www.ThePharmaJournal.com

The Pharma Innovation

ISSN (E): 2277- 7695
ISSN (P): 2349-8242
NAAS Rating: 5.23
TPI 2022; 11(4): 616-622
© 2022 TPI
www.thepharmajournal.com
Received: 02-02-2022
Accepted: 09-03-2022

Dr. Sanjay Kumar Jain
President, Amneal Pharmaceuticals, Ahmedabad, Gujarat, India

Jitendra Kumar Jain
Amneal Pharmaceuticals, Vice President, Ahemdabad Gujarat, India

Jagdish Gohel
Amneal Pharmaceuticals, General Manager, Ahemdabad, Gujarat, India

Bhavik Sanghavi
Amneal Pharmaceuticals, Sr. Manager, Ahemdabad, Gujarat, India

Corresponding Author:
Dr. Sanjay Kumar Jain
President, Amneal Pharmaceuticals, Ahmedabad, Gujarat, India

Quality risk assessment of equipment with PLC/HMI/SCADA in pharmaceutical industry

Dr. Sanjay Kumar Jain, Jitendra Kumar Jain, Jagdish Gohel and Bhavik Sanghavi

Abstract

The purpose of this paper is to describe the approach adopted in upgrading the computer systems of manufacturing and packaging equipment, equipped with PLC / HMI / SCADA in a running manufacturing plant by adopting quality risk assessment (QRM) process. The Failure Mode Effect Analysis (FMEA) model was used for performing QRM to identify the overall risk, which were ranked as priority 1, 2 or 3. High Risk items (Priority 1) were immediately taken up for upgradation, while Medium risk items (Priority 2) were accepted to upgrade the systems within stipulated timeline. Low risk items (Priority 3) were accepted as such without any further action. This approach has helped in continuing the business with scientific documentation ensuring that adequate risks are identified and eliminated based on risk ranking. This upgrade has helped to comply with regulatory requirement focusing on critical equipment.

Keywords: Quality risk assessment, data integrity, ALCOA, severity, probability, detectability

Introduction

Integrity of GMP data is critical in pharmaceutical industry. There are many cGMP Violations about breach of data integrity observed during regulatory audit by the USFDA investigators. This is disturbing because ensuring data integrity is an important component of industry's responsibility to ensure the safety, efficacy, and quality of drugs, and of FDA's ability to protect the public health. These data integrity-related cGMP violations have led to numerous regulatory actions, including warning letters, import alerts, and consent decrees. USFDA published guidance on data integrity in Dec 2018 clearly specifying the expectations to maintain the integrity of the data. In the guidance, USFDA suggested to ask the following questions to meet regulatory requirements:

- Are controls in place to ensure that data is complete?
- Are activities documented at the time of performance?
- Are activities attributable to a specific individual?
- Can only authorized individuals make changes to records?
- Is there a record of changes to data?
- Are records reviewed for accuracy, completeness, and compliance with established standards?
- Are data maintained securely from data creation through disposition after the record's retention period?

Since errors, mistakes by the humans while recording the details in GMP document resulted into breach of data integrity, most of the organization decided to automate the system to avoid any man-made issues. However, automated systems may also pose risk to the integrity of data hence validation of computer system is critical before making the system "Live". Risk assessment is key step while validating the automated systems.

Quality Risk Assessment

Quality risk management (QRM) is a systematic approach or tool in understanding risks, their root cause and impact on quality. According to the International conference on harmonization (ICH) Q9 guidance document "Quality risk management is a systematic process for the identification, assessment and control of risks to the quality of pharmaceutical products across the product lifecycle". It includes elements such as risk assessment, mitigation, elimination, communication and review.

The guidance provides the scientific knowledge-based evaluation of risk to the quality of product and links it to the patient's safety.

