Author: Allan Marinelli

Published on IVT Network (www.ivtnetwork.com)

JVT Volume 27, Issue 1 – February 2021

IVT NETWORK
INSTITUTE OF VALIDATION TECHNOLOGY
an informa business

PEER REVIEWED

COMPLETING A RISK ANALYSIS USING A FMEA APPROACH FOR RADIO FREQUENCY MONITORING DEVICES

An Instructional Overview

INTRODUCTION

Conducting a risk analysis on systems is more pertinent today than ever, as companies cannot afford to test every single attribute as part of the process/system design with results having little or no significant impact to quality and/or to GxP systems altogether. Whether control systems, computerized systems, automation systems, information technology systems, artificial intelligence systems, robotic systems, or radio frequency devices, we must consider the rapid change in technology along with the frequent changes to industry standards. The amalgamation of rapidly emerging technologies, increasing design standards and audit trails can benefit from FMEA review process. This process may assist in producing more accurate/precise outputs while maintaining data integrity and maintaining good practices (proper adherence) around CFR Part 11 and Annex 11 regulations for the Pharmaceutical, Medical Devices (Class I, II and III), Combination Products (Drug, Device and Biologics), Health, Food/Beverage industries, including all its related Cold Chain Management requirements/specifications controls throughout the life cycle of using these devices.

RADIO FREQUENCY (RF) DEVICES

A radio frequency (RF) can be defined as an RF signal refers to an electromagnetic signal used as a form of communication if one is discussing wireless electronics. Radio waves are a form of electromagnetic radiation with identified radio frequencies that range from 3kHz to 300 GHz. Frequency refers to the rate of oscillation of the radio waves 1.

RF modules, transceivers, and SoCs (System on Chip)2 often include data link layer support for one or more wireless communication protocols. These products are organized by wireless technology that entails “Bluetooth Signals, ZigBee Signals, Wi-Fi Signals, GPS Signals etc1. For additional information pertaining to Bluetooth Signals, ZigBee Signals, Wi-Fi Signals, and GPS Signals, refer to the definition section.

The data logger types (Probes) of equipment that would use RF devices involves capturing and monitoring data containing the following datapoints

(1) Differential Pressure
(2) CO2
(3) Temperature
(4) Humidity
(5) Dry Contact
(6) 4 to 20mA, and 0 to 5 Volts Data points (Probe) including the capacity to create additional data parameters

RISK ANALYSIS SECTIONS

There are many methods or practices in employing risk analysis whether the quantitative approach or the qualitative approach. Either would be conducted through employment of the proactive systematic method of evaluating a system or process of

Author: Allan Marinelli

Published on IVT Network (www.ivtnetwork.com)

JVT Volume 27, Issue 1 – February 2021

IVT NETWORK
INSTITUTE OF VALIDATION TECHNOLOGY
an informa business

PEER REVIEWED

utilizing the "Failure Mode and Effective Analysis" (FMEA) that is often used in Lean Six. The column sections of the FMEA constitutes the main sections as indicated below:

(1) URS or FS References
(2) Description
(3) Risk Identification that contains the following subsections:
    a. Failure Mode
    b. Effect
    c. Cause
(4) Risk Evaluation that contains the following subsections:
    a. Impact
    b. Detectability
    c. Initial Risk
(5) Risk Control that contains the following subsections:
    a. Risk Mitigation
    b. Final Risk
    c. Risk Verification
    d. Risk Acceptance

Each row of the FMEA with respect to the risk analysis consists of the following RF sections:

1. General Risk of the System	**2. Regulatory Potential Risk of the System**	**3. Business Potential Risk**
4. Potential Hosting and Type Risk	**5. Potential Risk of Data Classification**	**6. Risk Associated with the Equipment**
7. Utilities	**8. Training**	**9. Documentation**
10. Calibration	**11. Maintenance and Support**	**12. Commissioning**
13. Qualification	**14. General: Process and Alarms**	**15. Detail: Process Control and Alarms**
16. Design Requirements	**17. Software**	**18. Data Integrity of Software**
19. Hardware	**20. Overall Size Limitation**	**21. Standards**
22. CO2 Monitoring	**23. Pressure Monitoring**	**24. Differential Pressure Monitoring**
25. Analog Signal Monitoring	**26. Temperature Monitoring**	**27. Dry Contact Monitoring**
28. Environmental Limitations	**29. Function: Data Emission**	**30. Function: Data Acquisition**
31. Sensor Component	**32. Health and Safety**	**33. Receptor Component**

Author: Allan Marinelli

Published on IVT Network (www.ivtnetwork.com)

JVT Volume 27, Issue 1 – February 2021

IVT NETWORK
INSTITUTE OF VALIDATION TECHNOLOGY
an informa business

PEER REVIEWED

SUMMARY

By using the qualitative approach through the deployment of utilizing the FMEA methodology that contains the main sections of URS or FS Reference, Risk Identification, Risk Evaluation and Risk Controls, a risk analysis can be successfully conducted pertaining to RF monitoring devices.

Refer to attachment A that entails the procedure and accompanying FMEA risk analysis for the RF monitoring devices.

Author: Allan Marinelli

Published on IVT Network (www.ivtnetwork.com)

JVT Volume 27, Issue 1 – February 2021

IVT NETWORK
INSTITUTE OF VALIDATION TECHNOLOGY
an informa business

PEER REVIEWED

ATTACHMENT A

PROCEDURE

1) ***Identifier Number/URS/FS and Description***: In the respective column of the FMEA work sheet on the next pages, identify the corresponding URS or FS or other applicable reference identifier to delineate each corresponding potential failure modes as described in the "Description Column" relative to the system, and system components at question.
2) ***Risk Identification*****:** At a minimum, for each mode identified in the description column account for the negative condition to represent the "Failure Mode" column scenario, and continue to populate the next subsequent columns to relate with its "Effect", and "Cause" respectively. This would equate to represent the "Risk Identification" portion of the FMEA.
    a. You may need to add additional failure modes where warranted relative to the same description if more than one failure mode potentially exists.

3) *Risk Evaluation:*

a. With respect to the "Impact" Column, identify the potential failure mode relative to affecting quality as either "C" to represent critical, "M" to represent Major, "m" to represent minor, or "b" to represent business.
    i. The 'Impact" Column represents an overall encompassing combination of factoring in the "Severity" (Impact on Patient Safety, Product Quality, and Data Integrity or other Harm) of the event times the "Probability or Frequency" (Likelihood of the fault occurring or evaluated to occur "Often or Numerous Times or a Few Times or Rarely or Once" equating to Risk Class per GAMP 5 definition). Therefore, the resultant Severity times the Probability would equate to a qualitative designation of "C", or "M: or "m" or "b". Use the first table (Probability versus Severity) delineated in the GAMP 5 "A Risk-Based Approach to Compliant GxP Computerized Systems, 2008, Appendix M3 page 115 (4) to further understanding on applying Severity and Probability so you can subsequently reach a conclusion on assessing the impact Column.
    ii. NOTE: "C" equates to High Risk Class 1 whereas "M" equates to Medium Risk Class 2 while "m" equates to a Low Risk Class, and "b" designation per the nomenclature used in this article is intended to reflect low or very low risk to Quality impact and therefore equated to be Risk Class 3 relative to GAMP 5 terminology and intent.
        1. Typically the "b" was used for business non-GxP scenarios with low Quality Impact and therefore the "b" would be transcribed in the column while in some cases the "b" can involve a business with a High Criticality Priority coupled with a High GxP Quality Impact. In that case (High Criticality Business Impact and High Quality Impact), then we would assign in the Impact Column a "C_b" while in the "Initial Risk" column an "H" for High. For example, the Enterprise Resource Planning Software Data-Base is intended to be used for business applications such as Oracle. Oracle can be evaluated as a High business criticality Impact while encompassing a High GxP Quality Impact leading to an overall Initial Impact as High in this case.

2. The discussion of the details of Oracle is outside the scope of the intent of this article but used as an example to demonstrate the potential relationship of factoring in the "b" impact to result in an "H" in the "Initial Risk" Column.

b. With respect to the "Detectability" Column, identify the detectability level of detecting the potential mode failure as "H" for High, "M" for Medium, or "L.
   i. Use the second table (Detectability versus Risk Class) delineated in the GAMP 5 "A Risk-Based Approach to Compliant GxP Computerized Systems, 2008, Appendix M3 page 115 to further your understanding on applying Severity and Probability so you can subsequently reach a conclusion on assessing the impact Column.

c. Determine the initial risk level as "L", "M", or "H" based on the input information provided in both impact column and detectability column while referencing the two tables delineated in the GAMP 5 "A Risk-Based Approach to Compliant GxP Computerized Systems, 2008, Appendix M3 page 115.

