Vantage Risk Analysis

Revision E May 29, 2018

Table of Contents

11335 NE 122nd Way, Suite 100
Kirkland, WA 98034 USA
www.verasonics.com

REVISION HISTORY

Issue Date	Summary	Sections Revised	Revision Level	Issued
22 Oct. 2013	Initial Version	All	A	Ken Linkhart
4 Nov. 2013	Incorporate results of Risk Analysis Review held Oct. 31, 2013.	All	B	Ken Linkhart
9 Feb 2014	add UI.UE.7 that was omitted in Nov. 4, 2013 updates	Listing of Identified Hazards	C	Ken Linkhart
23 Aug 2016	Increase scope to include HIFU and Extended Transmit functionality, and expanded/clarified coverage of use on human subjects	All	D	Ken Linkhart
7 Sep 2016	Incorporate changes listed in Aug. 24, 2016 review minutes.			
28 Feb 2018	See rev E change summary below	H.AP.1; H.AP.4 & H.AP.5	E	Ken Linkhart

Revision E

"I have reviewed this document and agree with the information contained herein."

	Signature	Name	Date
Prepared		Ken Linkhart	
Reviewed			

Revision E change summary:

- RC.AP.1A revised to add user-programmable SW watchdog timeout interval.
- H.AP.4 updated to clarify potential HW watchdog schemes using either the 'sync' command or synchronous receive data DMA transfers.
- RC.AP.4 New risk control measure definition, and software release verification testing requirement for the mechanisms to implement HW watchdog functionality.
- UI.AP.4 Clarification of user documentation requirements to explain all possible mechanisms for implementing a HW watchdog function and the potential hazards if this is not done.
- New entries H.AP.5 and RC.AP.5 identified hazard and risk control for the situation where a SW fault leads to an excessive transmit voltage command while the system is running.

SCOPE

This document provides the results of the Risk Analysis for the Verasonics "Vantage" VDAS system product line, in accordance with the requirements of the Verasonics Risk Management Plan. This Risk Analysis covers all potential hazards identified by Verasonics that could lead to harm to either a human subject or the operator of a Vantage system, when used within the intended use statement and other guidelines given below.

The ISO Standard #14971 "Application of risk management to medical devices" (corrected version of the second edition, 2007-10-01) has been used as the basis for the content of this document and will hereafter be referenced as ISO 14971.

The current Revision E of this document applies to Vantage Software release 3.4.2 and any subsequent releases; the earlier revision D of the Vantage Risk Analysis applies to Vantage Software Releases 3.1 through 3.4.1.

VERASONICS' RESPONSIBILITIES versus USER'S RESPONSIBILITIES

This document only covers potential hazards that are specific to the Vantage system by itself, as provided by Verasonics. It is the user's responsibility to conduct a risk analysis of their overall investigational device based on the Vantage system, identify potential hazards, and appropriate risk control actions. Note that in many cases the user will have added probes, their own application level SW or acquisition scripts, other new features or accessories, or even modifications to the Vantage system itself. Any such additions or modifications are not covered by this document, and it is the user's responsibility to evaluate these changes both to determine if new potential hazards have been added and if any of the risk control measures provided by Verasonics have been compromised.

For the hazards identified in this document, any listed risk control item that has been identified as either "inherent safety by design" or a "risk control measure" represents an action Verasonics has taken within the design of the Vantage system, and for which Verasonics assumes responsibility for formal Verification testing. Where the risk control option is listed as "user information", it is the user's responsibility to act on that information and implement any protective measures or other responses as they determine. Verasonics assumes no responsibility for those risk controls, beyond actually providing the identified "user information" to the user.

INTENDED USE

This section addresses the requirements of ISO 14971 ¶4.2.

The devices covered by this risk analysis are the Vantage system products in released product configurations as provided by Verasonics, including any of the optional features or accessories available from Verasonics as part of the released system.

Vantage System Definition: Within the context of this revision of the risk analysis, the term "Vantage System" includes all of the following components:

- Vantage 32 LE, Vantage 64, Vantage 64 LE, Vantage 128, or Vantage 256 HW system in *Standard Frequency, High Frequency*, or *Low Frequency* configuration with or without the UTA probe connector interface feature or the *Arbwave Transmit*, *Extended Transmit*, or *HIFU* options.
- Released Vantage SW package at level 3.4.2 or later, including FPGA code for the HW, drivers, HAL SW, application-level SW and utilities, and with or without any of the available SW-licensed optional features.
- Host Computer, either as provided and configured by Verasonics or an equivalent computer provided by the customer meeting the minimum requirements given in the Vantage User Manual for the specific Vantage SW release being used.
- Operating System installed on the Host Computer, at a compatible release level as listed in the Vantage User Manual for the specific Vantage SW release being used.
- Matlab application software plus the Signal Processing Toolbox, at a compatible release level as listed in the Vantage User Manual for the specific Vantage SW release being used.
- Ultrasound transducer(s) appropriate for the intended application. Transducers may be purchased through Verasonics, or purchased by the customer from other commercial suppliers, or custom-built by the customer.

The Vantage system, as designed, built, and provided by Verasonics, is intended to serve a very broad range of markets and applications with the primary emphasis on use as a research and development tool, but also supporting use as an investigational device or an early prototype of a commercial product, or as a component within a full production release of a commercial product. From the standpoint of the risk analysis and associated regulatory / safety concerns, this broad range of applications can be subdivided into three different categories of "Intended Use" as defined below.

1. Uses without Human Subject Exposure

The Vantage system can be used as a research and development tool for a broad range of ultrasound applications, including non-medical applications such as non-destructive materials testing as well as both diagnostic and therapeutic medical applications, but in a laboratory environment that does not involve live human (or animal) subjects. In this context, potential hazards apply only to the operator of the system and to environmental emissions (EMC, heat, fumes, disposal, etc.). The scope of the Vantage Risk Analysis is intended to fully cover all potential hazards Verasonics has identified for this category of use. Vantage systems built after September 2015 and using SW releases 2.11 or later are certified to fully comply with the following international regulatory standards for laboratory test equipment:

· IEC 61010-1 3rd Edition (2010) and EN 61010-1:2010 3rd Edition
· UL 61010-1: 2012 and CAN/CSA-22.2 No. 61010-1-12

Testing and certification to the 61010 standards was done for Verasonics by TUV Rhineland, and is documented in their report # 31581407.001 dated May 29, 2015. This testing was done using the Vantage 2.10 SW release, covering all Vantage HW configurations supported by that release.

Note that as new configurations are added to the Vantage product line, full testing for conformance to the 61010 standards may occur at different times for each configuration. Look for the conformance sticker on the rear of the system chassis, to determine whether that particular system has met the standards.

2. Use as an Investigational Device with Human Subjects

In some cases, a Verasonics customer may use the Vantage system to create an investigational medical device for use on human subjects, either as part of a research project or as a prototype of a commercial medical device they are developing. The scope of this Risk Analysis includes this category of use, but only with regard to potential harm to the human subject arising directly from exposure to the system and excluding any diagnosis or treatment of the subject (see category 3 below). Note however that for this category of use, in some cases this risk analysis identifies a potential hazard for which Verasonics has not fully implemented the mitigations that would be required. In these cases, the mitigation included in this document is "user information" that will be provided by Verasonics in the documentation for the system. It is the responsibility of the developer of such an investigational device to respond appropriately to all of the user information and safety warnings provided in the system documentation ("user information" items identified in this risk analysis document are all included in the *Safety and Regulatory* section of the *Vantage User Manual*). The user must also conduct their own risk analysis of the overall system for their specific intended application, and ensure that applicable regulatory and safety standards have been met. This document may be used as an element of that overall risk analysis, to identify potential hazards that are specific to the Vantage system as provided by Verasonics and the control measures that have been incorporated to address those hazards. A companion document, "Ultrasound Imaging of human subjects — safety guidelines for research using the Verasonics Data Acquisition System", provides additional guidance to the user on characteristics of the Vantage system which may affect their risk analysis, and features the Vantage system provides to facilitate risk control for the overall investigational system.

Note however that an investigational device as developed by a Vantage customer typically will include components not provided by Verasonics (probes, application-level user scripts to program the system, changes to user interface or system packaging, etc.). The Vantage Risk Analysis cannot anticipate all of the new potential hazards that might arise from these additions and changes to the system. This is another area where the user can reference the Vantage Risk Analysis as a starting point but must conduct their own overall risk analysis review including all of the system changes and additions they have made.

