Interdisciplinary Description of Complex Systems 20(3), 222-229, 2022

IDENTIFYING FAILURES IN MOBILE DEVICES

Esmeralda Kadena[1], * and András Keszthelyi[2]

[1]Óbuda University, Doctoral School on Safety and Security Sciences
Budapest, Hungary

[2]Óbuda University, Keleti Faculty of Business and Management, Institute of Management and Organisation
Budapest, Hungary

DOI: 10.7906/indecs.20.3.1
Regular article

Received: 4 April 2021.
Accepted: 31 December 2021.

ABSTRACT

Mobile devices are well-known communication tools. People, especially young people, cannot go even one step without them. Technological advancements provide better features, but at the same time, such systems still face security risks. Protective layers do exist, but some systems are automated and engineered, while others rely on humans. This work begins with examining some critical points related to the weakest link in the security chain: the human factor. Errors are given in the view of the Swiss Cheese Model by emphasizing the role of latent conditions in "holes".

We found that the Swiss Cheese Model has some limitations. In order to enhance it, we have used the Failure Mode and Effect Analysis risk matrix methodology. Thus, we represent its application on mobile devices to demonstrate that it can give us more accurate results by identifying the most critical points where manufacturers should focus on. This work is based on qualitative data, and it provides the basis for quantitative research. In the end, we suggest that in order to obtain more accurate findings, the Failure Mode and Effect Analysis can be further extended.

KEY WORDS

mobile device, SCM, FMEA, human errors, failures

CLASSIFICATION

JEL: C25, L15, L63, L96

*Corresponding author, η: kadena.esmeralda@phd.uni-obuda.hu; -;
Doctoral School on Safety and Security Sciences, Obuda University,
H-1081 Budapest, Népszínház utca 8., Hungary

INTRODUCTION

Over the years, the industry of information technology has made increasing progress, and we can find it present whereever we are. People’s life is related to mobile devices as the use of them for personal, and business, purposes has become very popular. On the other hand, these devices and systems are posed to some risks. One of the main issues is the impact of human errors in such systems. Human and organizational errors stand for unanticipated or undesirable effects resulted by the poor performance of an individual or a group. The human factor is the weakest link in the interfacing process and keeping secure information with machines that they interact with [1]. The errors to hardware or software can be unintentional because of the lack of training or intentional violation of guidelines [2]. Information security loss also happens because of the corporations; the reactive management approaches that they use in security incidents [3] as well as a result of the human factor. The progress related to such issues is still slow and fails to keep pace with the evolution of threats [4].

Senders and Moray defined human error as a behavior that can be observed [5]. Its origin processes on different levels where performance standards are needed for its evaluation, and it is initiated by an event where there was a possibility to act in another way, but correctly. Hollnagel states that a human error can only be observed by observing human behaviors first. In his surveys’ review, it is showed that the estimated contribution of “human errors” to incidents ranges from about 20 % to around 80 % [6]. Accordingly, human errors are comprised of three parts. The first one is the evaluation of the human behavior against a criterion or standard performance. The second one is related to an event that results in a measurable performance the expected level of which is not met by the acting agent. The third part is a degree of volition where the actor can act in a way that will not be accounted for mistakes.

We examine how human errors and latent conditions are represented in mobile devices systems under the Swiss Cheese Model (SCM). Then we propose the application of the Failure Mode and Effect Analysis (FMEA) risk matrix methodology as an extension of the SCM. After applying this methodology in mobile devices, we present and discuss the results. Our conclusions are drawn in the final section.

HUMAN ERRORS IN VIEW OF THE SCM

The Swiss Cheese Model of accident causation, developed by Reason, is a popular tool used to analyze root cause and investigate incidents [7]. It was shown that accidents are a result of the relationship between active failures – “unsafe acts” by operators and latent conditions of the system. Active failures stand for unsafe acts made by operators [7]. Latent conditions are known as “pathogen agents” that involve factors that contribute to an accident such as organizational culture, decisions made by the management, design of procedures, or training deficiency. Accordingly, when active failures or underlying conditions successfully penetrate the defenses, accident(s) can occur [8, 9]. Moreover, the SCM can be seen as a means of communication and used for primary analysis and measurements [10]. The crucial point is related to knowing “holes” or system failures and what they are. After this, investigators should detect and eliminate them to avoid the occurrence of an accident [11].