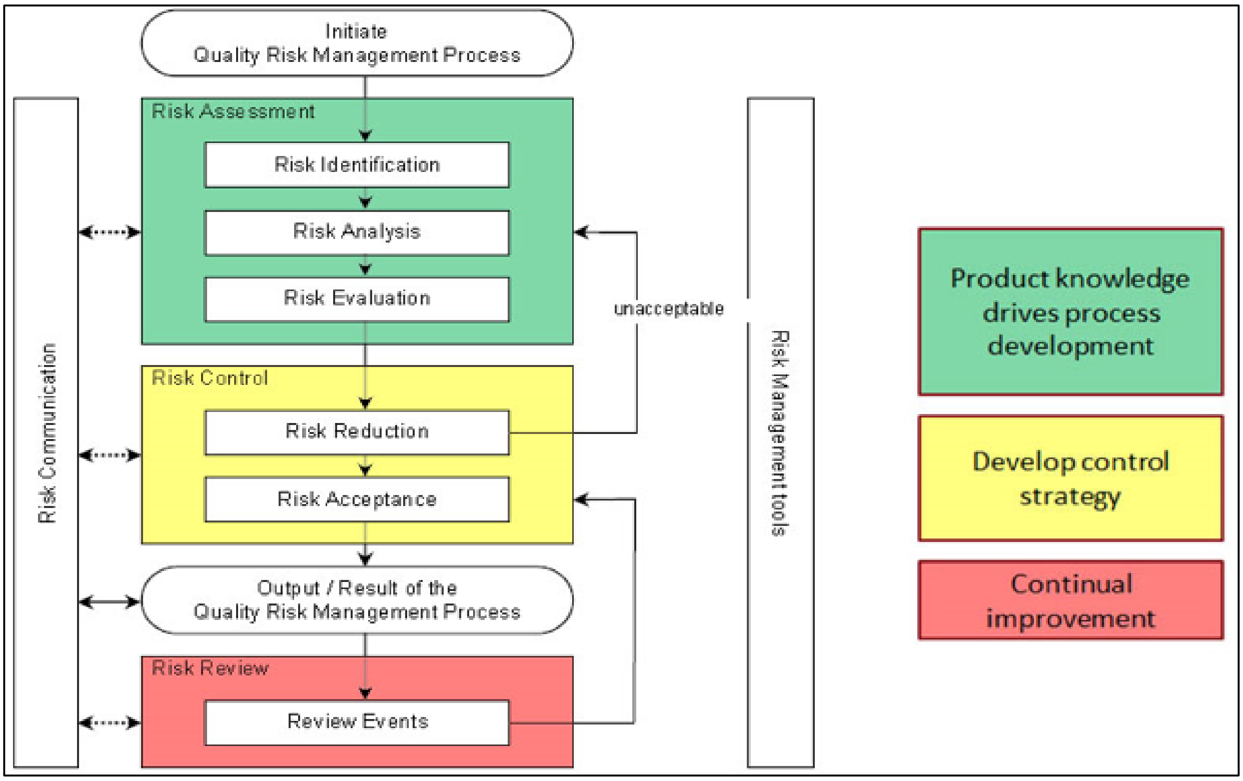
Quality Risk management Principles

There are primarily two basic principles for performing the quality risk management-

1. The evaluation of the risk to quality should be based on scientific knowledge and ultimately link to the protection of the patient
2. The level of effort, formality and documentation of the quality risk management process should be commensurate with the level of risk

Process flow of Quality Risk Management

Quality Risk management is a Systematic process designed to coordinate, facilitate and improve science-based decision making with respect to risk to quality of the product and safety of the patients. An effective risk management approach can assure highest Quality of drug product to the patients in providing means to identify and mitigate Quality issues at the early stages of product development. A model for the quality risk management is outlines in the diagram (figure 1).



Source: Quality Risk Management ICH Q9, version 4

Fig 1: Overview of a typical Quality risk management process

Quality Risk Management (QRM) is proactive tool to identify potential quality issues and take preventive action and it helps to take science-based decision in case any potential Quality issue may arises. Since this is science and knowledge-based process, it facilitates better and educated decision which gives greater assurance to the regulator. More scientific and data driven process adopted in QRM process reduces subjectivity and built the quality in product. A planned risk assessment is one that is performed, either prior to any activity is conducted or before further activity is conducted.