4) ***Risk Control***

a. Identify the potential Risk Mitigation as part of the "Risk Mitigation" column that the company can use to reduce the inherent risk of the system by design

b. Based on the input information provided in the Risk Evaluation columns, coupled with using the two tables delineated in the GAMP 5 "A Risk-Based Approach to Compliant GxP Computerized Systems, 2008, Appendix M3 page 115, determine the final risk as either High (H), Medium (M) or Low (L). An explanation on how the two tables can be interpreted was delineated and rationalized in the Risk Evaluation section.

c. If the company is going to conduct Script Testing, Stress Testing, Regression Testing, Validation Information Technology Testing, Computer System Validation Testing or other applicable Testing in order to test the design of the system for substantiating that the system is functioning or operating as intended in alignment with URS, FS, or FDS, then document what type of testing for that particular failure mode was performed or will be performed.

d. Determine the risk acceptance (Risk Acceptance Column) per failure mode while factoring in all input information from the previous columns.
   i. Moreover, with respect to the "Risk Acceptance" column while some stakeholders would name this "Final Accepted Risk or Final Risk", one needs to factor in the robustness and quality effectiveness of the mitigation method used or determined to be holistically claimed or stipulated as such that would constitute the rationalization basis for the company to convey to the FDA or other regulatory bodies representing a justifiable foundation of defense.
   ii. **NOTE**: Typically, the "Risk Acceptance" would be evaluated as one grade or level lower than the initial "Impact" (Equivalence to the determination of the Initial Risk) as established in the "Risk Evaluation Phase" provided ample robustness for justifying such claims are in place; Through subsequent rigor of testing such as the successful completion of adequately factoring in the requirements, in alignment with GAMP 5 guidance during the development of the IOQs and/or PQs or other script/protocol/test cases/test scenarios of testing etc, the overall risk would result in being assessed as a lower risk within the "Risk Control" phase" that is documented within the "Risk Acceptance " column. Conversely, if there was no justifiable testing to include IOQs and/or PQ or

Author: Allan Marinelli

Published on IVT Network (www.ivtnetwork.com)

JVT Volume 27, Issue 1 – February 2021

IVT NETWORK
INSTITUTE OF VALIDATION TECHNOLOGY
an informa business

PEER REVIEWED

the current IOQs and/or PQs were deficient that included many gaps without alignment with GAMP 5 guidance and/or violating the company's Quality policies, SOPs, then the "Risk Acceptance" or Final Risk Acceptance would be equal to or equivalent to the "Initial Risk" in that case.

NOTE: It is highly suggested to complete this FMEA using a cross-functional team or various stakeholders representing different departments or roles within the organization.

Author: Allan Marinelli

Network (www.ivtnetwork.com)

IVT NETWORK
INSTITUTE OF VALIDATION TECHNOLOGY
an informa business

Published on IVT

JVT Volume 27, Issue 1 – February 2021

PEER REVIEWED

Risk Analysis Using a FMEA Approach for Radio Frequency Monitoring Devices[1]

URS or FS Reference	Description	Risk Identification			Risk Evaluation			Risk Control			
		Failure Mode	Effect	Cause	Impact: C, M,m,b	Detectability: H, M, L	Initial Risk	Risk Mitigation	Final Risk	Risk Verification	Risk Acceptance
General Risk of the System											
1	The system and its ancillary components must conform to material engineering specification	Not meeting specification	The system is in-operative	Supplier or Vendor Issue	C	H	M	• A vendor/ Supplier Audit was conducted • Assessment of material engineering construction was performed on designated Devices and its ancillary components	L	IQ	L
2	The surfaces of non-product contact materials surfaces must be cleanable, resistant to cleaning agents and no cracks or any allowable penetration to affect the operation or to contaminate the device. **NOTE**: If this device is used in a classified area or area with the possibility of potential risk to the product functionality or contamination, then this requirement is applicable else non-applicable	Cleaning Ineffective	Contamination or damage to the device	Design inadequate	C	M	H	• A cleaning procedure was in place • Material certificate provided by the supplier	L	IQ	L
3	Product contact materials must be corrosion resistant to cleaning agents, surfaces cleanable without wore/tear on device, and compatible with all the product components **NOTE**: If this device is used in a classified area or area with the possibility of potential risk to the product functionality or contamination, then this requirement is applicable else non-applicable	• Cleaning Ineffective • Deterioration or degradation of the device materials	Contamination or damage to the device	Design inadequate	C	M	H	• A resilient protective coating on the device is impregnated as part of the material of construction to inhibit the deterioration of the materials	L	IQ	L

Author: Allan Marinelli

Network (www.ivtnetwork.com)

IVT NETWORK
INSTITUTE OF VALIDATION TECHNOLOGY
an informa business

Published on IVT

JVT Volume 27, Issue 1 – February 2021

PEER REVIEWED

URS or FS Reference	Description	Risk Identification			Risk Evaluation			Risk Control			
		Failure Mode	Effect	Cause	Impact: C, M,m,b	Detectability: H, M, L	Initial Risk	Risk Mitigation	Final Risk	Risk Verification	Risk Acceptance
4	The sensor, receptor, repeater allow easy and thorough cleaning to prevent cross-contamination. **NOTE**: If this device is used in a classified area or area with the possibility of potential risk to the product functionality or contamination, then this requirement is applicable else non-applicable	Cleaning Ineffective	Contamination or damage to the device	Design inadequate	C	M	H	• A cleaning procedure was in place • Material certificate provided by the supplier	L	IQ	L
5	The field conditions of the devices match the list of parameters outlined in the User Requirement Specification (URS)	The field conditions are not matching the URS or URS not clearly defined to match the original intended field conditions	The devices not matching the URS	Inaccurate URS	M	H	L	• The URS is continuously be updated as part of the life-cycle process and any anomalies discovered would be quickly corrected. Typically, the written specifications are not defined clearly signifying documentation discrepancies and quickly corrected after the fact versus in correctly receiving the wrong device or wrong device discovered in the field, notwithstanding	L	DQ	L
Regulatory Potential Risk of the System											

Author: Allan Marinelli

Network (www.ivtnetwork.com)

IVT NETWORK
INSTITUTE OF VALIDATION TECHNOLOGY
an informa business

Published on IVT

JVT Volume 27, Issue 1 – February 2021

PEER REVIEWED

URS or FS Reference	Description	Risk Identification			Risk Evaluation			Risk Control			
		Failure Mode	Effect	Cause	Impact: C, M,m,b	Detectability: H, M, L	Initial Risk	Risk Mitigation	Final Risk	Risk Verification	Risk Acceptance
6	(1) GMP Direct Impact? **(Yes)** (2) GCP/GLP Impact?**(Yes)** (3) GPVP Impact? **(Yes)** (4) Medical and/or Clinical Device **(Yes)** (5) Sox Impact? **(No)** (6) Transparency Impact (Sunshine Act; European Federation of Pharmaceutical Industries Association; Australian Transparency Requirements)? **(No)** (7) Data Retention Applicability? **(Yes)** (8) Electronic Record and Electronic Signatures" **(Yes)** (9) Privacy Impact? (Pertaining to Personal Information/ Personal Identifiable Information; Personal Health Information / Protected Health Information (PHI); Sensitive Personal Information; Pseudonymized/Anonymized Data; Personal data from residents of the European Union, or data that has originated from within EU borders; Personal Data from Canada, Asia, Russia Etc) **(Yes)** 10) Audit Trail Applicability (Audit Trail Review)? **(Yes)** 11) GxP Data Criticality? **(Yes)** 12) Data Classification? Critical; **Major**; Minor	Any violations or contradictions to the "Yes" replies as stipulated in the twelve (12) points highlighted in the description column of this row, would result in a **"Failure"** condition	A high probability of scrutinization of the system during a regulatory inspection	Failure to comply with the "Yes" attestations outlined in the description column	C	M	H	• DQ, IQ, and OQ	H to M	QA verification of completeness adhering to GAMP 5 approach (Guidelines) and company's policies, Master Plan. A final report summarizes (e.g: mentioning Electronic Records and/or Electronic Signatures or both conditions as applicable) the details of the system	M

Author: Allan Marinelli

Network (www.ivtnetwork.com)

IVT NETWORK
INSTITUTE OF VALIDATION TECHNOLOGY
an informa business

Published on IVT

JVT Volume 27, Issue 1 – February 2021

PEER REVIEWED

URS or FS Reference	Description	Risk Identification			Risk Evaluation			Risk Control			
		Failure Mode	Effect	Cause	Impact: C, M,m,b	Detectability: H, M, L	Initial Risk	Risk Mitigation	Final Risk	Risk Verification	Risk Acceptance
Business Potential Risk											
7	(1) Business Processes (Medium Overall Impact_ business Mission Critical) and Recovery Criticality? **(Yes)** (2) Low Impact plus revenue impact; negative customer satisfaction, compliance violation, damage to organizations' reputation, and/or risk to human health/environment unless manual control process is implemented by default	**"Failure"** of business process	A high probability of scrutinization of the system during a regulatory inspection	Failure to comply with the "Yes" attestations outlined in the description column	C	M	H	• DQ, IQ, and OQ	H to M	QA verification of completeness adhering to GAMP 5 approach (Guidelines) and company's policies, Master Plan. A final report summarizes (e.g: mentioning Electronic Records and/or Electronic Signatures or both conditions as applicable) the details of the system	M
Potential Hosting and Type Risk											
8	Third-Party Hosting Risk Impact Alarm Service monitoring **(Yes)**	**"Failure"** of the Parameter /Attribute specified in the description	A high probability of scrutinization of the system during a regulatory inspection	Failure to comply with the "Yes" attestations outlined in the description column	C	M	H	• DQ, IQ, and OQ	H to M	QA verification of completeness adhering to GAMP 5 approach (Guidelines) and company's policies, Master Plan. A final report summarizes (e.g: mentioning Electronic Records and/or Electronic Signatures or both conditions as applicable) the details of the system	M
9	On-Premise Risk Impact **(Yes)**	**"Failure"** of the Parameter /Attribute specified in the description	A high probability of scrutinization of the system during a regulatory inspection	Failure to comply with the "Yes" attestations outlined in the description column	C	M	H	• DQ, IQ, and OQ	H to M	QA verification of completeness adhering to GAMP 5 approach (Guidelines) and company's policies, Master Plan.	M

