International Journal of Engineering Applied Sciences and Technology, 2021
Vol. 5, Issue 10, ISSN No. 2455-2143, Pages 44-54
Published Online February 2021 in IJEAST (http://www.ijeast.com)

RISK ASSESSMENT OF A RFID - GSM BASED LOCK SYSTEM USING FMECA TECHNIQUE

S. O. Anaza
R&D Department
Power Equipment and Electrical Machinery Development Institute
Okene, Kogi State, Nigeria

J. D. Jiya
EEE Department
Abubakar Tafawa Balewa University Bauchi-Nigeria

Y. S. Haruna
EEE Department
Abubakar Tafawa Balewa University Bauchi-Nigeria

Abstract: Security systems are necessary everywhere especially in Banks, houses, offices etc. An RFID, GSM and Keypad Lock System is a multiprotocol device designed, constructed and customized to combine the security feature in RFID, Global System for Mobile communication (GSM) and password for the three components of access control which are identification, authentication, and authorization. The device was a series system (a failure of a unit result into failure of the system), therefore reliability analysis was conducted to reduce the failure rate using Failure Mode and Effects and criticality Analysis (FMECA). The aim of this paper is to present the reliability analysis of this security system. Each component/unit will be analyzed, depending on the degree; numbers were allotted for severity, occurrence and detection, and subsequently, the risk priority number (RPN) will be obtained for each unit and subsequently for the system before and after an action to increase its reliability. With the reliability measures, The result obtain shows that the severance of the system reduces by ~16.4, occurrence by 50% and detection by ~11%. The RPN also reduces by ~ 68%.

Keyword: FMECA, RPN, RFID, GSM, severity, occurrence and detection

I. INRODUCTION

Failure Mode and Effects Analysis (FMEA) is a proactive process aimed to evaluate a system, design, process and service for possible ways in which failures can occur [1]. An FMECA is generated from an FMEA by adding a criticality figure of merit. It is a technique used to identify, prioritize, and eliminate potential failures from the system, design or process before they reach the customer [2], it is used to resolve potential problem in a system during the design stage. FMECA can be required and applied during all stages of projects: at early design phase, during the detailed design and being the device in operation [3]. These analyses are performed for reliability, safety, and supportability information. The FMECA version is more commonly used and is more suited for hazard control. Terms and rules of safety analysis for electronic component are well described in well known ISO/IEC international standard series and technical reports [4]. A RFID-GSM base lock system is a security device designed, constructed and customized for a lock system. It has four security features which are: RFID system, the GSM module, password (keypad) and alarming mechanism (buzzer). The latter was additional security feature for notification. Each of this security features are used for three basic component of access control (identification, authentication and confirmation). Other component of the lock system are microcontroller and liquid crystal display (LCD), shown in figure 1.

The Microcontroller Controls the operation of the system while the GSM Module Send 4 digit code generated by the microcontroller to the person after the tag has been read successfully. The Buzzer notify any closer person any attempted intruder, LCD display any recommended information and the Key Pad will be use to enter the code after text message containing code is send to GSM of authorized user. The RFID reader reads the ID number from passive Tag and sends it to the microcontroller for confirmation,

From the literature reviewed, [5] highlighted the analysis of failure events observed in DC brush motors using the FMECA Technique. [6] performed a Failure Modes Effect and Criticality Analysis (FMECA) on a PV system through the use of an octopus diagram for functional analysis of the system. [7] identified, analyzed and evaluated the potential risks of unexpected failures occurring in

International Journal of Engineering Applied Sciences and Technology, 2021
Vol. 5, Issue 10, ISSN No. 2455-2143, Pages 44-54
Published Online February 2021 in IJEAST (http://www.ijeast.com)

rolling stock using a failure mode, effects and criticality analysis-based approach. [8] represented a generic process of FMECA for centrifugal pump failures and a case study on centrifugal pump failure cost estimation actual and after implementation of optimum strategies of maintenance. [9] Conducted research on reliability of transformer and proposed Failure Modes and Effects Analysis (FMEA) technique to increase the reliability and economic value. [10] conducted a high-level failure modes and effects analysis to characterize potential hazards from compressed-hydrogen fuel cell vehicles and identify potential safety issues for Federal Motor Vehicle Safety Standards, the National Highway Traffic Safety Administration in Washington DC. [11] in their research identified and eliminate current and potential problems from a manufacturing process of cylinder head in the company through the application of Failure Mode and Effects Analysis (FMEA).