Following are the major steps while performing Quality Risk Management-

1. Quality risk Management process initiation
2. Risk Assessment
3. Risk Control
4. Output/Result of the QRM process
5. Risk Review
6. Risk Communications

Quality Risk Management Process Initiation

QRM should include systematic process designed to co-ordinate, facilitate and improve science based decision making with respect to risk. Planning of the QRM process shall include-

- Defining the problem statement, scope, known assumptions and expected outcome
- Identifying the team which would include subject matter experts (SMEs) and a trained facilitator
- Selecting the appropriate tools to perform the QRM process
- Determining the level of documentation and formality
- Identifying and collecting relevant background information, reference documents and data related to the potential risks or product and patient impact.
- Stating a mitigation plan with target completion date and appropriate levels of decision making for the risk management process.

Risk Assessment

The risk assessment process comprises of following three steps-

1. Risk identification,
2. Risk analysis
3. Risk evaluation.

The level of rigor and type of risk assessment should be proportionate with the potential impact on product quality and patient safety and knowledge of risk associated with a risk question, problem statement.

Irrespective of the product, process, risk question, problem statement all risk assessment requires the same fundamental activities in a common sequence of events:

- Identify the owner of the QRM process
- Identify the stakeholders of the QRM exercise and individual responsible for its execution.
- Identify the areas of expertise required for the exercise and build the risk assessment team of cross functional Subject Matter Experts (SMEs).
- Describe the product, process or system for which QRM is to performed
- Define the risk question, problem description or problem statement
- Determine the appropriate risk management tools to be used
- Identify the criteria for risk evaluation
- Assemble background information and data on the potential hazard, harm or human impact relevant to the risk assessment.

Risk Identification

Risk identification is a systematic use of information to identify risks referring to the problem description. Information can include historical data, theoretical analysis, informed opinions, and the concerns of stakeholders. Three fundamental questions are asked to clearly define the risk(s) for Quality risk assessment purposes:

1. What might go wrong?
   This question raises the possibilities of harm from exposures to hazards
2. What is the likelihood (probability) it will go wrong?
   This question focuses on the probability of occurrence of specific harms
3. What are the consequences (severity)?
   This question focuses on the severity of outcomes, given that the risk event occurs

Risk Analysis

Risk analysis is the assessment of the risk associated with the identified hazards. It can be either qualitative or quantitative process which links with the likelihood of occurrence (probability) or severity of harms. The ability to detect (detectability) the harm also factors in the assessing the risk.

Risk analysis is beneficial when conducted with a multi-functional team of SMEs. This assures that risks are analysed from multiple perspectives. Team discussion is particularly useful so that different perceptions of the risk can be surfaced.

Risk Evaluation

The identified and analyzed risks are compared against pre-defined risk criteria during risk evaluation. The output of a risk assessment can be a quantitative estimate of risk or a qualitative description of a range of risk. When risk is expressed quantitatively, a numerical probability is used. Alternatively, risk can be articulated using qualitative descriptors, such as “high”, “medium”, or “low”. These descriptors should be defined in detail for better clarity while assigning the rating. In quantitative risk assessments, a risk estimate provides the likelihood of a specific consequence, given a set of risk-generating circumstances. Hence, quantitative risk assessment is useful for one particular consequence at a time.

Risk Control

Risk control includes decision making either to reduce or accept risks. The purpose of risk control is to reduce the risk to an acceptable level. The amount of effort used for risk control should commensurate to the significance of the risk identified. Benefit-cost analysis or any appropriate tool shall be used by the decision makers for understanding the optimal level of risk control.

Risk control might focus on the following questions

- Is the risk above an acceptable level?
- What can be done to reduce or eliminate risks?
- What is the appropriate balance among benefits, risks and resources?
- Are new risks introduced as a result of the identified risks being controlled?