3. Diagnostic or Therapeutic Applications on Human Subjects

As an extension of category 2, a Vantage system can also be used as an investigational device on human subjects that will include actual diagnosis or treatment of the subject. The Vantage system (or some components taken from the system) may also be used as a prototype for clinical evaluations of a commercial product being developed by a Verasonics customer, as well as potentially being used in the product itself. It must be understood that assessing the Relative Risk Level of identified failure modes in such applications is beyond the scope of this risk analysis.

For example, a potential failure mechanism that was fully identified in this risk analysis but with Severity rated as a minor annoyance may become a critical misdiagnosis hazard when the system is actually being used for diagnosis. This elevated Severity may in turn require additional risk mitigation measures.

For this category of use the user must conduct a thorough risk analysis, and the appropriate levels of regulatory submissions, reviews, and testing for their specific overall system design and intended use. Once again, the Vantage Risk Analysis can be used as a starting point but with the understanding that there may be potential hazards not anticipated by Verasonics and the identified hazards may need to be redefined in terms of Relative Risk Level and required mitigations. The "Identification of Safety-Related Characteristics" section of this document should also be carefully reviewed, since the user's intended clinical application may imply additional items that were not included here.

Overall scope of the Risk Analysis

For all three categories of intended use as described above, the intended scope of the Vantage risk analysis is to include all failure modes or potential hazards that can be attributed to the Vantage system as supplied by Verasonics. If in our experience or through feedback from Vantage customers additional potential hazards internal to the system are identified that have not been included in the Vantage Risk Analysis, a new revision will be prepared to include them.

IDENTIFICATION OF SAFETY-RELATED CHARACTERISTICS

This section identifies potentially safety-related features of the Vantage system as required by ISO 14971 ¶4.2. The questions in ISO 1497 Annex C have been used as a guide, and are referenced in the following list (Items from Annex C.2 that are not listed here have been determined to be non-applicable to the Vantage system or to investigational devices based on it). Note that several items in this list are described as non-applicable to the Vantage system under Intended Use 1, but have been included as a guide to users of the Vantage system since these items may be applicable to an investigational device using the system operating under Intended Uses 2 & 3.

Note also that this list was based on the Vantage System Definition given in the "Intended Use" section of this document. If a user's investigational system includes added features or HW or SW components that are not part of the system supplied by Verasonics, the user should review ISO 1497 Annex C.2 to see if additional items should be added in their risk analysis review.

1. **Intended Use** (C.2.1): This risk analysis identifies all foreseeable failure modes of the Vantage System. The Relative Risk Level of such failure modes are evaluated under Intended Use categories 1 or 2, i.e. it is assumed that the Vantage System will not be used directly for diagnosis, monitoring, or treatment of human subjects and will not be used to sustain or support life. If the Vantage system is applied under Intended Use category 3, then the user is responsible for conducting a more thorough risk analysis of the overall system. There may be additional application-specific potential failure modes of the Vantage system that have not been covered here, e.g. misdiagnosis hazards, and the Relative Risk Level of the identified failure modes may be different under Intended Use 2 or 3.
2. **Patient Contact** (C.2.3): The Vantage system itself is not intended to have direct patient contact, but an ultrasound transducer assembly connected to the Vantage system will typically be in direct patient contact for Intended Use cases 2 or 3. Interactions between the system and transducer as well as the transducer itself should be evaluated by the user for potential hazards associated with direct patient contact. This applies equally to transducers provided by the customer, and to transducers purchased from Verasonics. (Transducers sold by Verasonics are included in the IEC61010 approval covering Intended Use 1, but have no regulatory approval for use on human subjects and have not been tested for safety issues related to direct patient contact.)
3. **Energy delivered to Patient** (C.2.5): The system will deliver ultrasound energy to the patient through the connected transducer, and may also deliver heat through heating of the transducer during use.
4. **Measurements or other interpretative data** (C.2.11, 12): The Vantage system has the capability to provide a multitude of measurements, images, and other interpretative data in conjunction with the user's application SW. Any such use, and the analysis of any potential hazards associated with such use are beyond the scope of this Vantage system risk assessment and must be covered by the user's risk analysis of their overall investigational system.

5. **Combined use with other devices, medicines, or other medical technologies** (C.2.13): Combined use may be fairly common for investigational devices using the Vantage system (e.g. ultrasound contrast agents, use in conjunction with other imaging technologies or other medical devices, etc.). Any such use, and the analysis of any potential hazards associated with such use are beyond the scope of this Vantage system risk assessment. Any potential hazards in this area must be covered by the user's risk analysis of their overall investigational system.
6. **Unwanted Energy Outputs** (C.2.14):
    - Acoustic noise (primarily from system cooling fans)
    - Heat dissipated by the system
    - Leakage current (in the presence of a fault in the system ground through the AC line cord).
    - Electromagnetic radiation that may interfere with other devices or systems nearby.
7. **Environmental Susceptibility** (C.2.15):
    - Exposure during transport or storage to extremes of shock, vibration, temperature, or humidity.
    - Exposure during operation to extremes of ambient temperature, AC line power variations, electrostatic discharge, or electromagnetic interference.
    - Spills of liquids or other substances into the Vantage enclosure.
8. **Environmental Emissions** (C.2.16): The Vantage system may emit smoke or other toxic materials as a result of an internal component failure, overheating, or fire.
9. **Software Content** (C.2.19): The Vantage system contains extensive software components including FPGA code internal to the system HW, and drivers and application-level SW utilities running on the host computer. The Vantage system also requires user-supplied application level software to manage and control it.
10. **Safe Disposal** (C.2.25): Disposal or recycling of the Vantage system should be done in accordance with established environmental and regulatory guidelines for computers and electronic devices. The Vantage HW system contains no batteries or other components with specific toxic material handling or disposal constraints.
11. **Special Training for Installation and Use** (C.2.26, 27):
    - Installation: the Vantage System as supplied consists of multiple components as defined in the Intended Use section, including host PC, Vantage HW unit, and transducer. Instructions for setup are provided with the system, and are directed at Intended Use 1, e.g. installation in a research and development laboratory. If the Vantage system is incorporated into a system for usage under Intended Use 2 or 3, the User has the responsibility to assess and provide the installation instructions and/or training that may be required.
    - Use: for use under Intended Use 1, the Vantage System is provided with a detailed programming guide. For use under Intended Use 2 or 3, the User has the responsibility to assess and provide the usage instructions and/or training that may be required.

HAZARD IDENTIFICATION and ESTIMATION OF RISKS

This section provides definitions of the "Relative Risk Level" to be estimated for each hazard as required by ISO 14971 ¶4.3 and ¶4.4.

Throughout this document, the phrase "Relative Risk Level" is intended to be a specific reference to the definitions given in this section and the associated Relative Risk Index and Relative Risk Category, as defined by Verasonics through this Risk Analysis.

The estimated Relative Risk Levels given in this document are based on intended use categories 1 and 2 that do not involve diagnosis or treatment of human subjects. Users of the Vantage System in intended use category 3 should make their own re-assessment of the Relative Risk Level for all potential hazards identified in this document, since the both the estimated Severity Level and Probability of Occurrence could be significantly different for a category 3 application.

Risk Estimation Technique: The Relative Risk Level associated with each hazard will be estimated using a qualitative assessment of five Severity Levels, and a semi-quantitative assessment of five Probability of Occurrence ranges as described in ISO 14971 Annex D.3.

Severity Level

Severity Levels are defined based on the level of harm that could occur to either the patient or the operator of the system, as listed in the following table.