Author: Allan Marinelli

Network (www.ivtnetwork.com)

IVT NETWORK
INSTITUTE OF VALIDATION TECHNOLOGY
an informa business

Published on IVT

JVT Volume 27, Issue 1 – February 2021

PEER REVIEWED

URS or FS Reference	Description	Risk Identification			Risk Evaluation			Risk Control			
		Failure Mode	Effect	Cause	Impact: C, M,m,b	Detectability: H, M, L	Initial Risk	Risk Mitigation	Final Risk	Risk Verification	Risk Acceptance
										QA verification of completeness adhering to GAMP 5 approach (Guidelines) and company's policies, Master Plan. A final report summarizes (e.g: mentioning Electronic Records and/or Electronic Signatures or both conditions as applicable) the details of the system	
10	Website Risk Impact Public **(Yes)**	**"Failure"** of the Parameter /Attribute specified in the description	A high probability of scrutinization of the system during a regulatory inspection	Failure to comply with the "Yes" attestations outlined in the description column	C	M	H	• DQ, IQ, and OQ	H to M	QA verification of completeness adhering to GAMP 5 approach (Guidelines) and company's policies, Master Plan. A final report summarizes (e.g: mentioning Electronic Records and/or Electronic Signatures or both conditions as applicable) the details of the system	M
11	Software As A Service (SaaS)_**(Yes)** Platform As A Service (PaaS)_ **(Yes)** Infrastructure As a Service_ **(Yes)**	**"Failure"** of the Parameter /Attribute specified in the description	A high probability of scrutinization of the system during a regulatory inspection	Failure to comply with the "Yes" attestations outlined in the description column	C	M	H	• DQ, IQ, and OQ	H to M	QA verification of completeness adhering to GAMP 5 approach (Guidelines) and company's policies, Master Plan. A final report summarizes (e.g: mentioning Electronic Records and/or Electronic Signatures or both conditions as	M

Author: Allan Marinelli

Network (www.ivtnetwork.com)

IVT NETWORK
INSTITUTE OF VALIDATION TECHNOLOGY
an informa business

Published on IVT

JVT Volume 27, Issue 1 – February 2021

PEER REVIEWED

URS or FS Reference	Description	Risk Identification			Risk Evaluation			Risk Control			
		Failure Mode	Effect	Cause	Impact: C, M,m,b	Detectability: H, M, L	Initial Risk	Risk Mitigation	Final Risk	Risk Verification	Risk Acceptance
										applicable) the details of the system	
Potential Risk of Data Classification											
12	(1) Confidential/Restricted: Highly sensitive data intended for limited, specific use by a workgroup, department, or group of individuals that are legally bound to acquire authorization**….(Yes)** (2) Internal: Information that is belongs to the company only with respect to proprietary, ethical, or privacy considerations. Moreover, protection from unauthorized access (CyberSecurity), modification, transmission, storage or other use of information such as employment data, business partner, contracts etc**…. (Yes)** (3) Public…Information that may or must be open to the general public data, that is available to all employees and all individuals or entities external to the corporation including marketing materials. … **(Yes)**	**"Failure"** of the Parameter /Attribute specified in the description	A high probability of scrutinization of the system during a regulatory inspection	Failure to comply with the "Yes" attestations outlined in the description column	C	M	H	• DQ, IQ, and OQ	H to M	QA verification of completeness adhering to GAMP 5 approach (Guidelines) and company's policies, Master Plan. A final report summarizes (e.g: mentioning Electronic Records and/or Electronic Signatures or both conditions as applicable) the details of the system	M

Author: Allan Marinelli

Network (www.ivtnetwork.com)

IVT NETWORK
INSTITUTE OF VALIDATION TECHNOLOGY
an informa business

Published on IVT

JVT Volume 27, Issue 1 – February 2021

PEER REVIEWED

URS or FS Reference	Description	Risk Identification			Risk Evaluation			Risk Control			
		Failure Mode	Effect	Cause	Impact: C, M,m,b	Detectability: H, M, L	Initial Risk	Risk Mitigation	Final Risk	Risk Verification	Risk Acceptance
Risk Associated with the Equipment											
13	All associated connecting devices to the system that are being mechanical/analog or digital instruments type including their electrical components, cables per design must be correctly labelled/tagged on non-corrosive material and identified by a secure unadulterated method.	The systems' associated sensors and receptors cannot be traced	location cannot be identified	Inadequate identification	C	H	M	• A unique Identification is permanently stored in the local memory of the system as a digital tag output. Therefore, radio identification is till feasible nonetheless • The involvement of the IT department can be used to identify the Ethernet socket and its corresponding attributes	L	IQ	L
14	Probes data transmission will be conducted by using wireless connectivity / technology	Another method is used	Maintenance issue	Supplier Deficient	B	H	L	• A Design Specification is approved and updated periodically to ensure the requirement is met.	L	DQ OQ /PQ Regression Testing	L

Author: Allan Marinelli

Network (www.ivtnetwork.com)

IVT NETWORK
INSTITUTE OF VALIDATION TECHNOLOGY
an informa business

Published on IVT

JVT Volume 27, Issue 1 – February 2021

PEER REVIEWED

URS or FS Reference	Description	Risk Identification			Risk Evaluation			Risk Control			
		Failure Mode	Effect	Cause	Impact: C, M,m,b	Detectability: H, M, L	Initial Risk	Risk Mitigation	Final Risk	Risk Verification	Risk Acceptance
								• The required Hardware, Protocols, System Integrations, and Solution Scripting including regression testing is performed and completed as a requirement stipulated in the CSV/IT Program Management Master Plan			
15	IT Hardware (GAMP 5 Category 1L Infrastructure, servers, workstation etc)	Hardware and software do not abide to Design Specification	The System is functional despite not being in compliance to the deployment process stipulated in the User Requirement Specifications (URS), and Design Specifications (DS).	The URS and DS are not factored in	B	H	L	• A Design Specification is approved and updated periodically to ensure the requirement is met. • The required Hardware, Protocols, System Integrations, and Solution Scripting including regression testing is performed and completed as a requirement stipulated in the CSV/IT Program Management Master Plan	L	IQ	L
Utilities											

Author: Allan Marinelli

Network (www.ivtnetwork.com)

IVT NETWORK
INSTITUTE OF VALIDATION TECHNOLOGY
an informa business

Published on IVT

JVT Volume 27, Issue 1 – February 2021

PEER REVIEWED

URS or FS Reference	Description	Risk Identification			Risk Evaluation			Risk Control			
		Failure Mode	Effect	Cause	Impact: C, M,m,b	Detectability: H, M, L	Initial Risk	Risk Mitigation	Final Risk	Risk Verification	Risk Acceptance
16	Incoming Volts Supplied: from 100-240 Vac 50-60 Hertz	The system is not operational	No Data available	Electrical supply not available	M	H	L	• The wireless Probes represent a stand-alone system that retains sufficient power as part of its internal system to retain the data (data memory) upon power failure incident during the monitoring phase up to 48 hours. UPS (Uninterrupted Power Supply) is used to backup the servers in case of power loss	L	IQ	L
17	The system (Receivers, Repeaters, servers) will always be connected to a UPS regardless of a power loss or disaster recovery event	UPS not operational	During a power failure event, the system is not operational	UPS not functioning or disabled	M	H	L	• The wireless Probes represent a stand-alone system that retains sufficient power as part of its internal system to retain the data (data memory) upon power failure incident during the monitoring phase up to 48 hours. UPS is used to backup the servers in case of power loss	L	IQ	L
Training											

Author: Allan Marinelli

Network (www.ivtnetwork.com)

IVT NETWORK
INSTITUTE OF VALIDATION TECHNOLOGY
an informa business

Published on IVT

JVT Volume 27, Issue 1 – February 2021

PEER REVIEWED

URS or FS Reference	Description	Risk Identification			Risk Evaluation			Risk Control			
		Failure Mode	Effect	Cause	Impact: C, M,m,b	Detectability: H, M, L	Initial Risk	Risk Mitigation	Final Risk	Risk Verification	Risk Acceptance
18	Users including the vendors using the system are trained in company's SOP, User Access Controls, Segregation of Duties per Part 11 etc	Users not trained per SOP	Deficient in performing the tasks relative to the stipulation instructions in the SOP	Non-adherence to the SOP	M	H	L	• Users and Vendors (Vendor Qualification) are by default documented as part of their training portfolio prior to using the system per the requirements of the company	L	IQ	L
Documentation											
19	The complete list of documentation required for users to understand the operation, maintenance, troubleshooting scenarios amongst other needs is provided	Some missing documentation	Information inadequate	Vendor not in conformance with the company's requirements	M	H	L	• The URS contains the necessary information that would cross match the list of documentation	L	IQ	L