Human actions are classified as skill-based, rule-based, and knowledge-based [8]. There are also intentional actions that cause non-compliance routinely; when a rule is barely implemented, and its removal has become a norm. Before the entire culture is at high risk, there is a need to fix the wrong practice. Violations can also be exceptional when a calculated risk is taken because of specific conditions to carry out another task. According to Balaouras and Cser, employees have expectations for their mobile experience. They are not willing to wait for security leaders to provide them with the proper devices and apps they need to do their jobs effectively. The results show that employees do not fully understand the risks in mobile devices [12]. Maxion and Reeder found that undependable user interfaces are more prone to the flaws in the design, and they can be a significant factor in the human error that causes security breaches [13]. Malware is becoming more and more undetectable. Mobile devices are exploited by four vectors running in the background all the time, such as alarm clocks, emoji keyboard, music applications, and flashlight applications [14]. Additionally, when the lack of security in mobile devices is combined with the privileges granted in the privacy agreements, it poses a considerable risk to them.

Mobiles are always in the peoples' pockets, and they bring those to the workplace, too. BYOD is one of the challenges that mobile security is dealing with. In many organizations, people want to bring their own devices and use them on company networks. According to the Check Point, the companies allowing the use of mobile for work purposes were attacked 54 times more frequently on average [15]. Kaspersky found that more than half of industrial organizations permitting outsiders to access critical systems remotely and 63 % of those that allow access to outsiders are more likely to experience a cybersecurity breach than those that do not allow access [16]. People tend to be lazy while installing and accessing applications. Developers have realized that collecting keystrokes is useful for marketing purposes, and accessing the contact lists for it, is more profitable. Consequently, spying on customers and collecting data without peoples' permission help developers to make more money. Furthermore, employees do not access only their information on mobile devices; they also access sensitive organizational content (financial data, strategy materials of the corporate, etc.) [12].

Another critical issue is related to the coming and going of employees. They can bring risks they already have in their mobile devices even though the network might be locked down. Vanson Bourne states that from all the threats that organizations face these days, phishing attacks remain the most significant challenge, with 56 % of respondents identifying these attacks as a main concern [17]. There do exist some ways to address these challenges. A possible countermeasure might be the education and training of employees. Human errors may cause accidents, but accidents may not be caused purely by human errors. The confluence of a whole chain of mistakes can cause accidents. To reduce casualties, safety analysts must firstly identify the type of human and company errors that cause fatalities and then study and determine how accidents happen.

Following the SCM, the barriers presented as layers consist of technology, processes, and people in the end. So, we cannot imagine that the most significant holes are in the last layer. Neither that a single error can cause an accident. The presence of latent conditions that are present before a specific accident occurs is also significant [10]. Thus, not only the human factor in the end, but also the alignment of several holes through all layers can cause failures. The main point is to detect the "holes" and correct them before an accident occurs. These can be achieved by identifying what the "holes" are, how big they are, and what their correlation is [18]. Before developing new devices, engineers can consider human behavior as accepted in the way it is. A solution might be the approach of human-centered design, which puts on first-line human needs, capabilities, and behavior and then start designing to accommodate them [19]. For this, an understanding of psychology and technology is needed.

FAILURE MODE AND EFFECT ANALYSIS IN MOBILE DEVICES

FMEA was developed in 1949 and is used to identify and analyze all failure modes of various parts of the system [8]. FMEA is a step by step tactic, and its objectives are to identify all possible failures throughout the processes, study the consequences of these failures, find the links between causes and effects, search and solve and make decisions based on the requirements of the appropriate action [20]. According to Johnson and Khan, the aim of applying FMEA is to continuously develop products and procedures consistent with consumers' satisfaction [21].