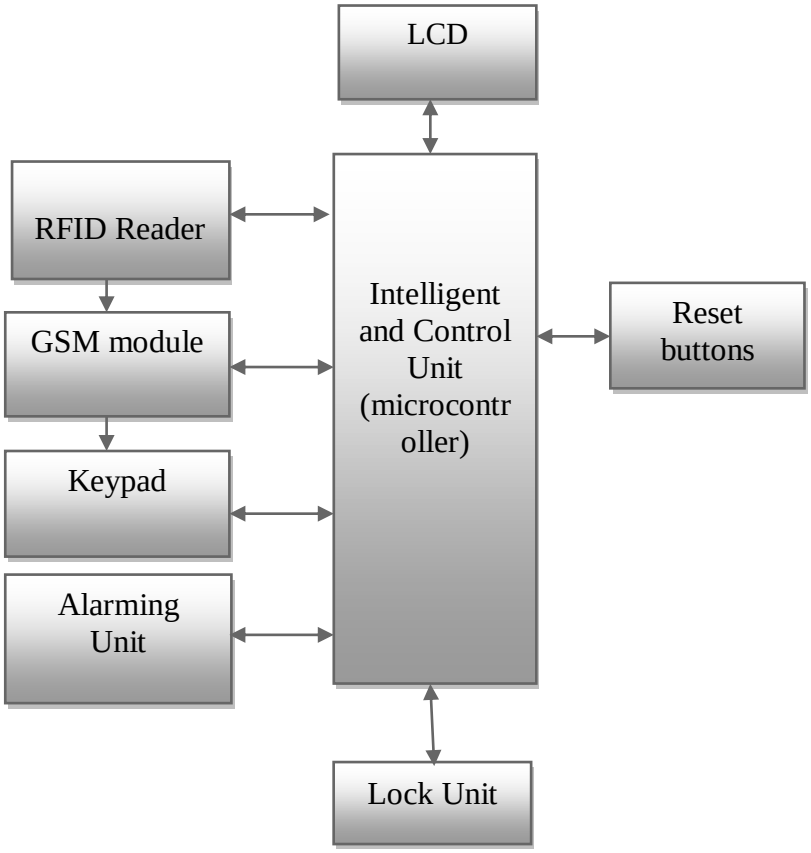


Figure 1: Block Diagram of the proposed Lock system

Everything that can fail, shall fail [12]. Due the important of security system, the reliability of such security lock system is as important as the security system itself. In most cases, developers of lock system ignore the risk assessment. These necessitate the needs to conduct reliability analysis on any designed lock system.

This paper presents the risk assessment of an RFID - GSM Based Lock System Using FMECA Technique by diligently studying the potential effect of fault, occurrence and possible detection. Depending on the degree, numbers were allotted and subsequently, the risk priority number (RPN) was obtained for each unit. Been a series system (a failure of a unit result into failure of the system), necessary actions were taken to reduce the RPN

II. FUNDAMENTAL CONCEPT OF FMECA

The following are the definition of some basic terms related to FMECA according to [13]. (i) Failure: Termination of the ability of an item to perform a required function. (ii) Failure mode: Manner in which an item fails. (iii) Failure cause and/or mechanism: Cause or sequence of causes that initiate a process (mechanism) that leads to a failure mode over a certain time. The most likely causes of

International Journal of Engineering Applied Sciences and Technology, 2021
Vol. 5, Issue 10, ISSN No. 2455-2143, Pages 44-54
Published Online February 2021 in IJEAST (http://www.ijeast.com)

the failure mode are listed under "Possible failure causes". (iv) Failure effects: Consequence of a failure mode in terms of the operation, function or status of the item.

The following are definition of terms related to FMECA according to [14]. (i) Severity: Severity is an assessment of the seriousness of the effect of the potential failure mode to the next component, subsystem, system or customer if it occurs. Severity applies to the effect only. A reduction in Severity Ranking index can be effected only through a design change. Severity Ranking is shown in Table 1. (ii) Occurrence (Event frequency): Occurrence is how frequently a specific failure cause/ mechanism are projected to occur. The likelihood of occurrence ranking number has a meaning rather than a value. Occurrence Ranking is shown in Table 2. (iii) Detection: Detection is the ability to detect the cause/mechanism/weakness of actual or potential failure. In Design FMECA, this must occur before the component, subsystem, or system is released for production. In Process/Service FMECA it must occur in time to prevent distribution in case of a product or catastrophe in case of an Asset / Maintainable Unit. In order to achieve a lower ranking, generally the planned control (e.g. preventative activities) has to be improved. Detection Ranking is shown in Table 3. (iv) Risk priority Number (RPN): The Risk Priority Number is the product of the Severity (S), Occurrence (O), and Detection (D) ranking. It is a measure of design risk.