Author: Allan Marinelli

Network (www.ivtnetwork.com)

IVT NETWORK
INSTITUTE OF VALIDATION TECHNOLOGY
an informa business

Published on IVT

JVT Volume 27, Issue 1 – February 2021

PEER REVIEWED

URS or FS Reference	Description	Risk Identification			Risk Evaluation			Risk Control			
		Failure Mode	Effect	Cause	Impact: C, M,m,b	Detectability: H, M, L	Initial Risk	Risk Mitigation	Final Risk	Risk Verification	Risk Acceptance
20	The EOMs (Equipment Operation Manual) will be coherently written in English for users to comprehend the system.	Document not clearly delineated for the user to comprehend	The correct operation and maintenance of the system is not performed consistently but performed based on the users limited experience	Vendor not in conformance with the company's requirements	M	M	M	• Prior to accepting the list of documentation and submitting the information to the computer systems /Information Technology Team designees/users, the designated Leaders of each team that will need those documents shall thoroughly review the list of documentation against the requirements while factoring in that the written information is clearly delineated for the users to understand	L	IQ	L
21	Datasheets including system configuration setting for the relevant devices used, must be easily presented and configurable for the system Administer to interpret	Missing Data sheets so complete configuration of the system to meet the intended uses is not possible	Loss of system information	Vendor not in conformance with the company's requirements	C	H	M	• As part of the Design Specification review, this will ensure adherence to the requirements	L	IQ	L
Calibration											

Author: Allan Marinelli

Network (www.ivtnetwork.com)

IVT NETWORK
INSTITUTE OF VALIDATION TECHNOLOGY
an informa business

Published on IVT

JVT Volume 27, Issue 1 – February 2021

PEER REVIEWED

URS or FS Reference	Description	Risk Identification			Risk Evaluation			Risk Control			
		Failure Mode	Effect	Cause	Impact: C, M,m,b	Detectability: H, M, L	Initial Risk	Risk Mitigation	Final Risk	Risk Verification	Risk Acceptance
22	Annual Calibration Certificates of the primary standard used to calibrate the probes including the corresponding calibration data for the relevant probes/devices shall be provided by the vendor	Calibration Certificate not available or received	Vendor's Calibration Certificate Status is unknown or un-determined	Vendor not in conformance with the company's requirements	M	M	M	• A self-diagnostic preliminary test prior to commencing the monitoring phase shall include an internal calibration of devices on each Probe by default	L	OQ	L
23	Instruments will be calibrated per traceable NIST Standards or equivalent to the countries calibration requirements of the industry	Other Calibration Methods used not accepted by the industry at question	Calibration not meeting current industry acceptable standards delineated in the URS	Violation of the URS requirements	M	M	M	• All calibration of devices including external calibration performed are managed and verified against the company's internal calibration program	L	OQ	L
24	As part of receiving the devices, the company should also receive the interfacing tools or kits required to acquire the capabilities of conducting their own annual internal calibration of all devices	The Calibration Kits or Interface tools are not provided	Unable to correctly calibrate the devices to calibration conformance	Vendor not in conformance with the company's requirements	M	H	L	• All calibration of devices requiring the calibration kits or tools are inspected by the designated members of the team prior to accepting the system for operation.	L	OQ	L
Maintenance and Support											

Author: Allan Marinelli

Network (www.ivtnetwork.com)

IVT NETWORK
INSTITUTE OF VALIDATION TECHNOLOGY
an informa business

Published on IVT

JVT Volume 27, Issue 1 – February 2021

PEER REVIEWED

URS or FS Reference	Description	Risk Identification			Risk Evaluation			Risk Control			
		Failure Mode	Effect	Cause	Impact: C, M,m,b	Detectability: H, M, L	Initial Risk	Risk Mitigation	Final Risk	Risk Verification	Risk Acceptance
25	Availability of Sparts Parts upon request, Qualified Maintenance Designees upon a need, and sustaining the "Support/Service" of the users upon resolution of queries	Not meeting this requirement	Un-resolved Maintenance issues due to lack of Maintenance Management and Maintenance System not adequately put in place	Supplier deficient / No respect of the URS requirement	M	M	M	• There is a maintenance contract in place with third party contract that ensures maintenance and support to users upon request.	L	N/A	L
Commissioning											
26	Execution of Vendor Audit (As an example: On-site, Paper Based Mail Audit, Public Search/Web Audit, Postal Audit, Desktop Audit)	Audit not performed or in-adequately executed	Insufficient information pertaining to the practices of the Vendor	The request to submit an Audit inquiry was not done in a timely manner	M	H	L	• Vendor Audit is a requirement per the company and is performed on annual basis	L	IQ	L

Author: Allan Marinelli

Network (www.ivtnetwork.com)

IVT NETWORK
INSTITUTE OF VALIDATION TECHNOLOGY
an informa business

Published on IVT

JVT Volume 27, Issue 1 – February 2021

PEER REVIEWED

URS or FS Reference	Description	Risk Identification			Risk Evaluation			Risk Control			
		Failure Mode	Effect	Cause	Impact: C, M,m,b	Detectability: H, M, L	Initial Risk	Risk Mitigation	Final Risk	Risk Verification	Risk Acceptance
Qualification											
27	Qualification is a requirement per company's QA Policy and under regulations (FDA, EU, KFDA, CFDA etc)	The Qualification was not done adequately	The Qualification was not executed completely, or the existent deviations were not properly addressed to close the loop	Qualification in-adequacy	C	H	M	• Qualifications are conducted in a timely manner as directed by the procedures in place	L	N/A	L
28	The database (Uploads and Downloads) is in compliance with the mandates from 21 CFR Part 11	The database information content is not correct	The results obtained does not reflect actual conditions retrieved by the probe	Installation upload(s) and download(s) are corrupted	C	H	M	• The information retrieved and obtained by each probe is programmed to show the timestamp data (Secure encryption. Probe memory contains data, and meta data which can be easily retrieved and uploaded to the servers and computers) at any time	L	OQ and PPQ	L

Author: Allan Marinelli

Network (www.ivtnetwork.com)

IVT NETWORK
INSTITUTE OF VALIDATION TECHNOLOGY
an informa business

Published on IVT

JVT Volume 27, Issue 1 – February 2021

PEER REVIEWED

URS or FS Reference	Description	Risk Identification			Risk Evaluation			Risk Control			
		Failure Mode	Effect	Cause	Impact: C, M,m,b	Detectability: H, M, L	Initial Risk	Risk Mitigation	Final Risk	Risk Verification	Risk Acceptance
29	The database adhered to the security attestations stipulated in the 21 CFR Part 11 regulations	Potential database modification	Existent Database corruption and/or alterations to the database was feasible	Access to database was conducted by unauthorized personnel	C	L	H	• A general user attempting to directly access the Database is not permitted due the default programmed limitation of the software permission unless an authorized system administrator requires the permission level in advance • The allowable access rights to the Physical Server is limited to authorized secured IT designee(s) with the relevant security clearance	M	OQ and PPQ	L

Author: Allan Marinelli

Network (www.ivtnetwork.com)

IVT NETWORK
INSTITUTE OF VALIDATION TECHNOLOGY
an informa business

Published on IVT

JVT Volume 27, Issue 1 – February 2021

PEER REVIEWED

URS or FS Reference	Description	Risk Identification			Risk Evaluation			Risk Control			
		Failure Mode	Effect	Cause	Impact: C, M,m,b	Detectability: H, M, L	Initial Risk	Risk Mitigation	Final Risk	Risk Verification	Risk Acceptance
30		Access to the system is allowed by unauthorized users	User access rights are allowed despite not intended due to inadequate completion of the training directives by the user	Training is not accomplished nor completed by the user	C	M	H	• The trainings are conducted by the vendor in adherence to the operating manual	M	OQ and PPQ	L
31	Access Controls (Security Access; Proper User Access Controls such as segregation of Duties, Roles and Privileges are established, etc) per 21 CFR Part 11 compliance - Security access		User has more access rights than initially due to lack or insufficient training	The default permissible access to the system does not differentiate between trained versus non trained users	C	H	M	• The various types of users with predefined access levels are configured meeting the user requirement specifications exhibiting a triangular type structure whereby a lot of users will have limited access levels whereas the system administrator will be authorized to perform most functions or permissible tasks	M	OQ and PPQ	L

Author: Allan Marinelli

Network (www.ivtnetwork.com)

IVT NETWORK
INSTITUTE OF VALIDATION TECHNOLOGY
an informa business

Published on IVT

JVT Volume 27, Issue 1 – February 2021

PEER REVIEWED

URS or FS Reference	Description	Risk Identification			Risk Evaluation			Risk Control			
		Failure Mode	Effect	Cause	Impact: C, M,m,b	Detectability: H, M, L	Initial Risk	Risk Mitigation	Final Risk	Risk Verification	Risk Acceptance
32		Audit-trail defective or not correctly displayed relative to the User Requirement Specification	Incomplete information shown from the output of the audit trail	Audit-trail is not correctly configured to meet the intent and user requirement specifications	C	M	H	• The software is defaulted to be configured to activate the "Part 11" mode. Therefore, the audit trail feature is inherently activated to function meeting the User Requirement Specification	L	OQ and PPQ	L