Severity Level	Qualitative Definition
Catastrophic	Results in death of subject or operator
Critical	Results in permanent impairment or life-threatening injury
Serious	Results in injury or impairment requiring professional medical intervention
Minor	Results in temporary injury or impairment not requiring professional medical intervention
Negligible	Annoyance, inconvenience, or temporary discomfort

Probability of Occurrence

For an ultrasound imaging system, it is more meaningful to define the Probability of Occurrence of an event in terms of individual patient exams conducted with the system rather than cumulative hours of use or age of the system. Thus the Probability of Occurrence p is defined as the probability the event will occur during the course of

a typical patient exam. In a typical clinical setting, a relatively heavily used system is expected to complete on the order of ten patient exams per day. The table below defines the Probability of Occurrence ranges to be used for the Vantage system risk analysis:

Probability Level	**Approximate Probability of Occurrence Range**
Frequent	More than once in five exams (more than once per day for a typical heavily used system) $p > 0.2$
Probable	About once per week for a typical, heavily used system $0.2 > p > 0.01$
Occasional	A few times per year for a typical, heavily used system $10^{-2} > p > 10^{-4}$
Remote	A few times in the useful life of a typical, heavily used system $10^{-4} > p > 10^{-6}$
Improbable	Unlikely to occur over the useful life of a population of 50 typical, heavily used systems (useful life defined as 5 years) $10^{-6} > p$

Relative Risk Level Definition

Based on these definitions of Severity and Probability of Occurrence, individual Relative Risk Levels are defined using a Relative Risk Index, based on the values listed in the risk evaluation matrix shown below. The index values have no absolute meaning; they only represent Verasonics' judgment of Relative Risk Levels for different combinations of Severity and Probability of Occurrence, with an index value of 1 representing the highest risk and 20 the lowest.

Relative Risk Index values have been grouped into three Relative Risk Categories of Unacceptable, Marginal, and Acceptable, as defined here.

- **UNACCEPTABLE:** Relative Risk Levels of 1 through 8, highlighted in pink in the table, are not acceptable. Additional risk control measures must be taken to reduce the severity and/or probability of the associated hazard.
- **MARGINAL:** Relative Risk Levels of 9 through 14, highlighted in yellow in the table, must be evaluated carefully to determine if a reduction in Relative Risk Index is feasible. At a minimum, documentation must be provided to the users of the system to warn them of every potential hazard with a marginal Relative Risk Level.
- **ACCEPTABLE:** Relative Risk Levels of 15 through 20, highlighted in green in the table, represent acceptable levels of risk for the Vantage system. No additional evaluation or risk control measures are required.

Probability	**Severity**				
	Catastrophic	Critical	Serious	Minor	Negligible
Frequent	1	4	7	12	16
Probable	2	5	8	13	17
Occasional	3	6	9	14	18
Remote	4	7	11	16	19
Improbable	6	10	15	17	20

Coding of Identified Hazards

Listed in the following section are all specific hazards that have been identified for the Vantage system, as of the current revision of the Vantage Risk Analysis/ Risk Management Plan. To facilitate references to individual hazards in other documents or other parts of this document, each hazard is identified with a category and a unique index number within that category as defined below:

- **H.EM.N** Hazard index number N for a hazard associated with **E**lectro**M**echanical issues (EMC, audible noise, electric shock, etc.).
- **H.AP.N** Hazard specifically associated with acoustic output levels from the system through the transducer (**A**coustic **P**ower). This category includes both acoustic power and acoustic intensity, and other factors directly associated with acoustic output such as transducer heating.
- **H.SF.N** Hazard associated with any aspect of **S**ystem **F**unctionality other than acoustic power output.
- **H.UE.N** Hazards associated with **U**ser **E**rrors in their utilization of the Vantage system. These could be issues with the programming and use of the Vantage system itself, or issues with the user's design & implementation of the overall system of which the Vantage system is a component.

To facilitate cross-reference to verification test documents, etc., risk control measures are identified using the Hazard ID code defined above, but with "RC" replacing the "H". For example, the second risk control measure identified in hazard H.UE.4 would be RC.UE.4B. Similarly, user information items will be identified with a "UI" prefix.

Note that in many cases, a potential hazard of the system has already been reduced or eliminated by other measures Verasonics has taken in the design of the system which were not motivated by safety concerns. In those cases, the design element in question will not be included in this document as a risk control item but may be considered an "inherent safety by design" factor if it also reduces the risk of a potential hazard. (As an example, Verasonics has incorporated extensive shielding within the system to reduce EMI susceptibility, simply to produce an instrument with a usable level of reliability and performance for the R & D customer. This shielding will not be listed as a risk control measure, since it is already present in the system independent of any potential EMC-related hazard.)

Note also that the Relative Risk Levels assigned in this risk analysis are based on Intended Use categories 1 and 2, e.g. research and development usage that does not provide diagnosis or treatment of human subjects. For Intended Use category 3, where a Vantage-based system could contribute directly to patient care, then the entire risk estimation process would have to be repeated (for example, the Severity of a fault condition which led to complete loss of system functionality might change from "Negligible" to "Critical").

RISK EVALUATION and RISK CONTROL

For each hazard in the listing below, the identification and risk estimation are followed by paragraphs addressing the risk evaluation and risk control to be applied for that hazard, as required by ISO 14971 ¶5 and ¶6. (These paragraphs are not included for hazards with an acceptable Relative Risk Level and thus requiring no additional evaluation or risk control measures.)

LISTING OF IDENTIFIED HAZARDS

This section lists specific hazards that have been identified for the Vantage system through the risk analysis process, including the estimated Relative Risk Level that has been assigned, and any associated risk control measures.

H.EM.1 Electric shock due to a fault in AC line input wiring or devices.

Relative Risk Level: 16 Acceptable (Severity: minor Probability: Remote)

Description & Evaluation: The AC line input devices and wiring methods used in the Vantage system conform to IEC 61010 and related standards for use as laboratory test equipment, including the OEM power supply (internal to the Vantage HW unit) which also conforms to the "medical grade" leakage current regulatory requirements. This approach provides redundant protection, greatly reducing the severity of the hazard in any single- fault situation. The severity rating of 'minor' is based on any such single-fault condition: In the event of an AC line isolation fault, the fault current will be shunted to ground through the direct connection of the system chassis to the AC line power ground conductor, and thus the operator would not be exposed to a potential of more than a few volts from contact with the system chassis or other grounded components. In the event of a fault (open) in the ground conductor, the medical-grade leakage current limit reduces the user exposure to a relatively harmless level. In the presence of a double fault (e.g. a short from the high side of the AC line to the chassis, and at the same time no connection from chassis to ground) the severity would be much worse (critical, on our scale) but the probability of occurrence would be in the "Improbable" range. The assignment of an acceptable Relative Risk Level is further justified by the observation that the system design approach conforms to the industry guidelines and regulatory standards applied to other AC line-powered medical devices; the Vantage system as provided by Verasonics is certified to comply with the IEC 61010 standards for laboratory test equipment.

Note however that this risk evaluation is based on the assumption that the system was actually built as designed. It is possible that during the manufacturing process a wiring error could be made in connecting the OEM power supply to the rear panel AC line cord connector, or that the OEM power supply had manufacturing defects or was damaged during shipping and handling. An undetected assembly error or manufacturing defect could expose the user to a much higher Relative Risk Level.

Risk Control Options: To minimize the probability of the system having an undetected defect in the AC line isolation or ground connection, Verasonics will subject each completed system to testing of the AC line isolation and ground impedance as part of the manufacturing test process, and repeat this test whenever a system has been partially disassembled/reassembled for repair or service. This approach will be both more effective and less costly than attempting to add automated leakage self-tests to the system design.

Risk Control Measures to be Verified:

AC Line Isolation and Ground Testing (RC.EM.1): Verasonics shall submit every production Vantage chassis assembly to a test of AC line isolation and ground impedance, as measured at the AC line cord IEC connector on the rear of the system. This test shall be

conducted after the system is fully assembled and side covers are installed, prior to delivery to the customer. This test shall be repeated after a system has been subjected to any repair or maintenance activity that required opening the chassis.

AC Line Isolation Warning (UI.EM.1): Vantage system shall include user information warning the user that for a medical application involving human subjects, the AC line isolation requirements will apply to all interconnected line-powered devices (typically the Vantage HW unit, host computer, display monitor, external power supply for HIFU configurations, and any other devices the user has connected to the system). Guidance on adding an isolation transformer or other alternatives for meeting the medical device requirements shall be included.

New Risks: Since the AC line isolation and ground impedance tests will not stress the system beyond its design limits, no new risks are created by this testing.

H.EM.2 Electric shock from internal system high-voltage power supplies.

