELOPMENT LIFE-CYCLE are revised, amended, reviewed, approved under a document control scheme in accordance with 4.5.2 of ISO 9001 or equivalent	(See 52.2Q1.2)	

System Safety Inc.
Safety Livecycle Services

Mapping of Required Evidence and Client Documents

Standard Clause	Deliverables	Title	Revi-vi-sion	Date
6.8.201	Instructions for Use			
6.8.201	Statements of Residual Risk			
52.201.1	Quality Record Procedures			
52.201.2	Document Control/Configuration Manage-ment Procedures			
52.201.3	Risk Management Summary			
52.202.1	Risk Management Plan			
52.202.2c	Statement of Quality Policy			
52.202.2c	Definition of Responsibility and Authority for all Development Personnel			
52.202.2c	Identification of Verification Resources and Personnel			
52.202.2c	Identification of Management Representative			
52.202.2c	Records of Management Review			
52.203.1	Life-cycle Definition			
52.204.3.1	Hazard Analysis Procedures			
52.204.3.1.8	Hazard Identification Methods			
52.204.3.1.9	Record of Results of Hazard Identification Methods			
52.204.3.1.10	Hazard List and Initiating Causes			
52.204.3.2	Risk Estimation Procedures			
52.204.3.2.3	Severity Categorization Methods			
52.204.3.2.4	Likelihood Estimation Methods			
52.204.3.2.5	Record of Estimated Risk for each Hazard			
52.204.4	Risk Control Procedures			
52.204.4.5	Risk Control Method for each Hazard			
52.204.4.6	Record of Estimation for the Effectiveness of each Risk Control Method			
52.205	Training Procedures			
52.205	Training Records			
52.206.1	PEMS Requirements Specification			
52.206.1	Subsystems Requirements Specification			
52.207.2	PEMS Architecture Specification			
52.207.2	Subsystems Architecture Specification			
52.208.1	Design Specification			
52.208.1	Test Specification			
52.208.2 c,f,j,k	Requirements Specification for CASE Tools, Human-PEMS Interface, Programming Lan-guages and Third Party Software			
52.209.2	Verification Plan			
52.209.3	Verification Methods and Results for each Hazard			
52.210.2	Validation Plan			
52.210.6	Validation Methods and Results for each Hazard			
52.211.1	Modification/Change Procedures			

Standard Clause	Deliverables	Title	Revi-vi-sion	Date
52.212.1	Assessment Report			