Author: Allan Marinelli

Network (www.ivtnetwork.com)

IVT NETWORK
INSTITUTE OF VALIDATION TECHNOLOGY
an informa business

Published on IVT

JVT Volume 27, Issue 1 – February 2021

PEER REVIEWED

URS or FS Reference	Description	Risk Identification			Risk Evaluation			Risk Control			
		Failure Mode	Effect	Cause	Impact: C, M,m,b	Detectability: H, M, L	Initial Risk	Risk Mitigation	Final Risk	Risk Verification	Risk Acceptance
General: Process and Alarms											
33	The Process and Alarms output information is managed and controlled under the electronic records and electronic signature 21 CFR Part 11	The system is not abiding to 21 CFR Part 11	The users cannot use the system and/or any data attributed to this non activated 21 CFR Part 11 feature since this is deemed as unusable data and any batches manufactured under these conditions during a submission process will be classified as a "Failure" resulting in the batch to be either destroyed or to be put under quarantine conditions	Vendor is deficient since no option is configured for the user to either activate or deactivate the 21 CFR Part 11 feature	C	H	M	• The vendor adheres to the mandate from the user and per URS for allowing the software to select the 21 CFR Part 11 feature	L	OQ and PPQ	L
Detail: Process Control and Alarms											
34	The functionality of disabling or enabling the devices can be performed through the local operator interface.	Not operational per as described in the description field	The functionality of the system is impacted	Vendor not meeting the intent of the client with respect to the URS	M	H	L	• The Design Specification reviewed by both the vendor and the client prior to approval	L	DQ OQ	L
35	Alarm activation will send action notifications to the respective sites of the client	Not operational per as described in	The functionality of the system is impacted	Vendor not meeting the intent of the client with respect to the URS	C	H	M	• The Alarm notifications are handled by third party	L	OQ	L

Author: Allan Marinelli

Network (www.ivtnetwork.com)

IVT NETWORK
INSTITUTE OF VALIDATION TECHNOLOGY
an informa business

Published on IVT

JVT Volume 27, Issue 1 – February 2021

PEER REVIEWED

URS or FS Reference	Description	Risk Identification			Risk Evaluation			Risk Control			
		Failure Mode	Effect	Cause	Impact: C, M,m,b	Detectability: H, M, L	Initial Risk	Risk Mitigation	Final Risk	Risk Verification	Risk Acceptance
		the description field						• Users are trained with respect to how to handle notifications including the following up actions demanded by the procedure			
36	Three types of alarms conditions as configured: (1) **Main Alarm**: occurs when current real time measurement is higher and lower than the configured setpoints. (2) **Technical Alarm**: occurs when communication is loss due to power failure or disaster recovery incident. (3) **Warning Alarm**: When the system temporarily acknowledges the Main Alarm so the system can continue to proceed to the next steps in the operation	No existence of Main alarm despite exceeded	No indication of exceeding the configured setpoints	Bad configuration	C	H	M	• The alarm setpoints are reviewed, and pre-approve prior to system handover post-commissioning phase	L	OQ	L
37		No existence of technical alarm	Alarm on sensors not receptive to changes in signal output to generate an alarm	Installation of senor not in meeting the specifications or faulty sensor by manufacture	C	H	M	• The technical alarms are preconfigured and activated by default by the vendor	L	OQ	L
38		No existence of warning alarm	No alarms generated	Faulty	C	M	H	• The alarm setpoints are reviewed, and pre-approve prior to system handover post-commissioning phase • The technical alarms are preconfigured and activated by default by the vendor	M	OQ	L

Author: Allan Marinelli

Network (www.ivtnetwork.com)

IVT NETWORK
INSTITUTE OF VALIDATION TECHNOLOGY
an informa business

Published on IVT

JVT Volume 27, Issue 1 – February 2021

PEER REVIEWED

URS or FS Reference	Description	Risk Identification			Risk Evaluation			Risk Control			
		Failure Mode	Effect	Cause	Impact: C, M,m,b	Detectability: H, M, L	Initial Risk	Risk Mitigation	Final Risk	Risk Verification	Risk Acceptance
39		Server or alarm history repository failure	No alarms generated in repository database	Faulty	M	M	M	• An installation sensor warning is configured by default and any faulty repository would be displayed on the computer	L	OQ	L
40	The transmitter sends an emergency measurement output next transmission cycle result if the preconfigured conditions or pre-requisites are not be adhered to upon initially activating the system	The alarm does not activate to the next transmission iteration cycle	Faulty transmission output	Transmitter deficient	C	M	H	• More than one sensor/probe is position within the same area as a backup in case one of the sensors/probes are faulty or not operating as intended	M	OQ	L
41	All preconfigured default alarms by the vendor should be activated regardless of additional requested alarms imposed by the client	Pre-configured alarms not functional	Alarm doesn't appear within an expected timeframe	Component or preconfigured parameters not configured as expected per the URS	C	H	M	• Software reviews and acceptance are conducted in both factory acceptance testing and site acceptance testing	M	OQ	L
Design Requirements											
42	A temperature specification range of the probe/sensor will be configured in alignment with the specifications received	The sensor/probe is not configured with the Design Requirements	System not operational	Vendor deficient	C	H	M	• The Design Specification review is reviewed and approved by both vendor and the client	L	IQ OQ	L
43	The calibration material provided to the client must constitute ample materials, including mapping locations and standards in order to conduct the calibration of the devices as expected	Incorrect or incomplete materials required to complete the calibration of devices	Incorrect data acquisition or Calibration not conducted per instruction	Location of sensors/probes not positioned in the range as instructed	C	H	M	• A mapping sensor drawing is in place at the deployment of the project	L	IQ	L

Author: Allan Marinelli

Network (www.ivtnetwork.com)

IVT NETWORK
INSTITUTE OF VALIDATION TECHNOLOGY
an informa business

Published on IVT

JVT Volume 27, Issue 1 – February 2021

PEER REVIEWED

URS or FS Reference	Description	Risk Identification			Risk Evaluation			Risk Control			
		Failure Mode	Effect	Cause	Impact: C, M,m,b	Detectability: H, M, L	Initial Risk	Risk Mitigation	Final Risk	Risk Verification	Risk Acceptance
44	The vendor and client collaboration will ensure that the material of constructions of the sensors/probes will not directly or indirectly affect the quality of the product being mapped.	Material of construction is not compatible to the product being tested	Contamination	Vendor deficient	C	H	M	• The vendor provides upfront the material of construction specification sheet that is reviewed and approved by both vendor and the client for each sensor received prior to usage • Certificate of Material of Construction is provided for all devices used as part of the Validation Test Scripts	L	IQ	L

Author: Allan Marinelli

Network (www.ivtnetwork.com)

IVT NETWORK
INSTITUTE OF VALIDATION TECHNOLOGY
an informa business

Published on IVT

JVT Volume 27, Issue 1 – February 2021

PEER REVIEWED

URS or FS Reference	Description	Risk Identification			Risk Evaluation			Risk Control			
		Failure Mode	Effect	Cause	Impact: C, M,m,b	Detectability: H, M, L	Initial Risk	Risk Mitigation	Final Risk	Risk Verification	Risk Acceptance
Software											
45	Upon post shutdown occurrence, the system is designed to automatically start.	System Auto Start Failure	Manual restart is required since the system does not auto restart	Incorrect Configuration or corrupt application	M	H	L	• UPS of all applications and components including servers, receivers, and repeaters are in place	L	OQ	L
46	Standardization/Calibration of measuring ranges on the designated devices are performed per SOP	Standardization and Calibrations are performed outside of the designated assigned ranges	Calibration and Maintenance issue	Violation of Calibration and standardization specification	M	H	L	• System process integration is assigned and managed under IT for control • The development of the Scripts are conducted by IT to ensure correct functioning and abiding to the requirements	L	IQ	L
47	Software components are in compliance to IT requirements/specifications	Software components not meeting IT requirements	Application can be used in IT infrastructure outside of the IT predefined requirements	Violation of IT Requirements	B	H	L	• System process integration is assigned and managed under IT for control • The development of the Scripts are conducted by IT to ensure correct functioning and abiding to the requirements	L	OQ	L

Author: Allan Marinelli

Network (www.ivtnetwork.com)

IVT NETWORK
INSTITUTE OF VALIDATION TECHNOLOGY
an informa business

Published on IVT

JVT Volume 27, Issue 1 – February 2021

PEER REVIEWED

URS or FS Reference	Description	Risk Identification			Risk Evaluation			Risk Control			
		Failure Mode	Effect	Cause	Impact: C, M,m,b	Detectability: H, M, L	Initial Risk	Risk Mitigation	Final Risk	Risk Verification	Risk Acceptance
48	Audit-trails requirements are in alignment with the stipulations specified in the SOP	Audit Trail directives not adhered	No traceability in place to capture the audit trail requirements	Violation of the Audit Trail SOP	C	M	H	• The part 11 mode is configured on the software that is provided to the vendor by default which inherently constitutes the requirements of the audit trail paradigms and requirements	M	OQ and PPQ	L

Author: Allan Marinelli

Network (www.ivtnetwork.com)