Relative Risk Level: 17 Acceptable (Severity: Minor Probability: Improbable)

Description & Evaluation: The Vantage system contains internal power supplies operating at levels up to approximately 100 Volts DC as well as the AC line input wiring, which could lead to serous injury if a user came into accidental contact with them. But since the system is fully enclosed within a grounded metal chassis and covers, there is no chance of such user contact other than at the external connector interfaces to the system. The only location at which the user could come into contact with voltages from the internal 100 V. DC power supplies is the transducer connector. All internal power supplies in the Vantage system conform to the IEC "PELV" (Protected Extra Low Voltage) definition: less than 120 V. DC or 50 V. RMS AC, and isolated from all non-PELV voltages (which for the Vantage system applies only to the AC line input wiring). Therefore, the severity of a user contact with these voltages is in the Minor category based on the IEC guidelines. Furthermore, the Vantage system includes interlocks that will automatically disable the internal HV (100 V.) power supplies to the transducer connector, when no transducer is actually connected. This reduces the probability of user contact to the Improbable category. Note, however, the Vantage system also provides SW utilities that can be invoked by the user to disable these interlocks, for development and system test purposes. When the system is operating with the transducer connector interlock disabled, a user could also be exposed to transmit output signals at the transducer connector, with voltages above 50 V. RMS but only at RF frequencies above approximately 1 MHz. At these frequencies there is no electric shock hazard; the RF energy 'skin effect' reduces the potential harm to a minor burn at the point of contact.

Risk Control Options: No additional risk control is required.

H.EM.3 System Release of smoke or toxic gases due to internal component failure.

Relative Risk Level: 18 Acceptable (Severity: Negligible Probability: Occasional)

Description & Evaluation: The Vantage system contains several internal power supplies and system functions operating at moderately high power levels (on the order of 50 to 500 Watts) that are capable of producing intense localized levels of heat in the presence of a component failure or other system fault. In the vast majority of such fault conditions, the result will be destructive failure of one or a few components which will prevent the associated circuitry or power supply from continuing to function and thus will prevent damage or overheating of other components. Minute quantities of smoke or gases may be released by the failed components, and thus the severity of potential harm to operator or patient is rated as negligible. See H.EM.4 for failure mechanisms leading to more extensive damage. The probability of occurrence of this type of hazard is inherently quite low, since the system has been designed to be as reliable as possible and to minimize 'cascading failures' that could be destructive to other components in the presence of a fault condition. The Verasonics HW system design process includes reviews and testing to ensure all components are conservatively rated for the temperature, voltage, current, and power levels they will be subjected to. The Vantage system uses a "distributed power supply" approach: the output from a single 12 Volt DC OEM supply is distributed to all modules in the system, with multiple small DC-DC converters provided on each module to produce the low voltage DC supply levels needed within that module. Where practicable, these individual DC-DC converters include overvoltage and overcurrent sensing to disable the system when excessive loads or other fault conditions are detected. Note that for the transmit HV supply additional fault detection and monitoring features are provided as described in hazard H.AP.2.

Risk Control Options: No additional risk control is required.

New Risks: A failure of one of the fault or overload detection and shutdown mechanisms identified above, or an incorrect setting of an overload detection threshold, could lead to a system shutdown that was unnecessary and thus from the users perspective a failure of the system. Refer to hazard H.SF.1.

H.EM.4 System Release of excessive heat, smoke, or toxic gases due to internal overheating or fire.

Relative Risk Level: 16 Acceptable (Severity: Minor Probability: Remote)

Description & Evaluation: See hazard H.EM.3 above, covering failures involving a very small number of components. This hazard condition covers failure mechanisms that do not fit the description in H.EM.3, and could result in a much larger release of smoke, combustion gases, and possibly significant

levels of heat. (For example, a failure that involves a large number of components and is not “self-extinguishing” because it did not trigger a power supply shutdown, and/or started a fire within the system). The severity level for these higher levels of emission is increased to minor, but the probability of occurrence is much lower, at the remote level based on the nature of the system design as described in H.EM.3. For the existing population of VDAS systems installed at customer sites and within Verasonics, there have been several system failures that involved the destructive failure of an internal component. But there is no known instance of such a failure resulting in the release of a perceptible level of heat, smoke, or fumes.

Risk Control Options: No additional risk control is required.

New Risks: A failure of one of the fault or overload detection and shutdown mechanisms as identified in H.EM.3, or an incorrect setting of an overload detection threshold, could lead to a system shutdown that was unnecessary and thus from the users perspective a failure of the system. Refer to hazard H.SF.1.

H.EM.5 Electromagnetic radiation from Vantage system and transducer disrupts operation of other devices.

Relative Risk Level: 16 Acceptable (Severity: Minor Probability: Remote)

Description & Evaluation: The Vantage system has been designed to meet state-of-the-industry EMC standards and design guidelines, in terms of system shielding, grounding, and noise filtering. The Vantage system has been tested and certified as complying with the IEC 61010 standards for EMC, including use with transducers available through Verasonics.

Risk Control Options: No additional risk control measures for the Vantage system are required. However, user information shall be provided to warn the user of the potential for EMC-related hazards if the grounding or shielding of the transducer to be used with the system is inadequate.

Risk Control Measures to be Verified:

Transducer Shielding Warning (UI.EM.5): Vantage system shall include user information warning the user of the potential hazard of EMC problems from a transducer with inadequate shielding. If the user does not have confidence in the EMC design of the transducer, the entire system plus transducer should be subjected to formal EMC testing.

H.EM.6 Acoustic noise level from system is disruptive or stressful to operator and/or patient.

Relative Risk Level: 17 Acceptable (Severity: Negligible Probability: Probable)

Description & Evaluation: Noise from system cooling fans (in both the Vantage HW system and the associated host computer) may be annoying or distracting to the operator, patient, or others in the vicinity of the system while it is in use. The severity level is judged as negligible since in the worst case it is only an annoyance; the audible noise level from the system is far below the threshold of potential injury. (When TUV Rhineland conducted testing of the system to the IEC 61010 standard, they did not make quantitative measurements of the audible noise output level, because in their judgment it was insignificant. Refer to category 1 in the Intended Use section for details of the IEC 61010 testing and approval.) The Vantage system includes automatic fan speed control that will result in much quieter operation for a typical user environment, well below the maximum operating ambient temperature limit. As a result, the Probability Level has been set to Probable.

Risk Control Options: No additional risk control measures for the Vantage system are required. However, user information **(Audible Noise Warning, UI.EM.6)** shall be provided to warn the user of the need to evaluate the acoustic noise level of their overall investigational device, and the potential hazard of operator errors, miscommunication, etc. in the presence of an excessive noise level.

H.EM.7 System HW malfunction resulting from damage in storage or transport.

Relative Risk Level: 18 Acceptable (Severity: Negligible Probability: Occasional)

Description & Evaluation: During shipping, storage, or transport the Vantage system could be subjected to high levels of stress from shock, vibration, or extremes of temperature or humidity. These stresses could in turn lead to HW faults that could degrade system functionality or performance in unpredictable ways. The severity has been rated as negligible since HW faults that could lead to more severe levels of patient or operator harm have been covered through control measures identified elsewhere (see H.AP.1, 2, and H.EM.3, 8). The Vantage system mechanical design adheres to state-of-the-industry guidelines and standards for minimizing the risk of damage from shock, vibration, and other environmental extremes. Verasonics also provides a custom-designed shipping container that is intended to protect the system from damage. This limits the probability of occurrence to the Occasional level.

Risk Control Options: To further reduce the probability of user or patient exposure to undetected HW faults, the system includes protective measures and user information as listed below:

Risk Control Measures to be Verified:

System Self-Test (RC.EM.7): System shall include an automated self-test function that can be invoked under user control, and will warn the user if all transmit-related functions and controls are not working properly.

Self-Test Instructions (UI.EM.7A): System shall provide instructions on use of the self-test functionality, and guidelines that the self-tests should be repeated after the system has been transported, or disassembled and reassembled for any reason.

Shipping & Receiving Inspection Instructions (UI.EM.7B): System shall provide instructions to the user to inspect the shipping container and system for any signs of damage during shipping and handling, and also to check the shock sensors attached to the shipping container. Verasonics must be notified if there are visible signs of damage or if any shock sensors have been tripped. The user shall also be instructed to retain the shipping container, and re-use it if it is ever necessary to ship the system to another location or return it to Verasonics.

Residual Risk: 19 Acceptable (Severity: Negligible Probability: Remote) If the user follows the stated guidelines, probability of an undetected fault will be further reduced.

New Risks: none.

H.EM.8 System HW malfunction due to extreme operating conditions.