The indicator used for determining the right corrective action on failure modes is called the Risk Priority Number (RPN). After calculating RPNs values, it is easy to identify the areas of the most significant problem. Then the focus shifts to the solution of failure modes [22]. The advantage of FMEA is that it can be used in all phases of the system lifecycle from requirement specification to design, implementation, operation, and maintenance [23]. The significant benefit from FMEA can be achieved at the early design phases because the weakest point in the structure of the system can be revealed and addressed before doing expensive design changes in later stages. The process of FMEA starts with the identification of the scope of the system and its functions [23]. Brainstorming can be a useful method to find possible failure modes. Later, the effects and the causes of potential failures are determined. Risk analyses are done after detecting these possible causes and effects. The final phase consists of documenting the process and taking actions to reduce the risks.

RELATED WORK

Few researchers have addressed the failures issues in mobile devices. Marques analyzed FMEA in mobile phones, specifically the hardware [24]. His results showed that when designing a mobile device, manufacturers should give top priority to the device's shell. Two other researchers were focused on finding the weakest point of a mobile device at the design stage [25]. They concluded that to receive what is expected from the device, it is crucial to know its performance reliability.

Cinque et al. analyzed software failure data regarding freeze, self-shutdown, unstable behavior, output failure, and input failure on Symbian OS [26]. The results showed that most problems are caused by memory access violation errors and heap management. Furthermore, Cinque studied enabling online dependability assessment of the Android smartphone [26]. The author discussed the logging platform for the collection of failure data. Usually two types of failure occur in mobile devices; one can be the result of an accident and the other of the malfunction of hardware or software. Vijayalakshmi studied FMEA in Android OS [27]. According to his conclusions, top priority should be given to hardware. Only a few years ago, a malware was part of the ROM on factory-default in brand new smartphones [28]. From the software side, the problem of self-shut down was most dangerous issue as it could contribute to data loss or the failure of the OS.

APPLYING FAILURE MODE AND EFFECT ANALYSIS IN MOBILE DEVICES

In this study, we determined nine of the most frequent mobile device failures by using the brainstorming technique [29]. Six of the most frequent failure modes related to hardware and three of the most frequent software failure modes were highlighted. The FMEA method was conducted based on the following steps.

Step1: Identification of potential failures and effects. The most problematic components that we found in a mobile device are classified as *Hardware Failure Modes:* Touchscreen; Battery; Device Shell; Front camera; Rear camera; Microphones, and *Software Failure Modes:* Freeze; Self-shutdown; Output failure. Step 2: Determining severity. Severity (S) is a rating of the seriousness of the effect of a failure mode to the system, assembly, product, customer, or government regulation [23]. It is related to the Failure effect. Severity rates on a scale of 1 to 10, where 1 is the lowest and 10 is the highest. Step 3: Estimating Occurrence. Occurrence (O) is a rating responding to cumulative numbers of failures that could occur over the design life of a system or component [23]. It is related to the Failure Cause, and CNF stands for

Cumulative Number of Failures. Step 4: Failure Detection. Detectability (D) that is a rating of the ability of the proposed design control to detect a potential failure mode or occurrence [23]. It is related to Failure Control. The higher the value of D, the more likely the failure will not be detected. Step 5: Calculating Risk Priority Number (RPN). RPN is calculated based on the three above explained criteria - formula (1): a) The severity of the effect on the user and the mobile system itself, b) How frequently the problem is likely to occur, and c) How easily the problem can be detected.

$$\mathrm{RPN} = S \times O \times D. \tag{1}$$

Considering these steps, first we filled the FMEA form. The potential causes of failure occurrence for each failure mode and effects have been determined by taking into account the influence they have on the components and on the whole system of the mobile devices. To eliminate or reduce the potential causes of failures, recommended actions were given for each of the defined failure modes.