IVT NETWORK
INSTITUTE OF VALIDATION TECHNOLOGY
an informa business

Published on IVT

JVT Volume 27, Issue 1 – February 2021

PEER REVIEWED

URS or FS Reference	Description	Risk Identification			Risk Evaluation			Risk Control			
		Failure Mode	Effect	Cause	Impact: C, M,m,b	Detectability: H, M, L	Initial Risk	Risk Mitigation	Final Risk	Risk Verification	Risk Acceptance
49	Back-up and restore tools are provided to the vendor in case of disaster recovery requirement.	No tools provided or available for backup and restore	No backup/restore in place under an expected amount of time to auto backup/restore	Backup/ Restore functionality inherent in the software not existent nor is there an existent Backup/ Restore plan in place	C	M	H	• The backup is performed through Application only Backup OR • An entire Backup of the system including the software and its corresponding Database (MySQL), configuration settings etc OR • Using the existent documentation that pre-defines how the system was initially configured in alignment with the Design Specifications including its default settings	M	OQ and PPQ	L
50		Loss of data backup	Loss of data	No backup	C	M	H				
51	The dataloggers have a long term inherent automatic long-term storage	The data obtained is unreadable or corrupted	Data loss	The saved data from the older datalogger types may not be retrievable in the future since the platform is no longer supported by the updated platform	C	M	H	• Retrieving the data from an older platform/ software is not dependent on the version of MySQL database	M	OQ	L

Author: Allan Marinelli

Network (www.ivtnetwork.com)

IVT NETWORK
INSTITUTE OF VALIDATION TECHNOLOGY
an informa business

Published on IVT

JVT Volume 27, Issue 1 – February 2021

PEER REVIEWED

URS or FS Reference	Description	Risk Identification			Risk Evaluation			Risk Control			
		Failure Mode	Effect	Cause	Impact: C, M,m,b	Detectability: H, M, L	Initial Risk	Risk Mitigation	Final Risk	Risk Verification	Risk Acceptance
								• The data from the database are always retained by default and only the indexes that are deleted as a function of time in order to free up space capacity space.			
52	All configurations (Parameters, Alarms Thresholds, Sensors/Probes, Receivers, Transmitters and Repeaters Access Permission Rights and/or other settings) must be performed in the approved Operator Interface	Approved Operator Interface was not used to set up all configurations	The system management is not configured as expected	Vendor non-adherence	M	H	L	• The vendor client relationship ensures that all configurations are completed in the Operator Interface so the Vendor can always obtain the congruence • All modifications to the system are tracked by the audit-trail mechanism	L	OQ	L
Data Integrity of Software											
53	The following are components to the Data Integrity of the software: (1) Data Management (Good Documentation Practices) (2) Data Life Cycle Management (Creation, Use, Change, Archiving) (3) Access Control and IT Security/Password (Segregation of Duties) (4) Data Management (Review of Data and Meta Data Including Audit Trail) (5) User Management (6) Data Management / Retention and Business Continuity) (7) ALCOA + Principles enforced	Any violations or compromise to the elements of the Data Integrity as described in the description column	Data may be comprised	Data Integrity not enforced and controlled	C	L	H	• Initial IQ, OQ , and PPQ Testing	H to M	• First release of the software and Initial PQ Testing. • **Worse Case Scenario**: Potentially disrupting the services (Availability of the system) to many users of system Vulnerabilities against hackers or outside interference.	M

Author: Allan Marinelli

Network (www.ivtnetwork.com)

IVT NETWORK
INSTITUTE OF VALIDATION TECHNOLOGY
an informa business

Published on IVT

JVT Volume 27, Issue 1 – February 2021

PEER REVIEWED

URS or FS Reference	Description	Risk Identification			Risk Evaluation			Risk Control			
		Failure Mode	Effect	Cause	Impact: C, M,m,b	Detectability: H, M, L	Initial Risk	Risk Mitigation	Final Risk	Risk Verification	Risk Acceptance
	(8) Protection against attack pertaining to system Vulnerabilities									• Also the monitoring data will be appended or supplemented to the batch release process which increases the likelihood of additional scrutiny during regulatory inspections	
Hardware											
54	The hardware components must be compliant IT requirements	Non-compliance of IT Components	Hardware performance and capacity is hampered	Violation of IT Requirements	B	H	L	• System process integration is assigned and managed under IT for control • The development of the Scripts are conducted by IT to ensure correct functioning and abiding to the requirements	L	OQ	L
Overall Size Limitation											
55	The minimum and maximum size of the sensors/probes must be within the design specification range	Violations to the principles outlined in the Design Specification Range	The Sensors/Probes cannot fit in the target location	Vendor deficient	m	H	L	• The Design Specification are reviewed and approved by both vendor and the client • The sensor/probes are confirmed to be meeting the requirements upon incoming shipment verification	L	DQ	L
Standards											

Author: Allan Marinelli

Network (www.ivtnetwork.com)

IVT NETWORK
INSTITUTE OF VALIDATION TECHNOLOGY
an informa business

Published on IVT

JVT Volume 27, Issue 1 – February 2021

PEER REVIEWED

URS or FS Reference	Description	Risk Identification			Risk Evaluation			Risk Control			
		Failure Mode	Effect	Cause	Impact: C, M,m,b	Detectability: H, M, L	Initial Risk	Risk Mitigation	Final Risk	Risk Verification	Risk Acceptance
56	The Network components must be in compliance with the IT Design Specifications	The network components are accepted to be outside the scope of the IT Design Specification	The System is not functional	Violation of IT Design Specification	B	H	L	• The IT Team reviews and approves the Design Specification in conjunction with the vendors input	L	DQ, IQ	L
CO2 Monitoring											
57	CO2 monitoring is a parameter available per system design	Analog signals cannot be converted to digital output to obtain CO2 results	Failing to monitor the CO2	Vendor deficient	C	H	M	• The IT Team reviews and approves the Design Specification in conjunction with the vendors input	M	DQ OQ	L

Author: Allan Marinelli

Network (www.ivtnetwork.com)

IVT NETWORK
INSTITUTE OF VALIDATION TECHNOLOGY
an informa business

Published on IVT

JVT Volume 27, Issue 1 – February 2021

PEER REVIEWED

URS or FS Reference	Description	Risk Identification			Risk Evaluation			Risk Control			
		Failure Mode	Effect	Cause	Impact: C, M,m,b	Detectability: H, M, L	Initial Risk	Risk Mitigation	Final Risk	Risk Verification	Risk Acceptance
Pressure Monitoring											
58	Pressure monitoring is a parameter available per system design.	Pressure signals cannot be accepted by the system	Failing to monitor the Pressure	Vendor deficient	C	H	M	• The IT Team reviews and approves the Design Specification in conjunction with the vendors input	M	DQ OQ	L
Differential Pressure Monitoring											
59	Differential Pressure monitoring is a parameter available per system design.	Differential Pressure signals cannot be accepted by the system	Failing to monitor the Differential Pressure	Vendor deficient	C	H	M	• The IT Team reviews and approves the Design Specification in conjunction with the vendors input	M	DQ OQ	L
Analog Signal Monitoring											
60	Generic Analog (Any other parameter other than CO2) monitoring is a parameter available per system design.	Analog signals cannot be converted to digital output to obtain desired output results	Failing to convert all analog signal to digital	Vendor deficient	C	H	M	• The IT Team reviews and approves the Design Specification in conjunction with the vendors input	M	DQ OQ	L
Temperature Monitoring											
61	Temperature monitoring is a parameter available per system design.	Temperature signals cannot be accepted by the system	Failing to monitor the Temperature	Vendor deficient	C	H	M	• The IT Team reviews and approves the Design Specification in conjunction with the vendors input	M	DQ OQ	L
Dry Contact Monitoring											

Author: Allan Marinelli

Network (www.ivtnetwork.com)

IVT NETWORK
INSTITUTE OF VALIDATION TECHNOLOGY
an informa business

Published on IVT

JVT Volume 27, Issue 1 – February 2021

PEER REVIEWED

URS or FS Reference	Description	Risk Identification			Risk Evaluation			Risk Control			
		Failure Mode	Effect	Cause	Impact: C, M,m,b	Detectability: H, M, L	Initial Risk	Risk Mitigation	Final Risk	Risk Verification	Risk Acceptance
62	Dry Contact monitoring is a parameter available per system design.	Dry Contact signals cannot be accepted by the system	Failing to monitor the Dry Contact Monitoring	Vendor deficient	C	H	M	• The IT Team reviews and approves the Design Specification in conjunction with the vendors input	M	DQ OQ	L

Author: Allan Marinelli

Network (www.ivtnetwork.com)

IVT NETWORK
INSTITUTE OF VALIDATION TECHNOLOGY
an informa business

Published on IVT

JVT Volume 27, Issue 1 – February 2021

PEER REVIEWED

URS or FS Reference	Description	Risk Identification			Risk Evaluation			Risk Control			
		Failure Mode	Effect	Cause	Impact: C, M,m,b	Detectability: H, M, L	Initial Risk	Risk Mitigation	Final Risk	Risk Verification	Risk Acceptance
Environmental Limitations											
63	The equipment, probes/sensors will be positioned in an explosion proof and flame proof area, ATEX classified.	No Safety Standard specified	Halt production	Vendor deficient	C	H	M	• An ATEX certificate or other environmental safety explosion proof standards relative to the country where the system is located	L	DQ IQ	L
64	The equipment, probe/sensors will function within the scope of its design range in specified classified conditions versus specified non-classified conditions with respect to predefined temperature and relative humidity ranges.	The sensor cannot function outside of its design environmental range with respect to predefine temperature and humidity ranges	Halt production	Vendor deficient	C	H	M	• Whenever the test locations falls outside of its design acceptable temperature and relative humidity ranges, an alarm "low battery "(due to temperature or humidity) will be generated to prevent the logging of data • The Design Specification is both reviewed and approved by the vendor and client in order to meet the requirements for its intended uses	L	DQ IQ	L