Risk reduction focuses on reducing the severity and probability of occurrence by implementing appropriate product, process, and system controls. Each identified risk should be assessed to determine if it is broadly acceptable, or unacceptable / intolerable. For unacceptable / intolerable risks, the risk reduction strategy should define the CAPA to attempt to reduce the risks to an acceptable level.

Regulatory Requirement

Data Integrity means state when data has not been altered in an unauthorised manner. Data Integrity covers data in storage, during processing, and while in transit. Tentative Definition for Falsification in Relation with GMP Inspection (EU) by Dr Thomas HECKER in his one of the presentation is “Any wilful mis-statement, misrepresentation, manipulation, adulteration, rewriting, hiding, replacing of quality related documents, materials, activities or buildings in order to give an item the appearance of GMP compliance when this is not the case, as these facts are not isolated and/or known, approved / supported by management (e.g. false analytical data checked and approved).” The integrity of data can be assured only in the absence of bias. Data integrity can be found in virtually any aspect of pharmaceutical manufacturing. Bias has no place in pharmaceutical science. Breach of Data Integrity means introducing Bias which can be deliberate or can be accidental, however either way, it can be detrimental to the Quality System.

Data integrity is fundamental in a pharmaceutical quality system which ensures that medicines are of the required quality as decisions on product quality are made based on the data. Electronic data and computerised systems have introduced new challenges to maintain data integrity; hence the data governance system should be integral to the pharmaceutical quality system as required by regulatory authorities. The effort and resource assigned to data governance should be commensurate with the risk to product quality and should also be balanced with other quality assurance resource demands. As such, manufacturers and analytical laboratories shall design and operate a system which provides an acceptable state of control based on the data integrity risk, and which is fully documented with supporting rationale.

Data integrity requirements apply equally to manual (paper) and electronic data. Manufacturers and analytical laboratories should be aware that reverting from automated / computerised to manual / paper-based systems will not in itself remove the need for data integrity controls.

The regulatory authorities have put much emphasis on data integrity in recent years because they uncovered serious cases of data integrity breaches. It is always better to proactively prevent issues, such as data integrity failures to occur, than trying to remediate and resolve inspection findings. Compliance excellence makes good business sense.

This document provides the regulatory requirement, graphical summary of the issues in recent past through review of warning letters, suggest the strategy to prevent the data integrity breaches by design, by procedural control and monitoring.

Data integrity is critical to regulatory compliance. USFDA has published the 21 CFR Part 11 and EU has published Annex 11 to spell out the requirement with respect to computerised system. 21 CFR Part 11 applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted under any records requirements set forth in Agency regulations. Part 11 also applies to electronic records submitted to the Agency under the Federal Food, Drug, and Cosmetic Act and the Public Health Service Act, even if such records are not specifically identified in Agency regulations. EU GMP Annex 11 applies to all forms of computerised systems used as part of a GMP regulated activities. A computerised system is a set of software and hardware components which together full fill certain functionalities. The application shall be validated; IT infrastructure shall be qualified. Where a computerised system replaces a manual operation, there should be no resultant decrease in product quality, process control or quality assurance. There should be no increase in the overall risk of the process. Both FDA and MHRA use the acronym "ALCOA Plus" to define its expectations of data integrity of electronic data.