$$RPN = S \times O \times D \quad \text{..... (1)}$$

Table 1: Table of Severity

Codes	Classification	Example
10	Hazardous Without Warning	Very High Ranking – Affecting safe operation.
9	Hazardous With Warning	Regulatory non compliance
8	Very High	Product becomes inoperable, with loss of function – Customer Very Much Dissatisfied
7	High	Product remain operable but loss of performance – Customer Dissatisfied
6	Moderate	Product remain operable but loss of comfort/convenience - Customer Discomfort
5	Low	Product remain operable but loss of comfort/convenience - Customer Slightly Dissatisfied
4	Very Low	Nonconformance by certain items – Noticed by most customers
3	Minor	Nonconformance by certain items – Noticed by average customers
2	Very Minor	Nonconformance by certain items – Noticed by selective customers
1	None	No Effect

Source: [11]

Table 2: Table of occurrence

Code	Classification	Example
10 and 9	Very High	Inevitable Failure
8 and 7	High	Repeated Failures
6 and 5	Moderate	Occasional Failures
4, 3 and 2	Low	Few Failures
1	Remote	Failure Unlikely

Source: [11]

Table 3: Table of Detection

Detection	Rank	Criteria
Extremely likely	1	Can be corrected prior to prototype/ Controls will almost certainly detect
Very High Likelihood	2	Can be corrected prior to design release/Very High probability of detection
High Likelihood	3	Likely to be corrected/High probability of detection
Moderately High Likelihood	4	Design controls are moderately effective
Medium Likelihood	5	Design controls have an even chance of working

International Journal of Engineering Applied Sciences and Technology, 2021
Vol. 5, Issue 10, ISSN No. 2455-2143, Pages 44-54
Published Online February 2021 in IJEAST (http://www.ijeast.com)

Moderately Low Likelihood	6	Design controls may miss the problem
Low Likelihood	7	Design controls are likely to miss the problem
Very Low Likelihood	8	Design controls have a poor chance of detection
Very Low Likelihood	9	Unproven, unreliable design/poor chance for detection
Extremely Unlikely	10	No design technique available/Controls will not detect

Source: [11]

III. RISK ASSESSMENT OF RFID - GSM BASED LOCK SYSTEM.

The following assumptions were made in order to complete this analysis.

(i) In situations where there are several failure results for one component failure mode, the most severe failure mode was documented in the analysis.

(ii) Single component failures only were investigated where possible, otherwise, failure of a unit was considered [15].

(iii) [11] and [16] were the documents used as the basis for the definition of the FMECA and component failure modes.

Depending on the degree, numbers were allotted for severance, occurrence and detection, and subsequently the risk priority number was obtained for each unit. Been a series system (a failure of a unit result into failure of the system), necessary action was taken to reduce the RPN. The analyses were presented in tables 4 to 10. The DFMECA of the system is presented in table 11

.

Table 4: FMECA of power supply unit

Parts of power supply unit	**Failure Mode**	**Effects(s) of Failure**	**S**	**Risk rating**					**Actions Taken**	**Revised risk**			
				Cause(s) of Failure	**O**	**Fault Detection**	**D**	**RPN**		**S**	**O**	**D**	**RPN**
electrical Power supply from mains	Failure of power from mains	loss of power supply to the entire system	8	Load shedding fault, system maintenance	8	Extremely Unlikely	10	640	Battery backup ,. Indicator for main power supply	2	2	2	8
Transformer	open circuit, short circuit	loss of power supply to the entire system	8	Manufacturer defect, over loading, ageing	2	Design controls have an even chances	5	80		2	2	2	8
Rectifier	open circuit, short circuit	loss of power supply to the entire system	8	Manufacturer defect, over loading, ageing	3	Design controls have an even chances	5	120		2	2	2	8
Voltage regulator and other component	open circuit, short circuit, Output struck, input struck,	Unfiltered and unregulated power supply	7	Manufacturer defect, over loading, ageing	3	Design controls have an even chances	5	105		2	2	2	8
	Average		7.8		4		6.3	236.		2	2	2	8

International Journal of Engineering Applied Sciences and Technology, 2021
Vol. 5, Issue 10, ISSN No. 2455-2143, Pages 44-54
Published Online February 2021 in IJEAST (http://www.ijeast.com)

Table 5: FMECA of microcontroller unit

Name of Unit/function	Failure Mode	Effects(s) of Failure	Risk rating						Actions Taken	Revised risk			
			S	Cause(s) of Failure	O	Fault Detection	D	RPN		S	O	D	RPN
Microcontroller / Interlink the units and house the software	Output struck, input struck, drift of frequency	Leads to entire system failure	8	Manufacturer defect, static charges	4	Extremely Unlikely	10	320	Component earthing	8	1	10	80