Author: Allan Marinelli

Network (www.ivtnetwork.com)

IVT NETWORK
INSTITUTE OF VALIDATION TECHNOLOGY
an informa business

Published on IVT

JVT Volume 27, Issue 1 – February 2021

PEER REVIEWED

URS or FS Reference	Description	Risk Identification			Risk Evaluation			Risk Control			
		Failure Mode	Effect	Cause	Impact: C, M,m,b	Detectability: H, M, L	Initial Risk	Risk Mitigation	Final Risk	Risk Verification	Risk Acceptance
Function: Data Emission											
65	A buffering data allowance is designed to: (1) A larger data measured capacity between transmissions for efficient battery usage (2) In case of an shutdown as a result of internal power outage (receiver, core application, server/client),or power loss or external power outage (power line, perturbation of radio-transmission, Ethernet Lan) the loggers/probes/sensors will be capable of maintaining and sustaining the data	Data transmission failure from sensor to receptor	Data cannot be transmitted to the server	Loss of com-munication	M	H	L	• Validation will test and emulate the scenarios with respect to internal versus external power failure/loss and the failure condition attested in the description field	L	OQ	L
66		Potential data Integrity or data loss as a result of the incidence	Data cannot be retrieved or be transferred to the database	Battery Failure The line of com-munication is broken between the incoming data source to the receiving data source	C	H	M	• Validation will test and emulate the scenarios with respect to internal versus external power failure/loss and the failure condition attested in the description field	L	OQ	L
67		Loss of Data at the source during the attempt to transmit the data	Total Data loss	Battery Failure The line of com-munication is broken between the incoming data source to the receiving data source	C	H	M	• Validation will test and emulate the scenarios with respect to internal versus external power failure/loss and the failure condition attested in the description field	L	OQ	L
Function: Data Acquisition											
68	A site inspection at the client/company must be performed prior to conducting any formal testing so to evaluate the effectiveness of the capacity of the radio frequency communication	Not all targeted required areas have radio frequency com-munication	Partial or no data available to transmit	Site Inspection in correctly assessed or the design of the facility design is inadequate to allow the flowability of radio frequency communications	M	H	L	• The vendor and client both review and approve the site inspection report prior to commencing the project to proceed to the next steps	L	IQ	L

Author: Allan Marinelli

Network (www.ivtnetwork.com)

IVT NETWORK
INSTITUTE OF VALIDATION TECHNOLOGY
an informa business

Published on IVT

JVT Volume 27, Issue 1 – February 2021

PEER REVIEWED

URS or FS Reference	Description	Risk Identification			Risk Evaluation			Risk Control			
		Failure Mode	Effect	Cause	Impact: C, M,m,b	Detectability: H, M, L	Initial Risk	Risk Mitigation	Final Risk	Risk Verification	Risk Acceptance
69	The design of the system must allow the sensor/probe to retain the necessary inherent data as part of the engineering study and ensuring that the system is resilient to the possibilities of losing any data from any the path sources to transmitter or acquisition data to repeaters to receivers to severs to databases	Failure of Sensor/probe recording	Incorrect data obtained	Defective Sensor Prober	C	M	H	• Validation will test and emulate the scenarios with respect to internal versus external power failure/loss and the failure condition attested in the description field	M	DQ OQ	L
Sensor Component											
70	Electronic system identification including labelling is mandated to outline the system intended uses with respect to type, use, location and history of the sensor/probe	Tag sensor violates the intent as described in the description field	Data Information is not complete or incorrectly identified, and labelled	Insufficient identification	C	H	M	• The probes/sensor identification is inherently intrinsic as part of the design to retrieve the necessary information by ROM (Read Only Memory) Radio.	L	DQ IQ	L
71	The sensors/probes including the transmitters represent the package submitted to the client that is intrinsically designed to provide enough battery bandwidth for retaining large number sample for an extended period of time.	Deficient Battery Design memory retaining output	Changing of battery more than the design specified range of retain-ability	Insufficient Design	B	H	L	• The Client has a preventative maintenance schedule to ensure correct functioning of the system • An existent alarm threshold condition will be activated by design so to allow the User to prepare for correcting the issue at question	L	DQ OQ	L

Author: Allan Marinelli

Network (www.ivtnetwork.com)

IVT NETWORK
INSTITUTE OF VALIDATION TECHNOLOGY
an informa business

Published on IVT

JVT Volume 27, Issue 1 – February 2021

PEER REVIEWED

URS or FS Reference	Description	Risk Identification			Risk Evaluation			Risk Control			
		Failure Mode	Effect	Cause	Impact: C, M,m,b	Detectability: H, M, L	Initial Risk	Risk Mitigation	Final Risk	Risk Verification	Risk Acceptance
72	Probes/sensor are designed for easy calibration through a user interface.	Calibration not feasible by design despite using the interface	Inaccurate calibration results	Corrupted programmed database or not updated accordingly by not allowing interfacing with the identified sensors/probes at question	C	H	M	• Upon incoming shipment of sensors/probes, the functionality of the Calibration interfaces are tested to determine if the identified sensors/probes appears on the interface database list • Calibration maintenance is performed by trained authorized Metrology department designees	L	DQ OQ	L
73	Calibration of all sensors/probes/readers indicators, and thermometers are performed in alignment with the Client's approved SOP	Violation to the Calibration SOP	Inaccurate Calibration results	The calibration values obtained will not be correctly reflective in the interfacing database	C	H	M	• Calibration maintenance is performed by trained authorized Metrology department designees	L	OQ	L
74	The sensors/probes us designed to operate with the design range specified in the Design Specification	Malfunction of sensors outside the acceptable design range	Data not recorded	Environmental condition outside the acceptable operating range of the sensors/probes	C	H	M	• Per SOP, the sensors/probes are pre calibrated or internal calibration is performed prior to usage.	L	DQ IQ	L
75	Maintenance phase requirements	Non-existent preventive maintenance of sensors in place	Sensor loss communicatio n	Non-existent Maintenance Plan	M	H	L	• Preventive maintenance is enforced by the SOP and trainings • Battery change at each checking	L	N/A	L

Author: Allan Marinelli

Network (www.ivtnetwork.com)

IVT NETWORK
INSTITUTE OF VALIDATION TECHNOLOGY
an informa business

Published on IVT

JVT Volume 27, Issue 1 – February 2021

PEER REVIEWED

URS or FS Reference	Description	Risk Identification			Risk Evaluation			Risk Control			
		Failure Mode	Effect	Cause	Impact: C, M,m,b	Detectability: H, M, L	Initial Risk	Risk Mitigation	Final Risk	Risk Verification	Risk Acceptance
								Sensor maintenance is performed by the supplier which used a tracking tools, consequently, it can provide us materiel trending			
Health and Safety											
76	The system, equipment, sensors/ probes etc must be identified and comply with the regulatory requirements relative to the country at questions. For Example, in the United States, the regulatory requirements with be the Federal Communication Commission (FCC). A certificate of compliance for each of the equipment, sensors/ probes used in alignment with the country regulation	Violation of regulatory requirements relative to the country at question	The system is in-operable	Vendor Deficient	B	H	L	• It is legal requirement that the vendor provides the necessary evidence attestation including the relevant certificates, and labelling of each equipment, sensors/probes to meet the requirements of the country where the equipment is being used.	L	DQ	L
77	Noise level requirements will meet the acceptable range as specified in the Design Specification	Noise level outside of acceptable range	System cannot be used with the possibility of being detrimental to humans	Vendor Deficient	B	H	L	• Relative to the static design of the system, there is insufficient attributable noise level outputted by the devices. This is also reviewed as part of the design specification in the DQ	L	DQ	L

Author: Allan Marinelli

Network (www.ivtnetwork.com)

IVT NETWORK
INSTITUTE OF VALIDATION TECHNOLOGY
an informa business

Published on IVT

JVT Volume 27, Issue 1 – February 2021

PEER REVIEWED

URS or FS Reference	Description	Risk Identification			Risk Evaluation			Risk Control			
		Failure Mode	Effect	Cause	Impact: C, M,m,b	Detectability: H, M, L	Initial Risk	Risk Mitigation	Final Risk	Risk Verification	Risk Acceptance
78	The equipment, system, probes/sensor, receivers, repeaters etc will be positioned in a suitable location where there is no risk of accident with respect to the design layout of the room, (material flow, process flow, personnel flow etc	Inappropriate location with respective to using the system as specified in the URS.	Potential risk of injury to the User and damage to the equipment	Equipment positioned in the wrong area to conduct engineering studies etc	B	H	L	• Sensors are intrinsically designed to be compartmentalize in a small area not requiring too much space. • Therefore, by design there is no risk to the User to experience an injury	L	IQ	L
79	To prevent injury to the User, all corners of the probes/sensors are designed to be rounded or no sharp edges to cause bodily harm	Violation of the safety/design principles	Injury to the User and the possibility of contaminating the product	Faulty Design	C	M	H	• If the system, equipment, probes/sensors are positioned in the classified area within the manufacturing suites, then this requirement is only applicable in these conditions else irrelevant in non-classified locations. • The Hardware Design Specification is reviewed and approved by the vendor and the client.t • A cleaning procedure is in place to avoid cross contamination to the product upon an occurring injury	L	DQ	L