Relative Risk Level: 18 Acceptable (Severity: Negligible Probability: Occasional)

Description & Evaluation: Environmental stresses during system operation (such as droop, dips, or surges in AC line voltage, high ambient temperature, or ESD events) may lead to HW faults that could degrade system functionality or performance in unpredictable ways. The severity has been rated as negligible since HW faults that could lead to more severe levels of patient harm have been covered through control measures identified elsewhere (see H.AP.1, 2, and H.EM.3, 8). The system design uses state-of-the-industry guidelines for ESD immunity and cooling system performance, and the OEM power supply used in the system conforms to the applicable industry and regulatory standards for immunity from AC line power disturbances. These factors reduce the probability of occurrence to the Occasional level.

Risk Control Options: To further reduce the probability of exposure to undetected HW faults, the system shall include user information on the required environmental operating conditions.

Risk Control Measures to be Verified:

Operating Environment Warning (UI.EM.8): System shall include clear documentation of the operating ambient temperature range, and allowable levels of AC line power disturbances. System shall also provide guidance to the user that they should verify their operating environment actually conforms to these limits.

Internal Temperature Monitoring and Over-temperature Shutdown (RC.EM.8): System shall include internal temperature sensors that are continuously monitored while system is in operation. An automatic HW shutdown shall be invoked if internal temperatures exceed a safe operating limit threshold. These monitoring and shutdown functions shall be self-contained within the system HW and FPGA code, independent of any system SW interaction.

Residual Risk: 19 Acceptable (Severity: Negligible Probability: Remote) If the user follows the stated guidelines, probability of an undetected fault will be further reduced.

New Risks: none.

H.AP.1 Uncontrolled acoustic output due to communication failure with host computer.

Relative Risk Level: 14 Marginal (Severity: Minor Probability: Occasional)

Description & Evaluation: There are a number of mechanisms that could lead to failure of the control link between the Vantage system and the system control SW running on the host computer, such as a lockup or error in the system control SW, failure of host computer HW or driver and OS SW, damage or disconnection of the control interface cables, or failure of the HW components associated with the control link. In any of these situations, it is possible that the HW sequencer and transmit functions within the Vantage system could continue to run but in an uncontrolled state that could result in excessive acoustic output levels.

Risk Control Options: An inherent safety by design approach to this hazard would be to require every transmit event on the Vantage system to be initiated by a control action from the application SW on the host computer. Because of the inherent delays and variable latency of the control link from the host computer application SW to the Vantage system HW, this approach would significantly degrade the performance of the system. Instead a control measure shall be implemented in the Vantage system design: a mechanism to automatically disable all transmit functions if communications from the host computer are disrupted for more than ten seconds. Starting with the 3.2 release the timeout interval was made user-programmable over a range from 10 milliseconds to 10 seconds, while still defaulting to 10 seconds if the user does not specify a value. The Verification Test procedure for RC.AP.1A has also been updated to verify the functionality of the user-programmable feature.

Risk Control Measures to be Verified:

SW Watchdog timer (RC.AP.1A): Vantage system HW shall include a watchdog timer function that will disable all transmit functionality within a user-programmable timeout interval (of 10 milliseconds to 10 seconds) if it does not receive a watchdog reset command from the application SW running on the host computer. This watchdog timer may be disabled under SW control to support system test activities, but the system's default operating state at system startup shall be with the watchdog timer enabled.

Host System Power Control (RC.AP.1B): The physical communication cable from the host computer to the Vantage system shall include a control signal that will disable all internal power to the Vantage system if the cable is disconnected or the host computer is turned off.

Residual Risk: 16 Acceptable (Severity: Minor Probability: Remote) The identified risk control measures dramatically reduce the probability of occurrence of this hazard, but do not completely eliminate it. For example, it is conceivable (but very improbable) that some aspects of the system control SW could fail in such a way that the watchdog timer function would continue to operate. But even in a situation such as that, it is likely that other routine interactions between the application SW and the Vantage system HW would also be disrupted, such as DMA transfers of acquired receive data or 'sync' command handshakes. The sync and DMA commands both have programmable timeout intervals, which will trigger an error condition and cause the HW sequence to stop if the timeout interval is exceeded.

New Risks: A failure of one of the control measures described above could lead to a system shutdown that was unnecessary and thus from the users perspective a failure of the system. Refer to hazard H.SF.1.

H.AP.2 HW fault results in incorrect transmit Voltage.

Relative Risk Level: 14 Marginal (Severity: Minor Probability: Occasional)

Description & Evaluation: A component failure or other HW fault condition could result in an error in the actual voltage output from the transmit HV power supply as compared to the commanded voltage from the user's application SW. The majority of fault conditions that could cause this error would result in reduced output or no output from the supply, and thus would not present any risk of harm to the patient. In some cases, however, a HW fault could lead to the output voltage being greater than the commanded level which would expose the patient to higher acoustic output levels and/or transducer surface temperature. Based on this analysis, the probability of occurrence is set in the Occasional range.

Risk Control Options: For faults of this type, inherent safety by design is not feasible. Redundant control paths could reduce the probability of a fault but not eliminate it, and would introduce new failure mechanisms and potential faults of their own. Instead, a control measure can be provided through a separate HW path to monitor the actual supply level, reducing the probability of occurrence to the level of simultaneous double fault conditions.

Risk Control Measures to be Verified:

Transmit HV Supply Voltage Monitor (RC.AP.2): The Vantage system HW design shall provide an independent means of monitoring the actual transmit HV supply output voltage, comparing it to the commanded voltage, and disabling the supply if the error exceeds normal tolerances either above or below the commanded level. The system HW and FPGA code design shall be structured to ensure that any failure mechanism that disrupts the operation of the monitor and shutdown function could not also cause the supply to go to a higher output level (and thus ensuring that no single-fault condition can lead to an increased output level). To provide the intended Relative Risk Level control, the error threshold for the monitor function should be restrictive enough to reduce the magnitude of undetected errors as much as possible while avoiding the risk of spurious error conditions from normal component tolerances or transient conditions. A fixed error level threshold of +/- 5 Volts over the full transmit voltage range has been chosen to meet this objective, for TPC profiles 1-4. This results in a much wider relative tolerance at lower voltages, but this is required due to offset and quantization errors in the control and monitor functions. This is judged to be acceptable since at these lower supply voltages the worst-case potential severity of a fault condition is also much lower. For TPC profile 5 (used for therapeutic HIFU transmit levels or other applications requiring much higher power levels than imaging), the error thresholds above and below the nominal level shall be user-programmable so the user can set the threshold optimally for a specific application.

Residual Risk: 17 Acceptable (Severity: Minor Probability: Improbable)

New Risks: A 'false positive' failure of the control measure described above could lead to a system shutdown that was unnecessary and thus from the users perspective a failure of the system. Refer to hazard H.SF.1.

H.AP.3 Corrupted transmit waveform results in excessive acoustic output.

Relative Risk Level: 16 Acceptable (Severity: Minor Probability: Remote)

Description & Evaluation: The complexity of the arbitrary waveform generator in the Vantage system requires a lengthy descriptor table to program it. For each transmit event in a user's script, a descriptor table must be generated in system SW, transferred to memory in the HW system, and then transferred from that memory to the FPGA programming registers when it is time to execute a specific transmit event. Corruption of the data in this table could lead to a very different transmit waveform than the one intended, in terms of frequency, burst duration, or other characteristics that could affect acoustic output. An 'inherent safety by design' feature has been included in the system to minimize the chances of an incorrect waveform due to SW or HW malfunction: a checksum is generated for each data table when it is synthesized by system SW to specify the waveform. When the table is transferred to the HW to actually generate the transmit output, the checksum is evaluated and the HW will report a fault condition and stop operation if a checksum error is detected. For diagnostic imaging applications, the severity level of a corrupted waveform has been judged to be Minor; with the checksum verification the Probability of Occurrence is Remote. Due to the complexity of the multiple layers of SW, HW, and FPGA code required to translate a user's waveform definition into the actual transmit output from the HW, verification testing must be repeated for each SW release to ensure the entire waveform generation path is functioning properly.

Risk Control Options: No additional risk control is required.

Risk Control Measures to be Verified:

Transmit Waveform Descriptor Checksum Testing (RC.AP.3A): The Vantage system SW release verification test plan for each customer release shall include tests to confirm the checksum test is functioning properly, such that a checksum error will be detected and will block use of the system.

Transmit Waveform Generation Functionality Test (RC.AP.3B): The Vantage system SW release verification test plan for each customer release shall include tests of the entire range of waveform definition techniques accessible by the user, to ensure they actually produce the correct transmit output waveform from the HW system.

H.AP.4 Uncontrolled acoustic output due to HW sequence running out of control.