Table 6: FMECA of software

Name of Unit/function	Failure Mode	Effects(s) of Failure	Risk rating						Actions Taken	Revised risk			
			S	Cause(s) of Failure	O	Fault Detection	D	RPN		S	O	D	RPN
Software (Mikro C) / Responsible control of the entire system	Data related [17]	System failure	8	Software designer defect	4	Very Low Likelihood	9	288	hardware redundancy, effective design and code reviews	5	2	9	90
	Event related [17]	System failure	8	Software designer defect	4	Very Low Likelihood	9	288		5	2	9	90
	Average		8		4		9	288		5	2	9	90

Table 7: FMECA of RFID system

RFID system	Failure Mode	Effects (s) of Failure	Risk rating						Actions Taken	Revised risk			
			SEV	Cause(s) of Failure	OCC	Fault Detection	DET	RPN		S	O	D	RPN
Tag failure.	Output struck, drift of frequency	System failure	8	Physical, Virus attack,	5	High Likelihood	3	120	Kept hidden	8	1	3	24
Failure of reader	input struck, drift of frequency	System failure	8	Physical, Virus attack, cloning, eavesdropping	6	Moderately High Likelihood	4	192		8	2	4	64
	Average		8		5.5		3.5	156		8	1.5	3.5	44

Table 8: FMECA of GSM module unit

GSM	Failure Mode	Effects	Risk rating							Revised risk			

International Journal of Engineering Applied Sciences and Technology, 2021
Vol. 5, Issue 10, ISSN No. 2455-2143, Pages 44-54
Published Online February 2021 in IJEAST (http://www.ijeast.com)

module		**(s) of Failure**	**SEV**	**Cause(s) of Failure**	**OCC**	**Fault Detection**	**DET**	**RPN**	**Taken**	**SEV**	**OCC**	**DET**	**RPN**
Communication network	Network failure	System failure	5	Bad network, complete network failure	5	High Likelihood	3	75	indicator	5	5	3	75
GSM Module	Output struck, input struck, drift of frequency	System failure	7	Manufacture defect,	2	High Likelihood	3	42	Careful selection	7	1	3	21
	Average		6		3.5		3	58.5		6	3	3	48

Table 9: FMECA of keypad unit

Name of Unit/function	**Failure Mode**	**Effects(s) of Failure**	**Risk rating**						**Actions Taken**	**Revised risk**			
			SEV	**Cause(s) of Failure**	**OCC**	**Fault Detection**	**DET**	**RPN**		**SEV**	**OCC**	**DET**	**RPN**
Key pad / provide access to key-in the password.	Open circuit, short circuit	System failure	8	Manufacturer defect, ageing	3	Moderately High Likelihood	4	96	Careful selection	8	2	4	64

Table 10: FMECA of lock unit

Name of Unit/function	**Failure Mode**	**Effects (s) of Failure**	**Risk rating**						**Actions Taken**	**Revised risk**			
			SEV	**Cause(s) of Failure**	**O**	**Fault Detection**	**D**	**RPN**		**SEV**	**OCC**	**DET**	**RPN**
The lock or motor /opens or lock the system	Winding Failure In short Mode	System failure	8	Low starting torque, Misalignment of teeth, worn out	5	High Likelihood	3	120	Current limit circuit introduced. Redundant motor and redundant winding to be introduced.	8	3	3	72

Table 11: FMECA of the lock system

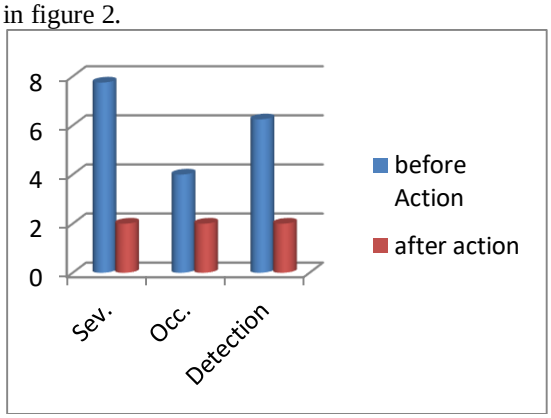
Name of system	**Risk rating**				**Revised risk**			
	S	**O**	**D**	**RPN**	**S**	**O**	**D**	**RPN**
lock	7.69	4.14	5.54	182.11	6.43	2.07	4.93	58

IV. RESULT AND DISCUSSION

The result of FMECA of each unit that make up the system shows an improvement in the system reliability. For the power supply unit, battery was used as a backup which changes severance from 7.75 to 2, occurrence from 4 to 2, detection from 6.25 to 2, and risk priority number (RPN) from 236.25 to. It thus reduces the severance if failure occur, possible occurrence and likelihood of failure detection by 74%, 50% and 68% respectively. Subsequently the risk priority number (RPN) reduces by 97% as shown

International Journal of Engineering Applied Sciences and Technology, 2021
Vol. 5, Issue 10, ISSN No. 2455-2143, Pages 44-54
Published Online February 2021 in IJEAST (http://www.ijeast.com)

in figure 2.



