World Academy of Science, Engineering and Technology
International Journal of Economics and Management Engineering
Vol:13, No:7, 2019

Identification of Risks Associated with Process Automation Systems

J. K. Visser, H. T. Malan

***Abstract*—**A need exists to identify the sources of risks associated with the process automation systems within petrochemical companies or similar energy related industries. These companies use many different process automation technologies in its value chain. A crucial part of the process automation system is the information technology component featuring in the supervisory control layer. The ever-changing technology within the process automation layers and the rate at which it advances pose a risk to safe and predictable automation system performance. The age of the automation equipment also provides challenges to the operations and maintenance managers of the plant due to obsolescence and unavailability of spare parts. The main objective of this research was to determine the risk sources associated with the equipment that is part of the process automation systems. A secondary objective was to establish whether technology managers and technicians were aware of the risks and share the same viewpoint on the importance of the risks associated with automation systems. A conceptual model for risk sources of automation systems was formulated from models and frameworks in literature. This model comprised six categories of risk which forms the basis for identifying specific risks. This model was used to develop a questionnaire that was sent to 172 instrument technicians and technology managers in the company to obtain primary data. 75 completed and useful responses were received. These responses were analyzed statistically to determine the highest risk sources and to determine whether there was difference in opinion between technology managers and technicians. The most important risks that were revealed in this study are: 1) the lack of skilled technicians, 2) integration capability of third-party system software, 3) reliability of the process automation hardware, 4) excessive costs pertaining to performing maintenance and migrations on process automation systems, and 5) requirements of having third-party communication interfacing compatibility as well as real-time communication networks.

***Keywords*—**Distributed control system, identification of risks, information technology, process automation system.

I. Introduction

A petrochemical plant in South Africa was used as a case study. Different process automation technologies are used at this facility. Some of the process automation systems currently in operation are still the same technology that was used more than 40 years ago when the various business units were initially commissioned. A crucial part of the process automation system is the information technology (IT) component featuring in the supervisory control layer. The evolution of technology, the concepts of Industry 4.0 and the Industrial Internet of Things (IIoT) have brought about significant changes on how operations and maintenance are done currently in the process automation environment. Research has shown that significant economic outcomes can be achieved when applying Industry 4.0 techniques on modern industrial production practices, logistics and services [1]. However, a certain degree of risk is associated with changes in technology. Changes in the process automation environment can include that of adopting a new communications protocol, a new operating system (OS), a new field device such as a flow transmitter, or connecting the process automation system to an Internet-based Cloud service. There is also the looming risk of not doing anything, not adopting new technology, interoperability and compatibility concerns, or the well-known risk of component obsolescence and end-of-life. This situation is all too familiar to management and usually leads to companies investing much capital in new technologies or spending money on problems without understanding the real sources of risks in the process automation environment.

A. Research Problem Statement

A preliminary, internal investigation suggested that the technical fraternities responsible for the process automation environment of the company might not share the same viewpoint on the various risks and the criticality of those risks emanating from their existing process automation systems. The ever-changing technology within the process automation layers and the rate at which it advances pose a risk to safe and predictable automation system performance. As the life-cycle of the current process automation equipment progresses, it becomes more challenging to effectively manage the technology environment. This applies especially, when technology managers or technical fraternities are not aware of the risks or do not share the same viewpoint on the criticality of the risks associated with process automation systems. The lifespan of commercial-of-the-shelf IT equipment, fading fieldbus technologies, legacy process control systems, discontinued OS, all contribute to the process automation risk from a maintainability, reliability, sustainability and even safety perspective. It is essential that the technical fraternities are capable to adapt and react to the rate at which technology is changing and still maintain or even improve the competitive advantage in the market.

The associated research questions, within the context of the processing company's business units, were:

- Do the technical fraternities share the same viewpoint on the sources of risks within the process automation domain?
- Do the instrumentation engineering groups have different

H. T. Malan was enrolled for the Masters in Engineering Management degree in the Department of Engineering and Technology Management, University of Pretoria, South Africa.

J. K. Visser is a Professor in the Department of Engineering and Technology Management, University of Pretoria, South Africa.

viewpoints on the criticality of risks within the process automation domain?
- What are the most important risks that need special attention and mitigation actions?