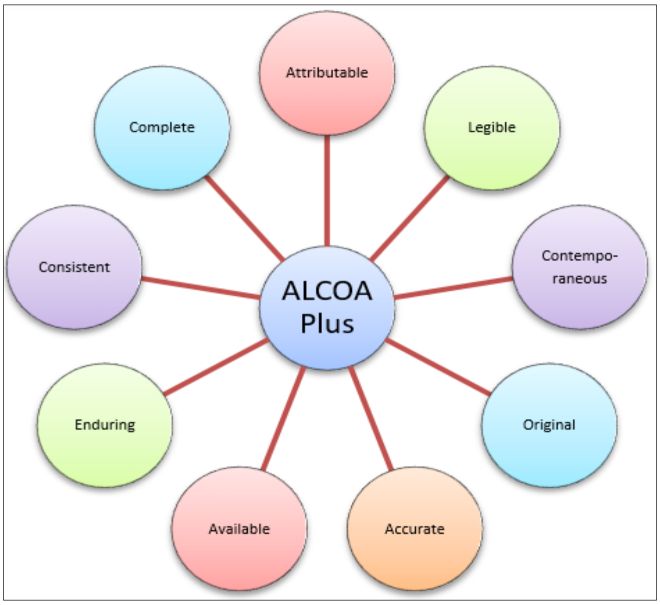


Fig 2: Alcoa Plus

- **Attributable:** 'Attributable' means information is captured in the record so that it is uniquely identified as executed by the originator of the data (e.g. a person, and/or a computer system).
- **Legible:** The terms 'legible', 'traceable' and 'permanent' refer to the requirements that data are readable, understandable and allow a clear picture of the sequencing of steps or events in the record.
- **Contemporaneous:** 'Contemporaneous' is the process of documentation (on paper or electronically) at the time of the occurrence of an activity.
- **Original:** 'Original' data includes the first or source capture of data or information and all subsequent data required to fully reconstruct the conduct of the GXP activity.
- **Accurate:** 'Accurate' means that data are correct, truthful, valid and reliable.
- **Complete:** 'Complete' means that all data from an analysis, including any data generated before a problem is observed, data generated after repeating part or all of the work, or re-analysis performed on the sample are contained the data record. For hybrid systems, the paper output must be linked to the underlying electronic records used to produce it.
- **Consistent:** 'Consistent' means that all elements of the analysis, such as the sequence of events, follow on and data files are date (all processes) and time (when using a hybrid or electronic systems) stamped in the expected order are contained in the record.
- **Enduring:** 'Enduring' means that all data have been recorded on authorized media which can be preserved for a period of time, e.g. laboratory notebooks, numbered worksheets, for which there is accountability, or electronic media. Data recorded on scrap paper or any other media which can be discarded later, e.g. backs of envelopes, laboratory coat sleeves or Post-It notes, etc. are not considered enduring.
- **Available:** 'Available' means that the complete collection of records can be accessed or retrieved for review and audit or inspection over the lifetime of the record.

In addition, definition of data integrity that FDA uses for internal training is: "Data are of high quality if they are fit for their intended uses in operations, decision-making and planning. as data volume increases, the question of internal consistency within data becomes paramount…."

For decision of safety, there must be rigorous and thorough application of fundamental scientific practices, irrespective of the purpose of study. Indeed, this is essentially its role in the pharmaceuticals industry-associated with recording data about good manufacturing practices, the creation and manipulation of the data base records, storage and any other activity that requires accountability within or of the organization.

Risk Assessment Methodology

Author and team wanted to upgrade their manufacturing / packaging equipment's computer systems (PLC/HMI/SCADA) to meet CFR Part 11 compliance requirements. Before taking up this project, it was decided to perform overall risk assessment of computer systems hence a protocol was written. The objective of the upgrade of PLC/HMI/SCADA was to ensure / improve compliance with Data integrity requirements; and hence non-compliance of Data Integrity (ALCOA) was considered as potential failure modes. Failure Modes and Effects Analysis (FMEA) model was selected for performing the quality risk assessment. FMEA is a systematic, proactive method for evaluating a process to identify where and how it might fail and to assess the relative impact of different failures, in order to identify the parts of the process that are most in need of change.

All three factors i.e. severity, probability of occurrence and detectability of failure were ranked for any potential risk while asking the question “What can go wrong”.

- Data Criticality shall be used to determine severity of impact.
- Functional capabilities of equipment for data storage shall be used to determine probability of occurrence.
- Existing Data Integrity controls shall be considered to determine detectability.

Risk priority was evaluated by taking into the consideration the severity of the risk, the probability of the occurrence of the risk and controls for detectability.