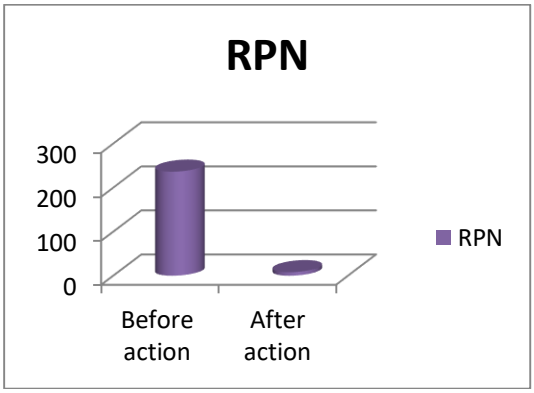
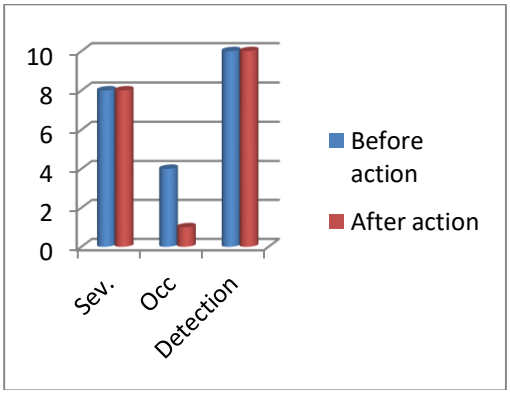


Figure 2: FMECA of power supply unit

In the microcontroller unit, Component earthing, careful selection of microcontroller was the action taken which changes only occurrence from 4 to1 and risk priority number (RPN) from 320 to 80. It thus reduces only the possible occurrence of failure by 75% whiles the severance and detection if failure occur remains unchanged. The risk priority number (RPN) also reduces by 75% as shown in figure 3.



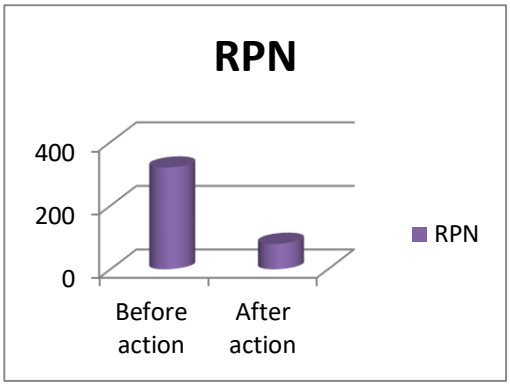
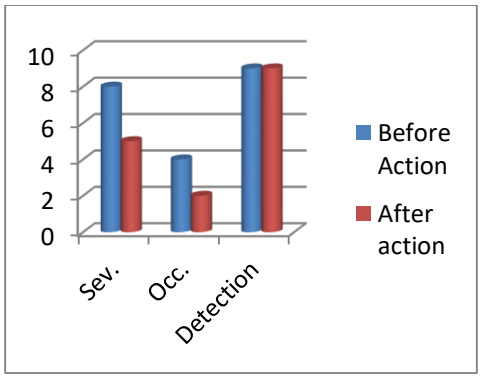
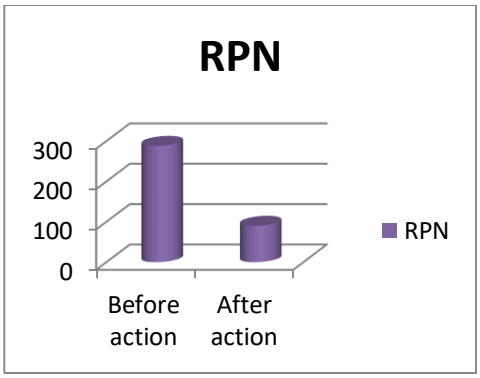


Figure 3: FMECA of microcontroller unit

To increase the reliability of the system, hardware redundancy, effective design and code reviews were the measures taken to increase the reliability of the software which changes the severance from 8 to 5 occurrence from 4 to 2 and risk priority number (RPN) from 288 to 90. This reduces the severance if failure occurs in the software by 37.5%, possible occurrence by 50% but the likelihood detection of such failure remains unchanged remains unchanged. Subsequently the risk priority number (RPN) reduces by 68.75% as shown in figure 4.