B. Research Objectives

The main objective of this research was to enable the identification of the sources of risks within an existing process automation environment, such as company operations and maintenance, as well to determine the criticality of those risks as perceived by the various technical fraternities. This would determine whether alignment is achieved between the different levels of the instrumentation technical fraternities. Managers can evaluate the risks as well as the risk criticality emanating from this study and apply the knowledge to their respective process automation environments. The risks identified by this research can be used to fill a gap in current literature and potentially be applied by managers in other process and manufacturing industries.

In order to effectively address the research problem, it is:
- Proposed that the technical fraternities share the same viewpoint on the sources of risks within the process automation domain.
- Proposed that the instrumentation engineering groups do not have different viewpoints on the criticality of risks within the process automation domain.

As part of the research objectives, it was required to develop and propose a framework which would facilitate the alignment of the various technical fraternities regarding the process automation risks as well as the criticality of the risks. The outcome of the proposed framework is also to address the abovementioned research questions. Hence, the goal is to prove that alignment on the various sources of risks, as well the criticality perception of the risks, exists between the different technical fraternities of company operations.

II. Literature

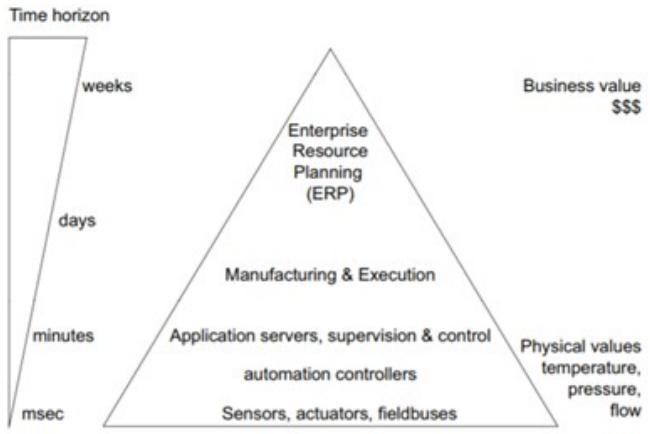

Fig. 1 Process automation pyramid [3]

In order to address the research problem and objectives, it was important to first explore and establish a sound theoretical framework from available literature on process automation systems. The system architecture of an automation system is one of the most important components responsible for the safe and efficient execution of a specific process. According to Samad et al. [2], the system architecture consists of various components together with its accompanying infrastructure which are logically organized and illustrated by the process automation pyramid in Fig. 1 [3].

A further explanation into the process automation pyramid is provided by the model in the International Society of Automation (ISA) standards, known as the ISA-95 functional hierarchical model as discussed in [4]. Samad et al. [2] further stated that the system architecture defines critical-to-quality parameters for the system architecture, which include criteria such as:
- *Capability of applications*, where the rate at which the software can be developed, implemented and maintained is dependent on the architecture of the process automation system.
- *Reliability of the components*, where the variety and scale of the process automation equipment found in a plant makes it almost impossible for all the components to function correctly all the time. Reliability and monitoring capabilities are designed into the automation system architecture to help overcome this problem.
- *Lowest total installed cost (LTIC)*, where the architecture of the system will influence the installation and integration costs of the product. The LTIC generally includes the product, delivery and installation cost to have the product integrated with the existing process automation system.
- *Maintenance and migrations*, where the computer and control system components will undergo maintenance and upgrades that require an online execution philosophy to prevent unwanted process interruptions. System or component redundancy also plays an important role when it comes to the upgrade of software releases. The system architecture is therefore key when performing online modifications and configuration of system components. Takata et al. [5] suggest that life cycle maintenance is an important part of life-cycle management and the goal is to retain the condition of an asset and allow it to fulfil its required functions for the rest of its life cycle.
- *Real-time* characteristics, where the architecture of the process automation system determines on-line characteristics such as monitoring, controlling and supervision of the process operation. It is important for the feedback control of the process automation system to be near real-time as possible to prevent any latency-related effects that will impact the response to react to the change in process conditions.
- *Security*, where cyber and physical security remains top priority for process automation systems due to some devices in the plant being connected to the Internet. Other measures would include access and password control for the various process automation systems.