Data Criticality Determination (Severity)

Process Mapping was carried out for Manufacturing & Packaging operations. The process mapping shall capture each process step, associated equipment, details of data generated, type of data / record (Process parameter or Quality Attribute), severity, data format (i.e. paper/electronic). Criteria for ranking “Severity” factor was defined qualitatively i.e. High, Medium and Low (Refer table 1).

Table 1: Criteria for Severity Ranking

Ranking	Description
High	Data Integrity requirement (ALCOA) not complied for data directly associated with product quality i.e. process parameters or quality attributes
Medium	Data integrity requirement (ALCOA) not complied for the data indirectly associated with product quality
Low	Data integrity requirement (ALCOA) not complied for the data not associated with product quality.

Determination of Probability of Occurrence

To determine probability of occurrence, it was decided to classify all the Manufacturing and Packaging equipment based on the capabilities of equipment w.r.t. data storage. See table below-

Table 2: Equipment Classification

Type of Equipment	Details
Type 01	A non-electronic system. No GXP data are stored. Typical examples are manual operated Cizer mill and sifters which are without display.
Type 02	An electronic system and the generated GXP data is not stored and manually transferred on paper. Typical examples include Stirrer, balances which are without printers.
Type 03	An electronic system with some limited manual adjustable input data and the generated GXP data is not stored but printed out. Typical examples include balances with printer, Data logger with printer, and simple HMI based production machines
Type 04	An electronic system with some limited manual adjustable input data and the generated GXP data is not stored but sent via an interface to another system. Typical examples include temperature sensors.
Type 05	An electronic system where GXP data are permanently stored and these GXP data are not modified (processed) by the user to generate results. Typical examples include standalone equipment such as IPC based production machines
Type 06	An electronic system where GXP data are permanently stored and the GXP data can be processed by the user to generate results. Typical example is Track and Trace System.

Note

- The equipment shall be evaluated based in relation to all GXP data it processes. In case of different outcomes, the highest classification considering worst case scenario shall be maintained.
- It is important that the evaluation is done from the point of view of the system where the GXP data is generated and not where the GXP data is being transferred to.

Criteria for ranking factor “Probability of Occurrence” was defined in table 3.

Table 3: Criteria for Probability of Occurrence Ranking

Type of Equipment	Equipment Description	Ranking
Type 01	Manual Operations, very high probability of human induced error.	High
Type 02	Paper Record, Manual process.	
Type 03	Electronic System (manual adjustable input data) with Paper generated Record.	Medium
Type 04	Electronic Systems (manual adjustable input data) with central storage.	
Type 05	Electronic systems with local storage and processing.	Low
Type 06	Electronic systems with central storage and processing.	

Rationale

When the acquisition of data is manual the probability of human induced errors is considered higher. As the capability of equipment automation increases the human errors can be reduced as it’s expected that automation bring more consistency.

Determination of Detectability

The detectability was decided based on adequacy of existing controls / practices for controlling data integrity errors. For this following data integrity-based requirements were considered.

Table 4: Detectability Expectations

Data Integrity Criteria	Expectations
Attributable	▪ Defined roles and responsibilities ▪ Authorized operations ▪ Unique user traceability ▪ Audit Trail
Legible	▪ Human readable data ▪ Recording on permanent media ▪ Audit Trail ▪ Ability to read archived data during the retention period
Contemporaneous	▪ Standardized Time Source ▪ Harmonization/synchronization of different time sources ▪ Only Authorized access to time sources ▪ Periodic Verification of time accuracy
Original	▪ Data Review (doer and checker) ▪ Authorized data/record creations ▪ Control over issuance/modifications ▪ Audit trail
Accurate, Consistent	▪ Calibration, Qualification, Validation ▪ Periodic Review (Re-qualification)
Enduring, Available	▪ Recording on permanent media ▪ Data storage ▪ Stored data protection ▪ Data backup ▪ Data restore verification ▪ Archival and Retrieval ▪ Retention

Criteria for ranking factor “Detectability” was defined in table 5.