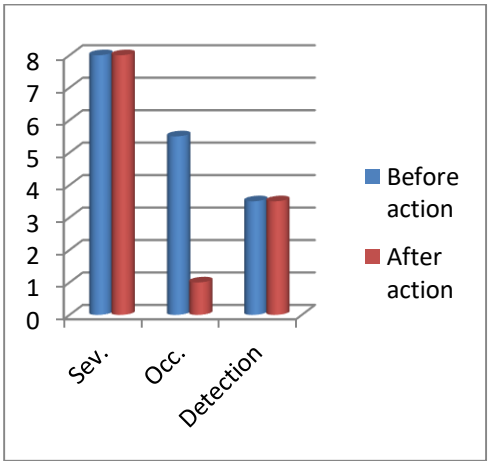




International Journal of Engineering Applied Sciences and Technology, 2021
Vol. 5, Issue 10, ISSN No. 2455-2143, Pages 44-54
Published Online February 2021 in IJEAST (http://www.ijeast.com)

Figure 4: FMECA of the software

For the RFID system: Physical, Virus attack, cloning and eavesdropping were the possible causes of failure. The RFID system (Tag and Reader) kept hidden which changes only occurrence from 5.5to 1.5 and risk priority number (RPN) from 156 to 44. It thus reduces the possible occurrence of failure by ~73% while the severance if it occurs and likelihood of detection remains unchanged. The risk priority number (RPN) reduces by ~72% as shown in figure 5.



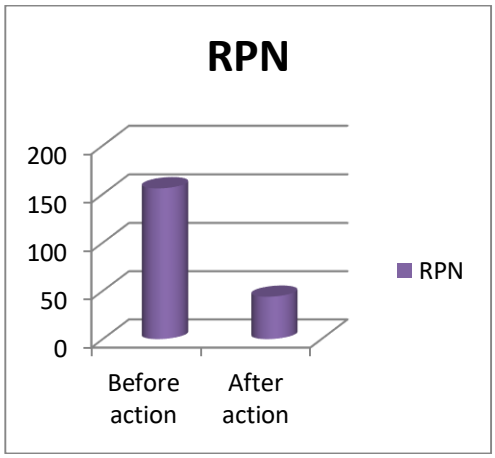
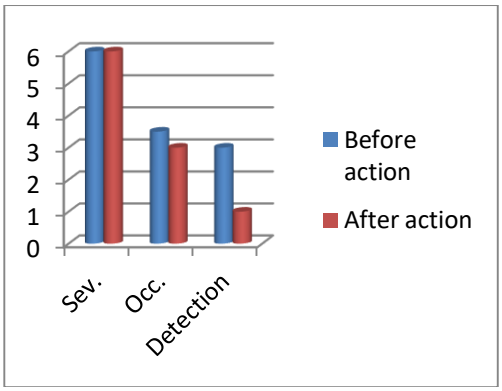


Figure 5: FMECA of RFID system

For the GSM module unit: Bad network, complete network failure and Manufacture defect, will have been the likely causes of failure. Careful selection was adopted to avert the latter and a light emitting diode (LED) to indicate when a command is given to the GSM module. These changes the occurrence from 3.5 to 3 detection from 3 to 1 and risk priority number (RPN) from 63 to 18 . Thus, reduce the possible occurrence of failure by ~43% and the likelihood of detection by 67% while the severance remains unchanged. The risk priority number (RPN) also reduces by ~76% as shown in figure 6.



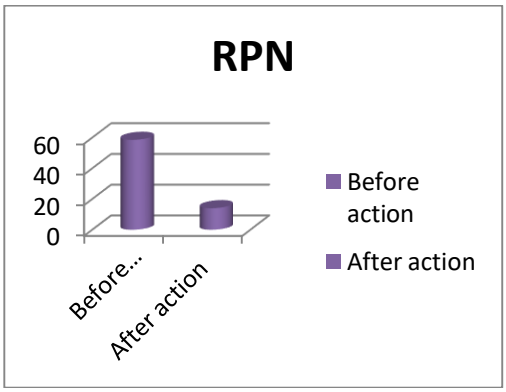
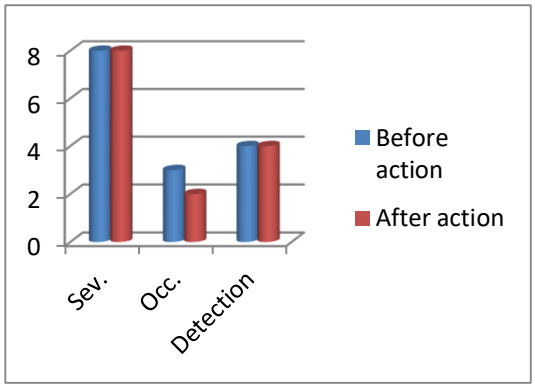