The application of process automation systems is discussed in [3]. According to Hollender [3], the automobile/discrete manufacturing industry introduced the programmable logic

controller (PLC), whilst the petrochemical or process industry established the use of a distributed control system (DCS). Supervisory control and data acquisition (SCADA) or human machine interface (HMI) systems were introduced for geographically separated processes. Hollender [3] stated that recent advances in hardware and software technology are reducing the gap between what is considered as a DCS and PLC system. The modern DCS will consist of automation controllers, application servers and workstations, process historians, and supporting network and peripheral components, which are illustrated in Fig. 2 [6].

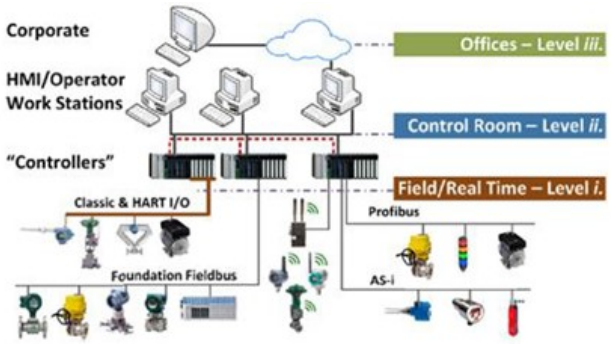

Fig. 2 DCS [6]

Another important aspect of a process automation system is the industrial communication technologies, alternatively known as field-level networks. These networks can be categorised into fieldbus networks, industrial Ethernet, as well industrial wireless networks [7]. According to Jämsä-Jounela [8], the evolution of communication technologies played an important role in shaping the current industrial automation systems and the advancements in field devices now include the intelligence capability of maintenance and monitoring tasks besides the traditional measurement functions. The standardisation of the fieldbus systems resulted in the open systems concept that further increased the interoperability between the different vendors and returned the customer trust in the new technology [7].

The literature study provided valuable constructs on the various facets of the process automation domain. The link between a typical industrial technical process and the process automation domain was established. The literature also provided an architectural overview of a typical process automation system as well as critical-to-quality system architecture criteria. Although the authors cited delved into much detail when capturing the various concepts of the current and future technologies for process automation and communication fields, they rarely contribute to the literature when it comes to risk identification associated with the process automation and subsystem domains. The literature therefore laid the foundation of where to focus the attention when identifying the sources of risks emanating from the process automation and subsystem domains and lead to the development of the conceptual model presented in the following section.

III. Conceptual Framework

The authors cited in the literature provided the reader with a holistic overview of the process automation environment as well as the various supporting pillars of technology. As highlighted previously, the authors rarely contributed to the literature by identifying the sources of risks associated with the process automation and subsystem domains. Samad et al. [2] defined the following main concepts related to process automation:

A. System Component Reliability and Architecture

The system architecture has an important role when it comes to the reliability of the components. The following characteristics are core architecture requirements: modularity of the process automation components, i.e. reliability of hardware and software, redundant configuration capability of hardware and software components, and real-time monitoring capability which allows for equipment health monitoring [2].

B. System Component Compatibility

The rate at which hardware and software can be developed, implemented (integrated) and maintained is dependent on the architecture of the process automation system. It is important that the OS and the process automation application are compatible with one another (interoperable) as well as supported by the hardware.

C. Maintenance and Migration

According to Swanson [9], it is necessary for a company to have a well-defined and cost-effective maintenance strategy to maintain its competitive advantage. Deteriorating equipment will put the plant at a disadvantage and hence equipment should be maintained well to enable high availability and life cycle. Some of the core characteristics are discussed in [9], i.e. maintenance and migration cost and strategies, online software maintenance activities, and hardware backward compatibility.

D. Operability and Life Cycle Management

The rate at which commercial-off-the-shelf (COTS) components (such as computers, servers, and switches) reach end-of-life or obsolescence surpasses that of the proprietary process automation system [2]. Companies should be cautious not to prematurely dispose of their assets, destroying their capital investment. By delaying substituting technology (jumping the S-curve) for too long can lead to an undesirable increase in failure rates, an increase in maintenance costs, and even environmental damage [10]. Some important factors captured by the literature were equipment installation date, life-cycle phase of the equipment, age or maturity of the process automation equipment, availability of certified spare parts, availability of skilled personnel, formal training opportunities, and vendor support [11]. In addition to these factors, one could also consider the availability of a vendor warranty policy, equipment renewal plans, and engineering cost.