Table 5: Criteria for Detectability Ranking

Ranking	Detectability of Potential Failure
High	Non-compliance to data integrity requirement can be identified during the process of manufacturing step of drug product.
Medium	Non-compliance to data integrity requirement can be identified after the process of manufacturing step of drug product.
Low	Non-compliance to data integrity requirement cannot be identified until the batch is released.

Rationale: Availability of either system and / or process driven detection is considered as higher detection controls and lesser risk.

Risk Priority Determination

Factors “Severity” and “Probability of Occurrence” were mapped to determine the Risk Class (I, 2 or 3) e.g., High Severity with High Probability of occurrence would be “Risk Class 1” (Refer Figure 3).

After determining “Risk Class”, it was mapped with “Detectability” of failure to determine overall Risk e.g., Risk class 1 with low detectability would-be High-Risk Priority (Refer Figure 3)

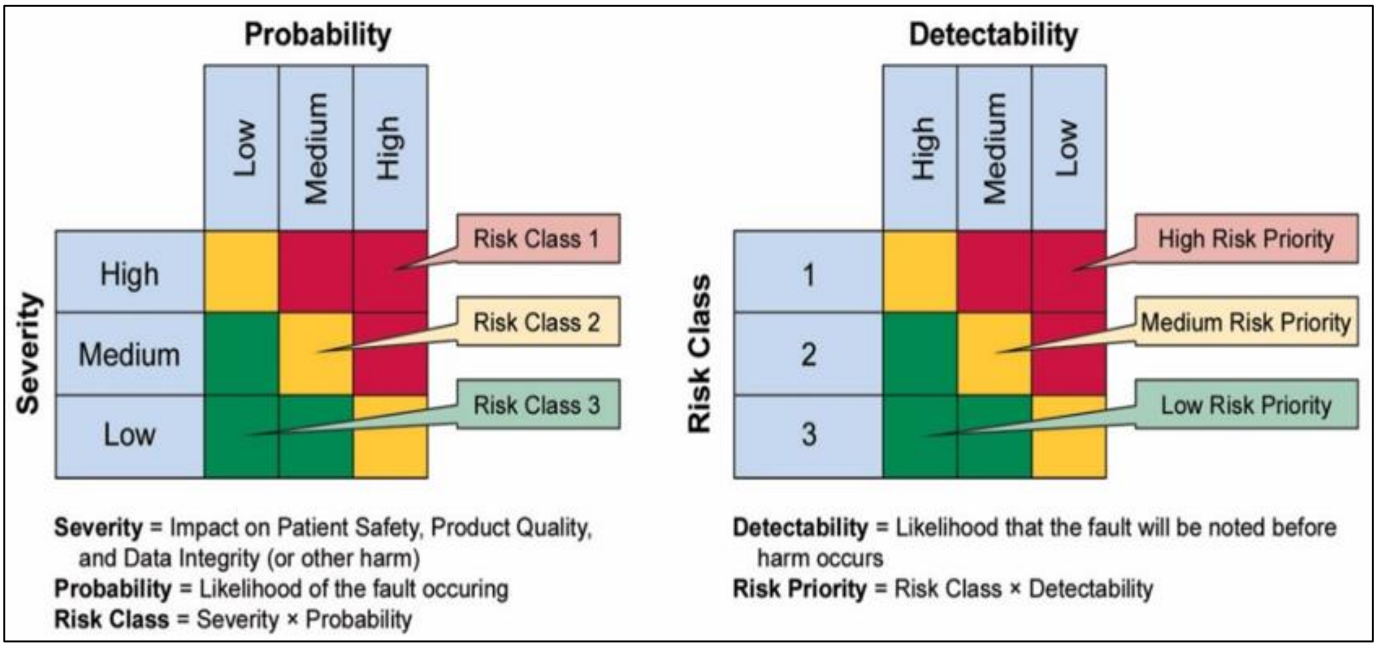

Probability
Low
Medium
High
Severity
High
Medium
Low
Risk Class 1
Risk Class 2
Risk Class 3
Detectability
High
Medium
Low
Risk Class
1
2
3
High Risk Priority
Medium Risk Priority
Low Risk Priority
Severity = Impact on Patient Safety, Product Quality, and Data Integrity (or other harm)
Probability = Likelihood of the fault occuring
Risk Class = Severity × Probability
Detectability = Likelihood that the fault will be noted before harm occurs
Risk Priority = Risk Class × Detectability

Fig 3: Risk Priority Determination

Based on the above criteria (figure 3), risks were prioritized as High, Medium and Low.