Author: Allan Marinelli

Network (www.ivtnetwork.com)

IVT NETWORK
INSTITUTE OF VALIDATION TECHNOLOGY
an informa business

Published on IVT

JVT Volume 27, Issue 1 – February 2021

PEER REVIEWED

URS or FS Reference	Description	Risk Identification			Risk Evaluation			Risk Control			
		Failure Mode	Effect	Cause	Impact: C, M,m,b	Detectability: H, M, L	Initial Risk	Risk Mitigation	Final Risk	Risk Verification	Risk Acceptance
80	The Ingress Protection (IP) Code rating will be within User's design range of operating environment to ensure sufficient degree of protection needed against intrusion, accidental electric conducting signals, water etc.	No available IP rating	EHS issue	Vendor deficient	B	H	L	• As part of the design specifications, the IP rating are specified and evidence to substantiate such claims are provided by a certificate of material of construction etc.	L	DQ	L
81	The radio communication trajectories between the different or various components (Repeaters, Receiver, Transmitters, etc) will have the necessary inherent infrastructure by design to abide by the frequencies and emitting power thresholds defined in the country's regulations.	Violation of regulations	System not to be used	Vendor efficient	B	H	L	• It is a legal obligation by the Vendor to ensure that all devices are in conformance with the regulations where the devices will be used.	L	DQ	L
82	The Quality Agreement (QAG) and Master Service Agreement (MSA) must cover strict confidentiality agreements to cover from the design of the product, the inception of the services of the product at the client's site, and guarantee of IT/Devices services attested by both parties, notwithstanding	There is no alignment with what was agreed in both QAG and MS in actual practice	Software support amongst other things are not consistently executed	Vendor Deficient	B	H	L	• The QA and MSA are strictly adhered by both parties and controlled under both party legal team	L	DQ	L
Receptor Component											
83	Electronic system identification including labelling is mandated to outline the system intended uses with respect to type, use, location and history of the sensor/probe	Tag sensor violates the intent as described in the description field	Data Information is not complete or incorrectly identified, and labelled	Insufficient identification	C	H	M	The probes/sensor identification is inherently intrinsic as part of the design to retrieve the necessary information by ROM (Read Only Memory) Radio.	L	DQ IQ	L

Author: Allan Marinelli

Network (www.ivtnetwork.com)

IVT NETWORK
INSTITUTE OF VALIDATION TECHNOLOGY
an informa business

Published on IVT

JVT Volume 27, Issue 1 – February 2021

PEER REVIEWED

URS or FS Reference	Description	Risk Identification			Risk Evaluation			Risk Control			
		Failure Mode	Effect	Cause	Impact: C, M,m,b	Detectability: H, M, L	Initial Risk	Risk Mitigation	Final Risk	Risk Verification	Risk Acceptance
84	The design of the system must allow the sensor/probe to retain the necessary inherent data as part of the engineering study and ensuring that the system is resilient to the possibilities of losing any data from any the path sources to transmitter or acquisition data to repeaters to receivers to severs to databases	Malfunction of Receptor	Data not transmitted from sensors to receptors)	Receptor Inoperative	M	H	L	• Despite the fact that there is a possibility that the receptors malfunctions, there is inherent data that is saved by the probe/sensor which can be subsequently retrieved at later time when the receptor are back working again. • This scenario is tested as part of the OQ to show that the data is still able to be retrieved by emulating a condition of the receptor malfunction	L	DQ OQ	L

Author: Allan Marinelli

Published on IVT Network (www.ivtnetwork.com)

JVT Volume 27, Issue 1 – February 2021

IVT NETWORK
INSTITUTE OF VALIDATION TECHNOLOGY
an informa business

PEER REVIEWED

OVERALL RISK

*****Total Attributes of Risk Acceptance Evaluation: **84**
*****Total Medium Risk Acceptance : 7 (Representing 12% of the Total System Attributes)
*****Total Low Risk Acceptance: 77 (Representing 88% of the Total System Attributes)

** Taking the conservative approach as this system was initially validated and never inspected under regulatory scrutiny despite the fact the company claims that their DQ(s), IQ(s),OQ(s) or PQ(s) were successfully completed, there is a possibility that there may be existent gaps in the Validation conducted which may lead to either creating or a combination of performing supplemental tests, repeating certain tests or repeating the entire validation package post regulatory inspection. Bearing these possibilities, a total Medium Risk Acceptance was enumerated to represent 12% of the total system attributes. As the system undergoes supplemental inspections, and a demonstration that the system retains its controls, the Medium Risk Acceptance percentage of 12% may be lower, notwithstanding.*

SUMMARY

By using the qualitative approach through the deployment of utilizing the FMEA methodology that contains the main sections of URS or FS Reference, Risk Identification, Risk Evaluation and Risk Controls, a risk analysis can be successfully conducted pertaining to RF monitoring devices.

Refer to attachment A that entails the procedure and accompanying FMEA risk analysis for the RF monitoring devices.

CONCLUSION:

Therefore, the actual risk evaluation prior to inspection would be classified as **"Medium".**

DEFINITIONS

***FIFO*:** Material arriving or incoming shipment from a First In First Out approach

[2]***SOX (Sarbanes-Oxley Act):*** is an act that was passed by the United States congress in 2002 to protect investors from fraudulent accounting by business

Installation Qualification (IQ)*:* verifies the field installation components, including its connections, interfaces, material of construction, documentation availability (User Operating Manual, Maintenance Manuals, Calibration Manual etc), spart parts list, server type as applicable, receiving or other applicable devices as part of the system, IT architectural drawings/other Computer Systems Drawings, Design Drawings, field Calibrations Status, associated computer names IP (Internet Protocol) address, type of sensors or probes, environmental conditions, transmitter receiver protocol attributes, description of the system with respect to the user requirements specifications, verifying the sensors capabilities, configurational settings etc

Operation Qualification (OQ): verifies that the operational parameters in a test environment [e.g:. Transmitters includes a buffering mechanism; a larger interval between transmission of measured value collected than the interval between measurement of these values, and to be able to temporary store the measured values in case of internal outage (receiver, core

application, server/client) or external outage (power line, perturbation of radio-transmission, Ethernet Lan. etc] with respect to the Functional Design Requirement Specification (FDRS)are configured and operate in the field as expected. This may or may not involve stress testing

Production Performance Qualification (PPQ): verifies the performance of the system not tested in the OQ within a Prod Environment in alignment with the User Requirement Specifications (URS) as part of GAMP 5 paradigms. This may or may not involve the need to conduct a regression test over and above.

Design Qualification (DQ): Verifies the design attributes in alignment with the Design Specifications (e.g: the device meeting FCC standards; noise level for statis versus dynamic; physical attributes of the device, the radio communication path between the different parts of the infrastructure with respect the frequencies and emitting power allowances or tolerances, the infrastructure solutions with respect to the Agreement paradigms, the design of the wireless connectivity's, etc)

Failure Mode and Effects Analysis (FMEA)[3]: is the process of reviewing as many components, assemblies, and subsystems as possible to identify potential failure modes in a system and their causes and effects.
FMEA is an inductive reasoning (forward logic) single point of failure analysis and is a core task in reliability engineering, safety engineering and quality engineering.

Functional analyses are needed as an input to determine correct failure modes, at all system levels, both for functional FMEA or Piece-Part (hardware) FMEA. An FMEA is used to structure Mitigation for Risk reduction based on either failure (mode) effect severity reduction or based on lowering the probability of failure or both. The FMEA is in principle a full inductive (forward logic) analysis, however the failure probability can only be estimated or reduced by understanding the failure mechanism. Hence, FMEA may include information on causes of failure (deductive analysis) to reduce the possibility of occurrence by eliminating identified (root) causes.

REFERENCES:

1. Marinelli, Allan (2014) A Workable Sampling Plan Using a Quality Risk Management Approach Relative to the PQ Phase f the Upgraded Purified Water Generation System at the Pilot Plant /Small Scale- A Validation Engineering Perspective. *Journal of Validation Technology* Volume 20 Number 2, June 18. https://www.ivtnetwork.com/article/workable-sampling-plan-using-quality-risk-management-approach-relative-pq-phase-upgraded-pur

2. Collinsdictionary.com. 2020. Sox Definition And Meaning | Collins English Dictionary. [online] Available at: https://www.collinsdictionary.com/dictionary/english/sox [Accessed 21 September 2020].

3. En.wikipedia.org. 2020. Failure Mode And Effects Analysis. [online] Available at: https://en.wikipedia.org/wiki/Failure_mode_and_effects_analysis [Accessed 21 September 2020].

4. GAMP 5 "A Risk-Based Approach to Compliant GxP Computerized Systems, 2008, Appendix M3 page 115