E. Communication Networks

The industrial communication technologies, alternatively

known as field-level networks, can be categorised into fieldbus networks, industrial Ethernet, as well industrial wireless networks [7]. Incompatibility and interface concerns across the automation layers occur due to the large number of communication or network protocols being available. Vendors had to ensure backwards compatibility and integration between the existing fieldbuses and new Ethernet installations. The ability to monitor, control and supervise the process operation will impact the response to changes in process conditions. The fieldbus and industrial Ethernet networks need to be capable of achieving this characteristic.

F. Security

The design of the cyber and physical security remains top priority for process automation systems, since some devices in the plant can be connected to the Internet. The implementation of password control (or role-based access control) and firewall protection is a method for added security. In addition to these security measures are the management of physical access control to the process automation systems.

The above process automation concepts are just some of the critical components highlighted by the literature [2]. Each concept has an impact on the process automation environment from a risk perspective. None of the literature sources consulted for this study presented a holistic model that represents the main sources of risk pertaining to the process automation environment. The process automation concepts discussed above should be viewed collectively to identify the different sources of risk associated with the process automation environment.

G.Proposed Conceptual Framework

It is proposed that integrating the above concepts will lead to the development of a holistic model which will allow sources of risks to be identified in the process automation field of a typical manufacturing company. The proposed conceptual framework to address the research problem is illustrated in Fig. 3.