Table 6: Risk Priority and action

Overall Risk Classification	Risk Priority (level)	Risk Acceptance (Yes/No)	Action
High	1	No	Usage shall be stopped immediately, and risk must be mitigated.
Medium	2	Yes	Recommendations shall be implemented within stipulated timeline.
Low	3	Yes	No action required.

Note: The Risk assessment shall be clubbed for similar equipment (with same functionality and same type of classification) to avoid duplicity of the activity performed.

Conclusion

Quality Risk Assessment was carried out for each manufacturing equipment. FMEA sheet was created for each equipment using the methodology explained in the paper and mitigation strategy / recommendations for improvements were part of the assessment. Short-term and long-term mitigation actions were defined considering significance of the risk. It is expected that proposed mitigations would lead to an increased control over process, GXP data or systems by reducing severity, probability of occurrence and increasing detectability. After implementation of short-term and long-term mitigation action plan, Risk was re-assessed to confirm that residual risk is acceptable.

Overall Risk classified as LOW was accepted without any further action. Overall Risk classified as MEDIUM was accepted on a temporary basis where no further mitigation actions are possible at the time of evaluation (e.g. upgradation / replacement of HMI/IPC and / or software solution) and such type of risks shall be periodically re-evaluated. Overall Risk classified as HIGH was immediately mitigated.

This approach ensured the continuity of the business without compromising on data integrity and overall product quality and equipment having PLC/HMI/SCADA systems were taken for upgrade within stipulated timeline successfully.

References

1. Data Integrity and Compliance with Drug CGMP, Questions and Answers; Guidance for Industry, US FDA, 2018 Dec.
2. MHRA ‘GXP’ Data Integrity Guidance and Definitions. March 2018.
3. Parenteral Drug Association-Technical Report No. 80. Data integrity management system for Pharmaceutical laboratory.
4. WHO-Technical Report Series 996, Annexure 5. 2016.
5. EudraLex The Rules Governing Medicinal Products in the European Union, Volume 4 Good Manufacturing Practice Medicinal Products for Human and Veterinary Use Annex 11: Computerised Systems, 2011 January.
6. Active pharmaceuticals ingredient committee (APIC), Practical risk-based guide for managing data integrity. Version 1, 2019 March.
7. Guidance for Industry Part 11, Electronic Records; Electronic Signatures Scope and Application, U.S. Department of Health and Human Services Food and Drug Administration August Pharmaceutical CGMPs, 2003.
8. EU GMP Annex 11: Computerised system, revision 1.
9. MHRA GMP data integrity definitions and Guidance for industry, revision 1.1 March, 2015.
10. Peter Baker’s Presentation, Assistant Country Director (Drugs), US FDA India Office, US Embassy-New Delhi.
11. Data Integrity in Manufacturing Records Multicentre International Data Integrity Workshop; Mumbai, 3/4 and 6/7 November Dr Thomas HECKER, EDQM Inspector Certification of Substances Division, EDQM. 2014.
12. Quality Risk Management ICH Q9. Version 4, dated 9 November 2005.
13. PDA technical report No 54, implementation of Quality Risk Management for Pharmaceutical and biotechnology manufacturing operations. 2012.
14. Jain Sanjay Kumar Strategy to avoid data integrity issues in pharmaceutical industry. The Pharma Innovation Journal. 2017;6(2):110-115.
15. Jain Sanjay Kumar Quality Risk Management – CAPA to prevent Potential Quality Issues. Asian Journal of Pharma research & Development. 2017;5(1):1-11.