Figure 6: FMECA of GSM module unit

To reduce the failure rate of the system, careful selection of keypad was the measure taken in the keypad unit. This changes the occurrence from 3 to 2 and risk priority number (RPN) from 96 to 64. This reduces the possible occurrence of failure of the unit by ~33% but the severance if failure occurred and likely detection of such failure remain unchanged. Subsequently the risk priority number (RPN) also reduces by 33% as shown in figure 7.

International Journal of Engineering Applied Sciences and Technology, 2021
Vol. 5, Issue 10, ISSN No. 2455-2143, Pages 44-54
Published Online February 2021 in IJEAST (http://www.ijeast.com)



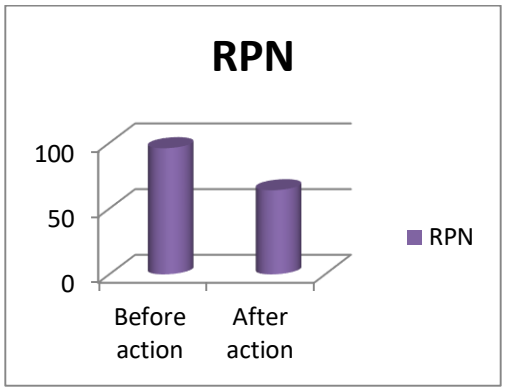


Figure 7: FMECA of keypad unit

High starting torques, Misalignment of teeth and worn out due to friction were predicted to be likely cause of failure. Lubrication is adopted to avert these which change the occurrence from 5 to 3 and risk priority number (RPN) from 120 to 72. Thus, rate of occurrence of fault is expected to reduce by 40%. The RPN also reduces by 40% as shown in figure 8.

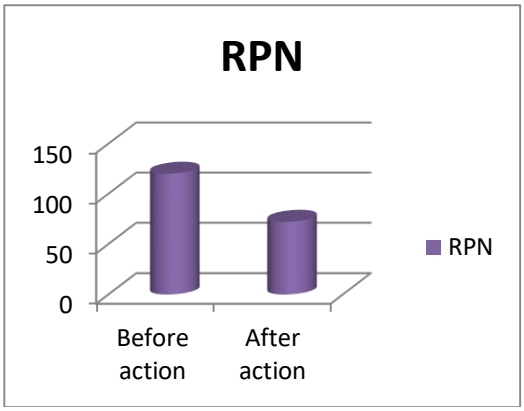
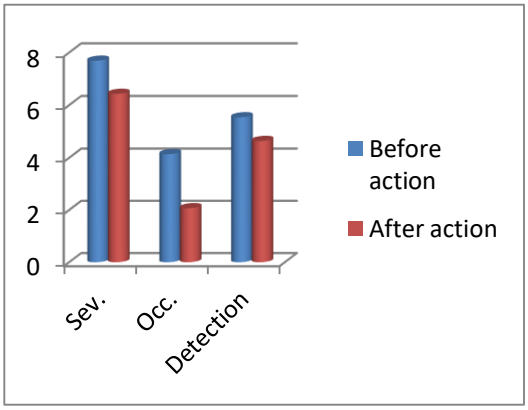


Figure 8: FMECA of lock system

With all the measures taken to increase the reliability of the system, the severance changes from 7.69 to 6.43, occurrence from 4.14 to 2.07, detection from 5.54 to 4.93 and risk priority number (RPN) from 182.11 to 58. Thus, the severance of the system due to failure reduces by ~16.4, the possible occurrence by 50% and the likely detection of such failure by ~11%. The RPN also reduces by ~ 68% as shown in figure 9.