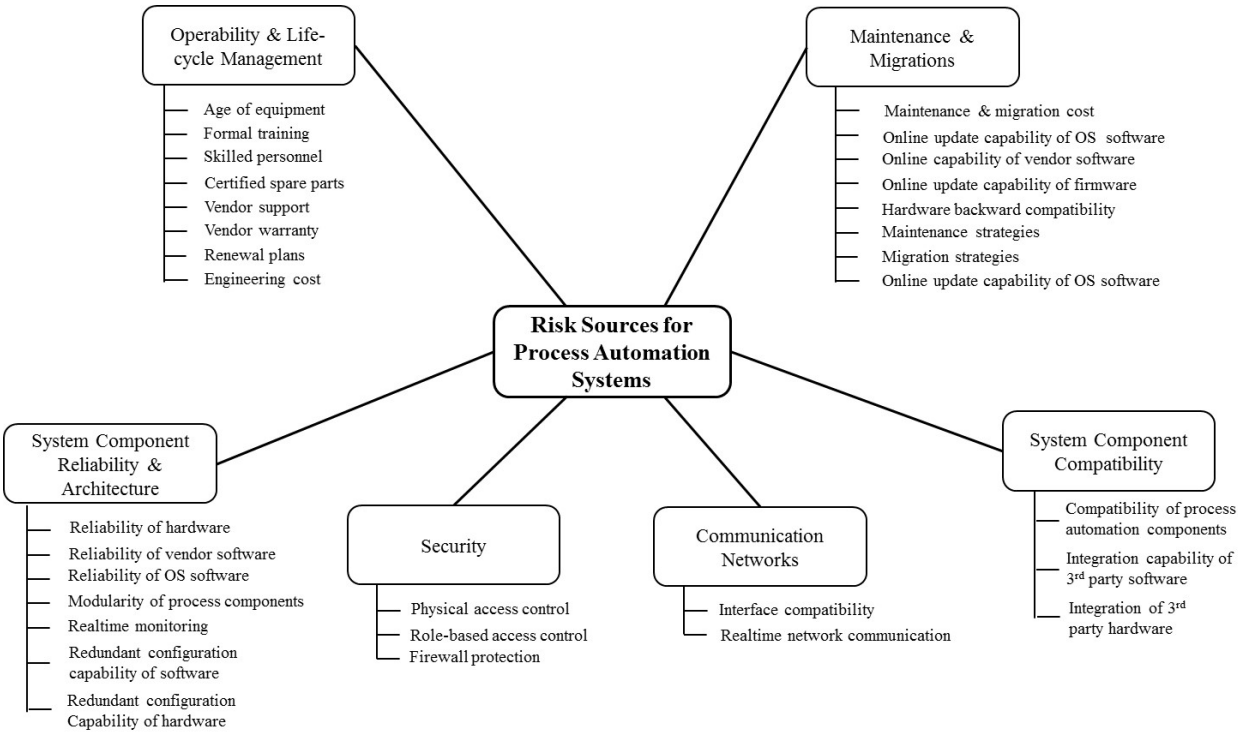

Fig. 3 Conceptual framework for process automation risk sources

IV. Research Methodology

The research commenced with a thorough landscaping of the literature to identify the various concepts pertaining to process automation systems. Based on the research objectives and the research problem, proposals were formulated and tested. Primary data were gathered from a survey questionnaire that was distributed to the different technical fraternities of the company. The conceptual framework shown in Fig. 3 was used to design a questionnaire with six categories and 32 questions. Two main instrumentation sample groups have been identified for this study, i.e. Senior Level and Junior Level.

The primary data from the quantitative survey were obtained by using a five-point Likert-style scale ranking. The data were then statistically analysed using IBM® SPSS® Statistics software (Version 25). As part of the research analysis, the reliability of the six categories was tested by analysing the results of each category's questions. The reliability test was performed by averaging the results of each category using the internal consistency coefficient, i.e. the Cronbach's Alpha [13].

Saunders et al. [12] suggested that an exploratory data

analysis approach (EDA) should be followed when trying to describe and compare variables numerically. Saunders et al. [12] also suggested that the central tendency of a variable can be described using three different descriptive measures, namely the mode, median and mean.

V. Results

A total of 172 survey questionnaires were distributed by means of an embedded link using company e-mail service. 85 respondents returned the completed questionnaire but 10 were incomplete and therefore discarded. Thus, 75 valid responses were available for analysis.

A. Composition of Sample Group

The sample group comprised some role categories or job positions as illustrated in Fig. 4. Engineers and foremen were the best represented in the sample.

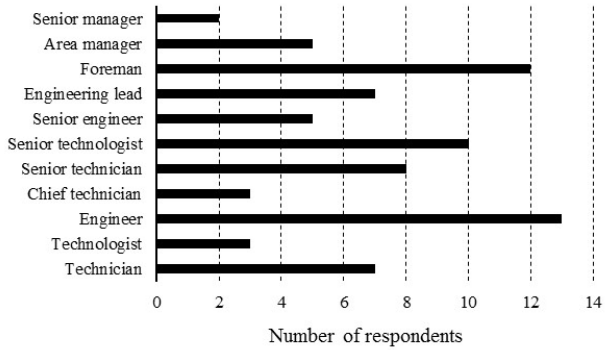

Fig. 4 Composition of two sample groups

B. Validity and Reliability of Data

The internal consistency coefficient (Cronbach's Alpha) was determined with the SPSS® software to confirm the reliability of the six categories by testing each category's questions (variables) for internal consistency. An alpha value of greater than 0.7 is an indication of high internal consistency. All the proposed categories had alpha values greater than 0.7, which meant that the data passed the reliability test and can be used in further analysis.

C. Verification of the Proposition

Each category of the proposed model comprised a number of questions as indicated in the Appendix. The responses for each question were summarised for each group and averaged to produce an overall risk ranking for each individual category. The analysis is followed by descriptive results in the form of means and standard deviations for each question. The descriptive analysis summary results for each category are illustrated in Fig. 5.

The mean value results are an indication that the sample population shares the same perception to the various sources of risks. The Operability & Life Cycle Management category registered the highest perception of risks, whereas Security measured the lowest as seen in Fig. 5.

In the Operability & Life Cycle Management category, the respondents viewed the 'lack of skilled personnel' as the highest risk in the category. An 'insufficient vendor warranty policy' was perceived as the lowest risk in the category, but also had the highest standard deviation indicating uncertainty amongst the respondents.

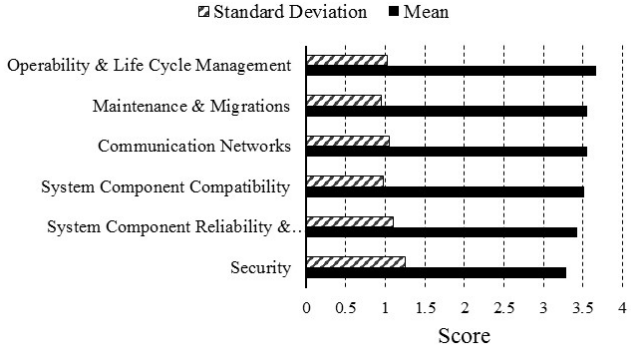

Fig. 5 Mean and standard deviation for risk categories

In the System Component Compatibility category, the respondents viewed the 'integration capability of third-party system software' as the highest risk, however 'the integration capability of third-party system hardware' was perceived as a less-risky area.