Relative Risk Level: 14 Marginal (Severity: Minor Probability: Occasional)
Description & Evaluation: During normal operation, the Vantage system design relies on two distinct event sequences operating in parallel but largely independent of each other- the HW event sequence executing actual transmit/ receive events in the HW system, and a SW event sequence executing data processing and display events in the host computer. It is possible that a fault condition (such as described in H.SF.3 and H.SF.4) could result in failure of the HW event sequence, or HW execution of a corrupted event sequence that differs from what was intended. If the malfunctioning HW event sequence was undetected by the system SW, the result could be uncontrolled acoustic output from the system.
Risk Control Options: The system employs an inherent safety by design approach to this hazard for most typical user scripts involving receive data acquisition, since handshakes between the HW and SW event sequencers are required to start and complete a DMA transfer of receive data from the HW system to the host computer. The SW DMA processing includes a DMA timeout feature if the next DMA from the HW system does not arrive within a specified maximum interval (default is one second). The DMA timeout is processed as a system fault condition that will stop the HW and SW sequencers and notify the user of the fault. The sequence control "sync" command with programmable timeout can also be used for HW-SW synchronization and will trigger a fault condition if the interval is exceeded. Either of these approaches can be used to provide a "HW watchdog" monitoring the state of the HW sequence, the complement of the SW watchdog timer monitoring operation of the system SW in H.AP.1.

Note however that the user may design an event sequence that operates asynchronously, with no mechanism for HW watchdog monitoring by the system SW. This is a legitimate operating state as far as the system design is concerned, but it exposes the system to the potential hazard of a HW sequencer that has failed or is not executing the intended sequence. The control measure to avoid this situation is user information that a script should always be designed to include some form of handshaking or monitoring between the HW and SW event sequences, for applications where uncontrolled acoustic output could be a hazard for the subject.

Risk Control Measures to be Verified:

HW Watchdog Timer Functionality (RC.AP.4): The Vantage system SW release verification test plan for each customer release shall include tests to confirm the programmable software timeout error conditions are functioning properly for both the "sync" sequence control command and for synchronous DMA transfer commands, and that in both cases if the timeout interval is exceeded the HW and SW sequencers will be forced to stop and a fault condition will be reported to the user.

HW Watchdog Timer Documentation (UI.AP.4): System documentation shall include a user warning describing this potential hazard and the need for inclusion of some type of HW-SW handshake in any transmit-only event sequence. All methods of implementing the HW Watchdog shall be explained, including Sequence Control 'sync' command with timeout, synchronous DMA transfers with DMA timeout, and the potential use of the receive data time tag feature to provide precise SW monitoring of HW event sequence timing.

Residual Risk: 16 Acceptable (Severity: Minor Probability: Remote) The identified risk control measure dramatically reduces the probability of occurrence of this hazard.

New Risks: A failure of one of the handshaking control measure described above could lead to a system shutdown that was unnecessary and thus from the user's perspective a failure of the system. Refer to hazard H.SF.1.

H.AP.5 SW fault results in incorrect transmit Voltage.

Relative Risk Level: 14 Marginal (Severity: Minor Probability: Occasional)

Description & Evaluation: Since the transmit voltage from the HW system is under direct software control, a malfunction in the software could conceivably result in a transmit voltage command at a level beyond the limits that had previously been set for the allowed transmit voltage operating range. A malfunction such as this could occur in many possible ways, such as an undetected software design flaw, an unexpected sequence of user control inputs, a software configuration fault such as leaving test/debug utilities enabled inappropriately, etc. For the specific situation being addressed by this potential hazard, the software would have to function properly through the "initialization" phase of an application where the system is being set up for the desired operating sequence, and then fail with an out-of-range transmit voltage command while the application is running. Based on this analysis, the probability of occurrence is set in the Occasional range.

Risk Control Options: For faults of this type, inherent safety by design is not feasible and/or may not be very effective since any error checking or redundant control paths within the application software may be susceptible to the same flaw that created the out-of-range command. A more robust control measure has been provided in the Vantage system design, by implementing a function to monitor transmit voltage commands that runs independently of the system application software while a sequence is running and is also physically independent of the host computer where the system application software is running.

Risk Control Measures to be Verified:

Transmit HV Command Monitor in FW (RC.AP.5): The Vantage system HW design shall include a 'validity check' function in the HW-level FPGA code that reviews all transmit voltage commands received while the system is running and compares them to a maximum voltage limit for the current application that was set during system initialization. The maximum voltage limit must be write-protected while the system is running, to ensure it could not be corrupted by any malfunction of the application software. If a command is received that exceeds the maximum limit, an error condition shall be triggered that immediately stops system operation and notifies the user of the illegal voltage command fault condition. If the maximum voltage limit is not programmed during system initialization, it shall default to the minimum allowed voltage and thus effectively disable any normal use of the system.

Residual Risk: 17 Acceptable (Severity: Minor Probability: Improbable)
New Risks: A 'false positive' failure of the control measure described above could lead to a system shutdown that was unnecessary and thus from the user's perspective a failure of the system. Refer to hazard H.SF.1.

H.SF.1 System not functioning due to fault in a protective measure.

Relative Risk Level: 17 Acceptable (Severity: Negligible Probability: Probable)

Description & Evaluation: The system employs numerous fault detection/ shutdown features to protect it from additional damage in the presence of a fault condition, and also to reduce the risk of harm to the user or patient from a potentially hazardous condition. (Refer to hazards H.EM.3, H.EM.8, H.AP.1, H.AP.2 as specific examples). A 'false positive' response from one of these fault shutdown features could prevent an otherwise normal system from functioning and thus would be a system failure from the user's perspective. If the investigational system is being used in a manner consistent with intended use categories 1 or 2 (system does not contribute directly to patient care, treatment, or diagnosis) then the severity of this fault condition is negligible since it is no more than an annoyance to the user and patient.

Risk Control Options: No additional risk control is required.

H.SF.2 System malfunction due to installation or configuration errors.

Relative Risk Level: 18 Acceptable (Severity: Negligible Probability: Occasional)

Description & Evaluation: The Vantage system is a moderately complex assembly of multiple HW and SW components. If a system was configured with incompatible versions or revision levels of some of these components (e.g. as a side effect of installing an upgrade to a new SW release from Verasonics), the result could be degraded system functionality or performance. The severity of this potential fault has been rated as negligible since fault conditions that could lead to more severe levels of patient harm have been covered through control measures identified elsewhere (see H.AP.1, 2, and H.EM.3, 8).

Risk Control Options: The hazard of configuration errors is implicit in the Vantage system architecture as a complex SW-controlled system made up of a large number of HW and SW components. To reduce the probability of configuration errors, the system includes the following protective measures and user information:

Risk Control Measures to be Verified:

Automatic Configuration Checks: (RC.SF.2): The critical HW and SW modules that make up the system shall include revision identifiers that can be read by the system control SW. During every system power-up cycle these identifiers shall be checked for compatibility by system SW routines, and configuration errors shall block system operation and be reported to the user.

Installation-Upgrade Warnings: (UI.SF.2): System shall provide user warnings about the need to follow installation and upgrade instructions very carefully and explicitly (such as the need to do a power cycle instead of just a warm reboot, or the need to do multiple restarts for some changes to fully take effect), to minimize the chance of configuration errors. After completing an installation or upgrade, the user should run the system self-test diagnostics utilities to confirm no latent faults are present. If a user has conducted acoustic output measurements or other verification tests on a system, they should evaluate whether those tests should be repeated after the installation of upgraded software, HW repairs, or other system modifications.

Residual Risk: 19 Acceptable (Severity: Negligible Probability: Remote) If the user follows the stated guidelines, probability of an undetected fault will be further reduced.

New Risks: none.

H.SF.3 System malfunction resulting from memory corruption, due to a transient event

Relative Risk Level: 16 Acceptable (Severity: Minor Probability: Remote)
Description & Evaluation: During operation, the Vantage HW runs from a copy of the system's operating state stored in internal FPGA memory. The system control SW writes to this memory as needed so the HW state matches the operating state maintained by the SW on the host computer. A transient event (e.g. electrostatic discharge, cosmic ray, line power disturbance, etc.) while the system is in use could cause the HW operating state to differ from the state in the system SW, and there is no comprehensive mechanism in the system that would immediately detect all such discrepancies. The probability of occurrence of this fault condition is estimated to be in the Occasional range, but the vast majority of these faults would result in the HW not functioning at all and thus the severity would be Negligible resulting in an acceptable Relative Risk Level of 18 (Negligible, Occasional) for those cases. For those instances where the HW continues to function the severity is increased to Minor since acoustic output or other parameters could be changed without the operator realizing it, but the probability of this situation is Remote, leading to the Relative Risk Level of 16 (Minor, Remote) given in the heading. If acoustic output was affected significantly by a transient-induced fault, the protective measures identified in H.AP.1, H.AP.2, and the transmit waveform descriptor checksum testing described in H.AP.3 would further reduce the probability of the fault not being detected.
Risk Control Options: No additional risk control is required.