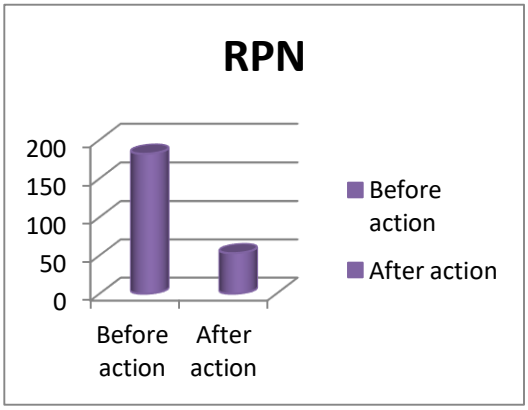


Figure 9: FMECA of the system

V. CONCLUSION

In this paper background information on an RFID-GSM based Lock System, and FMECA was presented. Reliability analysis has been conducted by defining the unit/component parts, identifying the failure modes, Effects(s) of Failure, Cause(s) of Failure and detection of fault. An action has been taken to improve the system reliability and a number has been allotted depending on the degree for severance, occurrence and detection and subsequently the RPN was calculated for both before and after the action. As shown in the result, the system reliability improved. While it is quite unlikely that any system can be made 100% reliable, identifying the failure modes and taking an action to increase the system reliability are vital steps toward improving any system reliability.

VI. REFERENCES

[1] Sellappan N. and Palanikumar K. (2013) "Modified Prioritization Methodology for Risk Priority Number in Failure Mode and Effects Analysis" International Journal of Applied Science and Technology Vol. 3 No. 4pp 27-36

[2] Tamer M. E., Ahmed M. E., Islam H. A. and Ahmed A.(2016), "Implementation of FMECA and Fishbone Techniques in Reliability Centered Maintenance Planning" International Journal of Innovative Research in Science, Engineering and Technology, Vol. 5, Issue 11 pp 1801-1811

[3] http://media.futuresmag.com/futuresmag/article/2012/07/05/istock_000019129829XSmall- resize-380x300.jpg

[4] Illiashenko O. & Babeshko E (2012): "choosing FMECA-based techniques and tools for safety analysis of critical systems" Information and security, An international journal, vol 28, No 2, pp 275-285

[5] Shwetha K, Narahari N. S. & Chandra S. P. (2013), "Failure Mode Effect and Criticality Analysis Performance Test on DC Brush Motors Used in Spacecraft Applications" International Journal of Research in Engineering & Technology (IJRET) Vol. 1, Issue 2, pp 169-176

[6] Omar N. S. et al, (2017), "Analysis of Failure Modes Effect and Criticality Analysis (FMECA): A Stand-Alone Photovoltaic System", Science Journal of Energy Engineering. Vol. 5, No. 2, pp. 40-47. doi:10.11648/j.sjee.20170502.11

[7] Fateme D., Babakalli A. Mahmood S. Christophe B. and Ashraf L. (2016) "Risk Evaluation of Railway Rolling Stock Failures Using FMECA Technique: A Case Study of Passenger Door System" Urban Rail Transit DOI10.1007/s40864-016-0043-z www.springerlink.com

[8] Deeptesh S. and Amit S. (2015) "Study of Centrifugal Pump Using Failure Mode Effect and Critical Analysis Based on Fuzzy Cost Estimation: A Case Study" International Journal of Science and Research (IJSR) Volume 4 Issue 7, pp 19-22 www.ijsr.net

[9] Mohsen A., Khazaee P. Sabetghadam I., and Karimifard P. (2013) "Failure Modes and Effects Analysis (FMEA) for Power Transformers" paper presented at 28th Power System Conference - 2013 Tehran, Iran

[10] Denny R. S., Susan E. R., Stephanie A. F., Stephen M. R., and Paul E. G. (2009) "Failure Modes and Effects Analysis for Hydrogen Fuel Cell Vehicles – Subtask 1" Battelle Memorial Institute 505 King Ave Columbus, OH 43201

[11] Tejaskumar S. P. and Mihir T. P (2014) "A Case Study: A Process FMEA Tool to Enhance Quality and Efficiency of Manufacturing Industry" Bonfring International Journal of Industrial Engineering and Management Science, Vol. 4, No. 3 pp145-152

[12] Ebeling, C. (2010), " Intro to Reliability & Maintainability Engineering," 2nd ed. Waveland Press, Inc.

[13] Akbari M, Khazaee P. Sabetghadam I. and Karimifard P. (2013) "Failure Modes and

Effects Analysis (FMEA) for Power Transformers" 28th international power system conference Tehran Iran

[14] SYDNEY WATER (2010) , "Failure Mode Effects and Criticality Analysis (FMECA)", Document Owned by Manager, Strategic Asset Management BMIS Number: AMQ0006 Version 03 Issue Date: June Page 1-11

[15] Final Report of FMECA analysis for Battery Charger board prepared for AEi Systems, LLC 5933 W. Century Blvd. Suite 1100 Los Angeles CA 90045 (2006)

[16] ANNEX 6: EEE Components Failure Modes for FMECA

[17] Ann M. N. (2010) "Software Failure Modes Effects Analysis Overview" SoftRel, LLC pp 1-26 www.softrel.com amneufelder@softrel.com