In the System Component Reliability & Architecture category the 'degree of reliability of the process automation hardware' was viewed as the highest risk and the respondents perceived the 'requirement for modular process automation system components' as the lowest risk.

In the Maintenance & Migrations category the respondents viewed the 'excessive costs pertaining to performing maintenance and migrations on process automation systems' as the highest risk. The respondents viewed the 'requirement to have the capability of performing periodic online updates of the vendor application software' as the least risky requirement,

In the Communications Network category, the respondents were given only two risks and 'inadequate interface compatibility of the communication networks' and 'inability to achieve real-time network communication' were both viewed as high risks (see numbers 28 and 29 in Table I).

In the Security category the respondents viewed 'insufficient role-based access control' as the highest risk in the category. The risk 'inadequate physical access control to the process automation equipment' was viewed as the lowest for this category.

D. Most Important Risks

The following seven risks from all six categories were identified as the most important by the respondents.

a) Lack of skilled personnel
b) Integration capability of third-party system software to the existing process automation system
c) The degree of reliability of the process automation hardware
d) Excessive cost related to process automation maintenance and migrations
e) Inadequate interface compatibility of real-time communication networks

f) Excessive installation and integration cost of new system hardware or software
g) An undersupply/scarcity of certified spare parts for the process automation system

E. Testing of Propositions

In order to address the research problem, it was also proposed that the instrumentation engineering groups do not have different viewpoints on the criticality of risks within the process automation domain.

1) Ranking of Categories

Respondents were requested to rank the six risk categories on a scale of 1-6, with 1 being the lowest and 6 being the highest risk to the process automation systems. The mean values for the senior level and junior level respondents are compared for the six categories in Fig. 6.

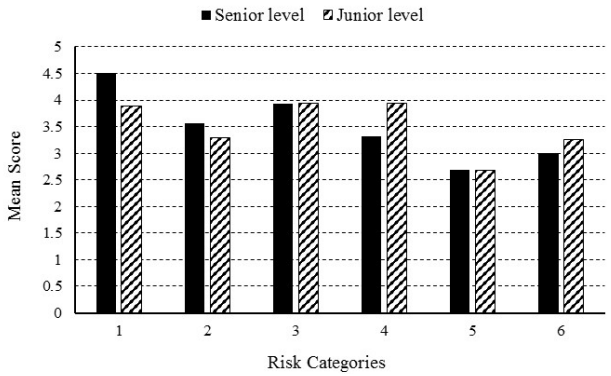

Fig. 6 Mean scores for two sample groups

The ranking analysis showed that the Senior Level perceived the Operability & Life Cycle Management (Category 1) and System Component Reliability & Architecture (Category 3) as the highest risk categories, whilst perceiving the Communication Networks (Category 5) as the lowest risk category. The Junior Level perceived the System Component Reliability & Architecture (Category 3) and the Maintenance & Migrations (Category 4) as the highest risk categories, with Communication Networks (Category 5) as the lowest risk category. Overall, Fig. 6 shows that the two groups share a similar mindset in most of the categories, especially in the System Component Compatibility (2), System Component Reliability & Architecture (3), Communication Networks (5) and Security (6) categories.

From Fig. 6 it is evident that good agreement exists between the various engineering levels of the technical instrumentation fraternity. The only noticeable differences in viewpoints exist in the Security (6) category. The descriptive statistical analysis is however not sufficient to draw conclusions on whether the views of the two groups differ significantly. The final step of the analysis is to determine whether there is a significant difference between the perceptions of the two sample groups, with regards to the six categories. One method to test for significant difference between two independent variables is by using the independent sample t-test. However, a requirement of this test is that the data sets do not violate the normality assumption. Since the two sample groups each consist of less than 50 respondents, the Shapiro-Wilk test can be applied to test for normality of the ranked data sets. This test was executed by means of the *Explore* function of the SPSS® software. Should the p-value be greater than 0.05, the data are normally distributed. However, the Shapiro-Wilk test for the Senior and Junior Level groups for each of the six categories showed $p < 0.05$ and the normality assumption is therefore incorrect.