H.SF.4 System malfunction resulting from memory corruption or incorrect HW programming, due to a software issue

Relative Risk Level: 18 Acceptable (Severity: Negligible Probability: Occasional)
Description & Evaluation: During operation, the Vantage HW runs from a copy of the system's operating state stored in internal FPGA memory.
A potential failure mechanism could occur if the memory location in which the operating state is stored is inadvertently altered, either due to an FPGA software issue or from an undetected bug in the "sequence load" SW that translates the operating state defined in the host computer to the corresponding state actually programmed in the HW FPGAs. For Intended Use cases 1 and 2 the severity of both of these failure mechanisms is rated as negligible since failure of the system to function as intended would be no more than an annoyance to the operator and human subject unless acoustic output actually increased due to the state corruption, but the probability of this situation is far lower due to the mitigations covered in section H.AP. The following design features are included in the system, which lead to the Probability assessment of Occasional:

- The memory locations in which the operating state is stored are written to only during system initialization and "sequence load" at system startup (or during subsequent transitions to a new operating sequence); when the system then switches to actually executing the sequence these memory locations are treated as read-only.

- When the operating state is adjusted by the system user (for example changing the focal depth of a B-mode scanning sequence), the operating state of the system is recreated and reloaded in its entirety. This prevents any potential errors from partially updating the operating state.
- The system initialization and sequence load functions that translate a user's script into the actual programming used by the SW and HW event sequences are thoroughly tested for each SW release using test scripts designed to exercise the full range of system features and operating states. Refer to the "Verification Test Plan" documents for a specific Vantage SW release, for a detailed listing of the test procedures and associated test scripts. With each new SW release, Verasonics incrementally increases the scope of the verification tests to improve their overall coverage in addition to adding specific tests related to new features or bug fixes in the release.
- Example scripts provided by Verasonics are thoroughly tested to verify they function as intended and do not stimulate any undiscovered bugs in system SW or FPGA code, including while exercising all user controls provided by the script. For scripts developed by a customer, similar verification testing must be done (See UI.SF.4).

Risk Control Options: See UI.SF.4 below. No additional risk control is required,

Risk Control Measures to be Verified:

Verification Testing of User Scripts: (UI.SF.4): System shall provide user warnings about the need to conduct thorough verification testing of Setup scripts they have developed or modified, to confirm the script functions as intended and produces the intended levels of ultrasound transmit output, event timing, etc. Since the Vantage system is designed to be as flexible as possible, virtually every aspect of the system operating state and event sequence is user-programmable. This leads to the possibility that a user script may put the system in an operating state that triggers an undetected bug in the system design. The most effective means of detecting and correcting this situation is thorough testing of the user script on the system to verify the actual system operating state matches what was intended.

H.UE.1 Electric shock due to AC line input wiring errors in overall system.

Relative Risk Level: 9 Marginal (Severity: Serious Probability: Occasional)

Description & Evaluation: When the user assembles the Vantage system into an overall system for use as an investigational device, this will typically require the use of multiple interconnected AC line-powered devices (Vantage system, host computer, display monitor, other external recording devices, power supplies, test equipment, other interconnected medical equipment, etc.). The combined effect of all these interconnected devices may be an excessive level of AC line leakage current. User errors in assembling the overall system may also result in inadequate or incomplete ground connections. Such a situation could represent a latent potential hazard to the user's safety, since a system with ground faults or excessive AC line leakage current is likely to function properly, and provide no indication to the user that a potentially hazardous condition is present.

Risk Control Options: Since the situation leading to this hazard is external to the Vantage system, protective measures attempted from within the system would be impractical and ineffective. User information shall be provided to warn the user of this hazard and identify control measures they can take.

Risk Control Measures to be Verified:

AC Line Connections Warning (UI.UE.1): Vantage system shall include user information warning the user of the potential hazard of ground faults or excessive leakage current when assembling an investigational system with multiple AC line-powered devices. User should subject the overall system to testing for ground impedance, line isolation, and leakage current. An external isolation transformer can be added if leakage current is excessive. These AC line safety tests should be repeated whenever the system has been disassembled and reassembled, or subjected to rough transport or other environmental stresses.

Residual Risk: 16 Acceptable (Severity: Minor Probability: Remote) If the user follows the suggested guidelines, the risk of electric shock from their investigational system will be no greater than for AC line powered commercial medical devices that have gone through formal regulatory submission, testing, and approval.

New Risks: No new potential hazards are created if the user follows the stated guidelines.

H.UE.2 Electric shock from user contact with internal wiring with covers removed.

Relative Risk Level: 9 Marginal (Severity: Serious Probability: Occasional)

Description & Evaluation: If a user operates the Vantage system with the covers removed, or if the user has modified the system in a way that compromises the integrity of the covers, then there is a risk that a user could accidentally come in contact with exposed, potentially hazardous voltage levels within the system. The system does not provide interlocks to disable power when covers are removed. An inherent safety by design approach reduces the probability of this situation, since the system is designed such that the user should never need to remove the covers and all service or repair is to be done by Verasonics, not the customer. Anti-tampering seals are applied by Verasonics to the screws that retain the side covers. These will further discourage customers from opening the system, and will allow Verasonics to determine if that has been done.

Risk Control Options: While it would be possible to provide interlocks to disable power when covers are removed, this would significantly impair the utility of the system for its intended use in the research and development environment, where users of the system should have the skills and training to qualify them for working around exposed potentially hazardous voltages. User information shall be provided to warn the user of this potential hazard, and steps they can take to minimize the risk.

Risk Control Measures to be Verified:

User Tamper Avoidance Warning (UI.UE.2A): The system documentation shall include a user warning that there are no user-serviceable components inside the system, and that the system must be returned to Verasonics for repair, upgrades, or other HW maintenance. Unauthorized tampering by the user may result in cancellation of the system warranty.

Internal Electric Shock Warning (UI.UE.2B): Vantage system shall include user information warning the user of the presence of potentially hazardous voltages at exposed points within the system when covers are removed, and that system must always be operated with all covers securely in place. Some system test activities may require operation with covers removed, but such activities should only be done by trained and qualified personnel who are aware of the hazards.

Residual Risk: 15 Acceptable (Severity: Serious Probability: Improbable) If the user follows the suggested guidelines and warnings, the probability of exposure will be dramatically reduced.

New Risks: No new potential hazards are created if the user follows the stated guidelines.

H.UE.3 System cooling and EMC features are degraded with covers removed.

Relative Risk Level: 14 Marginal (Severity: Minor Probability: Occasional)

Description & Evaluation: If a user operates the Vantage system with the covers removed, or if the user has modified the system in a way that compromises the integrity of the covers, then the effectiveness of the system's forced-air cooling and EMC shielding will be significantly degraded. This in turn could affect the Relative Risk Levels and control measures for other hazards identified in the Vantage system risk analysis. The severity of this situation is difficult to assess, since it will depend on the specific circumstances associated with the use of the system.

Risk Control Options: While it would be possible to provide interlocks to disable power when covers are removed, this would significantly impair the utility of the system for its intended use in the research and development environment as discussed in H.UE.2. User warnings not to open or tamper with the system, as identified in UI.UE.2, will reduce the probability of occurrence of this hazard.

Risk Control Measures to be Verified:

Cover Warning (UI.UE.3): Vantage system shall include user information warning the user that covers must be properly installed while system is in use, and that the covers are required for proper functionality of the system cooling and EMC shielding.

Residual Risk: 17 Acceptable (Severity: Minor Probability: Improbable) If the user follows the suggested guidelines, the probability of harm will be dramatically reduced.

New Risks: No new potential hazards are created if the user follows the stated guidelines.

H.UE.4 User application script sets excessive acoustic output levels.