2) Mann-Whitney U Test

To test the hypothesis, it will be required to use the non-parametric test namely Mann-Whitney U test for data which is not normally distributed. The Mann-Whitney U test was performed using legacy non-parametric 2- independent sample test of the SPSS® software.

Based on the results of the Mann-Whitney U test, there is no evidence to reject the null hypothesis at the 5% level of significance since none of the categories have $p < 0.05$. Therefore, the null hypothesis (H_0) is accepted and the alternative hypothesis (H_1) is rejected, which is an indication that the instrumentation engineering groups do not have different viewpoints on the criticality of risks within the process automation domain.

F. Summary and Discussion

In each risk category the respondents indicated some high-risk events which are summarized in the following paragraphs.

1) Operability & Life Cycle Management

A potential risk can emanate from not having enough skilled personnel. This could potentially be caused by having a multitude of process automation systems and the lack of knowledge from the first line maintenance to support the various systems. Skills can also be lost with higher turn-over of the maintenance support personnel. This could also mean that some personnel leave the company very soon after obtaining the relevant training and certifications for the specific process automation systems. This could mean that skill retention and transferal of knowledge within the organization is poor.

2) System Component Compatibility

The incompatibility and lack of integration of some third-party software can lead to a risk in this category. This risk can potentially be averted if the different software applications are running on the same platform. IT and software service providers sometimes provide systems that are difficult or even impossible to support and this can lead to production risk implications. This risk can be averted during the initial technology selection process.

3) System Component Reliability & Architecture

If the process automation hardware is not reliable and available to operate the plant, then the maintenance and downtime costs can escalate dramatically. Due to the age of some of the hardware, the reliability depends on the backup

system instead of itself. If hardware redundancy is built in, then reliability is not that important since a backup system will take over.

4) Maintenance & Migrations

Excessive costs of performing maintenance and migrations can prevent the maintenance manager or business from adopting new technology. High cost of maintenance can cause the production managers and senior managers to stall on migration and maintenance due to cost cutting measures. If the maintenance or migration is critical and is not done, it can lead to potential problems in the future.

5) Communication Networks

There is also the risk of having third-party communication interfacing problems as well as real-time communication issues when interfacing the existing process automation system with older communication network technologies. To overcome this issue, it is required to install some sort of protocol translator, thus introducing another point of failure. These translators or converters are normally non-redundant devices and a black box that can be forgotten about or cause long hours of troubleshooting. This can be circumvented by doing proper technology selection during the initial design stages before a system is purchased.

6) Security

Personnel with minimal knowledge of the system should not be granted access until the relevant training competency can be confirmed. If not, an inexperienced user can potentially make modifications which can render the plant inoperable. System passwords that are shared by team members also introduce system security risk since one will not be able to trace who made the changes. This can lead to a serious production event.

VI. Conclusion

The preliminary internal investigation suggested that the technical fraternities responsible for the process automation environment of the company operations and maintenance might not share the same viewpoint on various risks and the criticality of those risks emanating from their existing process automation systems. To address the research problem and objectives, it was important to first explore and establish a sound theoretical framework. A holistic framework was proposed that integrated the main concepts from the literature study (Fig. 3). This allowed sources of risks to be identified in the process automation field of a typical manufacturing company. To succeed in the scientific relevance of the research, it was required to follow an EDA approach by applying quantitative data analysis techniques on the primary data gathered from survey questionnaires.

The outcome from the descriptive statistics indicated that there was little difference in the viewpoints of the technical personnel on what they perceived as risks in their respective environments. It was also determined that the viewpoints on the criticality of risks within the process automation domain are mutually perceived. This meant that alignment between the Senior and Junior levels of the instrumentation technical fraternity does exist. Some of the main questions for each risk category stood out as high-risk events from the rest.

Appendix

The first two questions of the questionnaire requested information on the respondent's experience and the business unit or which he/she was working. The technical part of the questionnaire comprised 30 questions related to risk sources in the instrumentation division as shown in Table I.

TABLE I
Questions 3-32 of Questionnaire

No.	Description
3	Lack of skilled personnel (certification and/or years' experience in process automation systems)
4	Lack of formal training opportunities for all your process automation systems
5	Age (maturity) of the process automation equipment
6	An undersupply/scarcity of certified spare parts for the process automation system
7	A shortfall in locally available vendor support (recognized vendor support)
8	An insufficient vendor warranty policy
9	Inadequate equipment roadmaps for your process automation systems (renewal plans)
10	Excessive installation and integration cost of new system hardware or software (engineering cost - "rip and replace")
11	The degree of compatibility (interoperability) between hardware, vendor application software and operating system software
12	Integration capability of third-party system hardware to the existing process automation system
13	Integration capability of third-party system software to the existing process automation system
14	Redundant configuration capability of process automation hardware
15	Redundant configuration capability of process automation software
16	The degree of reliability of the process automation hardware
17	The degree of reliability of the vendor application software
18	The degree of reliability of the operating system software (Windows)
19	The degree of modularity of the different process automation system components
20	Inadequate access to real-time monitoring (equipment health monitoring)
21	Periodic/Ad-hoc online update capability of operating system software (Windows)
22	Periodic/Ad-hoc online update capability of vendor application software
23	Periodic/Ad-hoc online update capability of process automation component firmware
24	Process automation hardware backward compatibility
25	Inadequate maintenance strategies for process automation hardware and software
26	Inadequate migration strategies for process automation hardware and software
27	Excessive cost related to process automation maintenance and migrations
28	Inadequate interface compatibility of the communication networks to allow for multiple systems to communicate with each other over different mediums
29	The inability to achieve real-time network communication between the different process automation system components
30	Inadequate physical access control to the process automation systems
31	Insufficient role-based access control to the process automation systems (password control)
32	Inadequate firewall protection and access lists (cyber security)

REFERENCES

[1] K. Upasani, M. Bakshi, V. Pandhare, & B. K. Lad, Distributed maintenance planning in manufacturing industries. Computers & Industrial Engineering, 108(1), pp 1-14, 2017.
[2] T. Samad, P. McLaughlin & J. Lu, System architecture for process automation: Review and trends. Journal of Process Control, 17(3), pp 191-201, 2007.
[3] M. Hollender, Collaborative process automation systems. Research Triangle Park, NC: ISA, 2010.
[4] C. Johnsson, ISA 95-how and where can it be applied? ISA Expo 2004, Houston, TX, USA, 7(1), pp 1-10, 2004.
[5] S. Takata, F. Kirnura, F. J. A. M. van Houten, E. Westkamper, M. Shpitalni, D. Ceglarek, & J. Lee, Maintenance: Changing Role in Life Cycle Management. CIRP Annals - Manufacturing Technology, 53(2), pp 643-655, 2004.
[6] T. Tran, & Q. P. Ha, Dependable control systems with Internet of Things. ISA Transactions, 59(1), pp 303-313, 2015.
[7] T. Sauter, The Three Generations of Field-Level Networks, Evolution and Compatibility Issues. IEEE Transactions on Industrial Electronics, 57(11), 2010, pp 3585-3595.
[8] P. S. L. Jämsä-Jounela, Future Trends in Process Automation. IFAC Proceedings Volumes, 40(1), 2007, pp 1-10.
[9] L. Swanson, An information-processing model of maintenance management. International Journal of Production Economics, 83(1), 2003, pp 45-64.
[10] R. J. Ruitenburg, A. J. J. Braaksma, & L. A. M. van Dongen, A Multidisciplinary, Expert-based Approach for the Identification of Lifetime Impacts in Asset Life Cycle Management. Procedia CIRP, 22(1), 2004, pp 204-212.
[11] D. Centindamar, R. Phaal, & D. Probert, Technology Management. Activities and Tools. Basingstoke, New York: Palgrave MacMillan. 2010.
[12] M. N. K. Saunders, P. Lewis, & A. Thornhill, Research methods for business students, Seventh edition, Harlow, Essex, England: Pearson Education Limited. 2016.
[13] M. Tavakol, & R. Dennick, Making sense of Cronbach's alpha. International Journal of Medical Education, 2(1), 2011. pp 53-55.