Relative Risk Level: 12 Marginal (Severity: Minor Probability: Frequent)

Description & Evaluation: As a key aspect of the Vantage system's design for use in the research and development environments, it provides direct independent control from the user's application SW script of all operating state parameters that affect acoustic output: transmit waveform, transmit aperture steering and focusing, transmit output Voltage level, PRF and frame rate. It is the responsibility of the user's application script to manage these parameters such that acoustic output remains within the applicable regulatory and safety limits for the specific transducer and clinical application(s) being used with the system. The Vantage system by itself provides no comprehensive mechanism for managing acoustic output levels. The Vantage system's transmit power supply has an output capacity of approximately 150 Watts, to allow rapid transitions from one voltage to another at system mode changes. For the HIFU configuration, total available transmit output power can exceed 1000 Watts. In the context of a user script programming error, much of this output capacity could be delivered directly to the transducer resulting in an acoustic output level that could potentially be well above the regulatory limits for diagnostic ultrasound imaging (or the higher levels as set by the user for therapeutic HIFU applications). In light of this, the severity is rated as minor and the probability as frequent, in the absence of adequate acoustic output level controls in the user's script.

Risk Control Options: The architecture of the Vantage system is structured to provide the user with an extremely flexible platform for research and development activities. A key aspect of this architecture is that responsibility for acoustic output control resides in the user's control SW. The Vantage system by itself does not provide automatic acoustic output control or limiting functions, since it is up to the user to define appropriate limits for a specific clinical application, transducer, and operating state. Therefore user information is the only option available for controlling this risk. The Vantage system does, however, provide features that can augment acoustic output control functions in the user's application SW.

Risk Control Measures to be Verified:

Transmit HV Maximum Limit (RC.UE.4A): To facilitate user implementation of mechanisms for acoustic output control, the Vantage system shall provide a user-programmable maximum limit to the transmit HV power supply Voltage setting with a separate independent limit for each of the TPC profiles supported by the system, including Profile 5 for Extended Transmit or HIFU applications.

Transducer ID EEPROM Codes (RC.UE.4B): Vantage system shall provide a mechanism for reading a transducer ID code (and optional transducer calibration data) from the physical transducer. User's SW control script can use this feature to ensure that the SW is compatible with the connected transducer.

Acoustic Output Control Warning (UI.UE.4): Vantage system shall include guidelines for the user on managing acoustic output levels in their system control SW scripts, covering the system parameters that affect acoustic output and how they interact; example algorithms for limiting acoustic output; how to use the maximum HV supply level

control limit and transducer ID code features; some guidance on use of instrumentation to measure actual acoustic output levels from the transducer; the need for thorough verification testing to ensure the acoustic output control functions are working properly; and the need for rigorous HW configuration and SW revision control techniques. User must also be warned that the example programming scripts included with the Vantage system for use with commercially available transducers do not provide any mechanism for control of acoustic output levels and thus should not be used for imaging of human subjects without adding output limits based on testing of actual acoustic output levels.

Residual Risk: 16 Acceptable (Severity: Minor Probability: Remote) If the user follows the suggested guidelines, the probability of harm can be reduced- but an assessment of the residual Relative Risk Level must be done as part of the user's own risk analysis process for their specific investigational system.
New Risks: No new potential hazards are created if the user follows the stated guidelines.

H.UE.5 Potential for patient harm from direct contact with transducer

Relative Risk Level: Unknown

Description & Evaluation: Since the patient is in direct contact with the transducer, there are numerous potential ways in which a patient could be exposed to the risk of harm from that contact such as: biocompatibility or sterility problems; electric shock; transducer heating; electromagnetic emissions (either directly or through their impact on other medical equipment). These potential hazards are separate from and in addition to the acoustic output issues covered elsewhere in this risk analysis. Since the nature of any patient contact and the system operating state during that contact are set by the user and unknown to Verasonics, Verasonics cannot estimate the potential risk from these other factors.

Risk Control Options: Since the potential hazards listed above result primarily from the design of the transducer itself and the manner in which the transducer is being used with the system, no effective control measures can be provided by the Vantage system other than to include user information alerting them to these potential hazards and the need for the user to conduct a risk analysis to assess and control them.

Risk Control Measures to be Verified:

Transducer Safety Warning (UI.UE.5): Vantage system shall include user information warning the user of the potential risks associated with transducer patient contact, and the need to conduct a risk analysis of the transducer design and intended use to minimize those risks.

Transducer Labeling (RC.UE.5): For any transducers sold directly by Verasonics for use with a Verasonics system, a label shall be applied to the transducer clearly indicating that the transducer is not for use on human subjects. Documentation shall be provided to the user explaining that no safety analysis or qualification testing has been done on these transducers, and it is the user's responsibility to conduct a risk analysis and perform any testing deemed necessary based on that analysis, before using any Verasonics-supplied transducer on a human subject.

Residual Risk: Unknown (must be determined by the user).

New Risks: Unknown (must be determined by the user).

H.UE.6 Hazardous condition resulting from liquid spills onto or into system

Relative Risk Level: 14 Marginal (Severity: Minor Probability: Occasional)

Description & Evaluation: The Vantage system enclosure and internal HW design are not intended to provide any level of protection from liquid spills. Exposure to a spill could significantly disrupt system functionality, including the performance of risk control features identified elsewhere in this document, and thus subject the user and patient to an increased Relative Risk Level.

Risk Control Options: Adding any level of spill immunity would be counter to the intended use objectives for the system, and may also compromise performance of other system features such as the forced-air cooling system. Therefore user information is the only applicable option.

Risk Control Measures to be Verified:

Spills Warning (UI.UE.6): Vantage system shall include user information warning the user of the potential risks from spills when the system is used in a clinical environment. When the user assembles an investigational device using the Vantage system, they must take care not to restrict cooling airflow through the system yet at the same time protect if from liquid spills.

Residual Risk: 17 Acceptable (Severity: Minor Probability: Improbable) If the user follows the suggested guidelines, the probability of harm will be dramatically reduced.

New Risks: No new potential hazards are created if the user follows the stated guidelines.

H.UE.7 Patient harm due to operator error.

Relative Risk Level: 17 Acceptable (Severity: Negligible Probability: Probable)

Description & Evaluation: When a user assembles an investigational device for use on human subjects based on the Vantage system, the device's features, user interface, and overall behavior may differ significantly from typical commercial ultrasound systems. In light of this, the user should provide ample training and practice time with the system for operators who will be using it on human subjects to minimize the chances for operator errors. (See UI.UE.7.) Note, however, that if the investigational system is being used in a manner consistent with the intended use statement for this risk analysis (Intended Use cases 1 and 2, where the system does not contribute directly to patient care, treatment, or diagnosis) then the severity of this potential hazard is negligible since it would be no more than an annoyance to the user and patient. If the user has designed adequate acoustic output level controls into their control SW, it should not be possible for the operator to put the system into a state with excessive acoustic output (see H.UE.4).

Similar concerns arise with regard to installation and setup of a Vantage-based investigational device or early product prototype: the developer of the system must provide sufficient documentation and instructions to ensure users will be able to install it correctly and complete any required setup, calibration, or system test procedures prior to use.

Risk Control Options:

User Training Warning (UI.UE.7): Vantage system shall include user information warning of the need to provide adequate training and instructions for operators who will be setting up or using a Vantage-based investigational system on human subjects since the system's installation requirements, features, user interface, and overall behavior may differ significantly from typical commercial ultrasound systems.

H.UE.8 Transmit waveform programming error results in excessive acoustic output.

Relative Risk Level: 14 Marginal (Severity: Minor Probability: Occasional)

Description & Evaluation: The "arbitrary transmit waveform" capabilities of the Vantage system are intended to allow the user to define transmit waveforms with virtually any desired duration, pulse shape, frequency content, etc. Along with this flexibility comes an increased risk that a user error in the definition of the transmit waveform could result in acoustic output levels very different than what was intended.

Risk Control Options: To reduce the probability of exposure to undetected waveform definition errors, the system shall include user information on the need to verify the actual transmit waveform matches their intent, and to measure actual acoustic output levels before using the system on live subjects.

Risk Control Measures to be Verified:

User Transmit Verification Warning (UI.UE.8): System shall include clear documentation of the need to verify the correct implementation of an arbitrary waveform definition, and suggestions of test techniques to facilitate that verification.

Residual Risk: 16 Acceptable (Severity: Minor Probability: Remote) If the user follows the stated guidelines and conducts appropriate verification tests, probability of an undetected fault or programming error will be significantly reduced.

New Risks: none.