RESULTS AND DISCUSSION

Following FMEA steps, we calculated the values of Severity, Occurrence, and Detectability and then calculated the RPNs according to the respective formula (1). Our findings are represented in the table below:

Table 1. Collection of evaluated S, O, D and RPNs values.

COMPONENT	S	O	D	RPN
Touchscreen	9	6	3	162
Battery	9	7	4	252
Shell	4	8	4	128
Front-facing camera	4	2	8	64
Rare-facing camera	3	2	7	42
Microphones	5	6	3	90
Freeze	8	6	5	240
Self-shutdown	8	5	4	160
Output failure	7	4	5	140

According to the details and results from the FMEA method, we analyzed the RPNs values and reached our conclusions. The results highlight that the critical failures of the battery (RPN = 252) followed by mobile device freeze (RPN = 240) show that these should be given high priority. Their severity values are also high, and we can state that they pose a high risk. Severity criteria should be prioritized as they are related to failure effects in the whole system. Thus, touchscreen and self-shutdown components have to be considered. Possible recommendations derived from the FMEA form for each failure are as follows:

In the Hardware part – Touch-screen: more supervision; selection of more resistant material; improve sensitiveness; improve the quality design of (sys) apps - here responsive design should be taken into consideration. Battery: continuous work on making chips and OSs more efficient to save power; manufacturers should think seriously about the replacement of existing batteries. Device Shell: more supervision; selection of appropriate and more resistant material. Front camera: more supervision; improving the default camera app. Micro-phones: more supervision; improving the quality.

In the software part – Freeze: selection of proper and reliable software; more supervision. Self-shut-down: batteries should be checked; more supervision. Output failure: more cautiousness from the manufacturer side; more supervision.

We suggest that when conducting FMEA, it is essential to understand and decide which failure modes are more significant than others by extending this method with an additional weighting factor [30]. Moreover, by considering the potential causes, many of them are closely related to users' practices and behaviors in mobile devices. The digital habits of users and their unconsciousness about potential online threats pose a high risk in mobile device systems [31]. As human error is inevitable, two options can be seen: one is related to the acceptance of the current level of harm, and the other is to start viewing the current failures as a result of the present conditions of the system. Putting continuous effort into training, education, and programs about user awareness is a good measure, still, it does not promise the wanted results. Therefore, we suggest that on the extension of FMEA, increased attention must be paid on human errors. Putting more effort and focus on the design of elements in mobile device systems would be a good attempt to reduce or eliminate potential failure effects.

CONCLUSIONS

This article has highlighted the importance of the human factor in mobile devices. Following the SCM, any of the elements of such systems can contribute to the likelihood of an error occurrence. The design has a crucial role in reducing the risks. The evidence from this work suggests that as the SCM is a theoretical framework and not a prescriptive investigation technique, it has few details on its application in a real word. So, the SCM has its limitations as it does not provide a detailed accident model or a comprehensive theory of how functions and entities in a complex socio-technical system interact and depend on each other.

We suggested the application of FMEA Risk Matrix Methodology in mobile devices. Here, nine failure modes were considered. The RPNs results revealed that a failure on battery, followed by the freeze of mobile devices are the ones with the highest priority. On the other hand, touchscreen and self-shutdown failures also have high severity, and even though their RPNs are not the highest, they should be considered with top priority as well. Besides, we propose an extension of the FMEA method that uses additional weighting factors. More focus is needed on a human-centered design by taking into account people's needs, capabilities, and behaviors.

REFERENCES

[1] Metalidou, E. et al.: *The Human Factor of Information Security: Unintentional Damage Perspective.*
Procedia - Social and Behavioral Sciences **147**, 2014,
http://dx.doi.org/10.1016/j.sbspro.2014.07.133,

[2] Beatty, P.C.W. and Beatty, S.F.: *Anaesthetists' intentions to violate safety guidelines.*
Anaesthesia **59**(6), 528-540, 2004,
http://dx.doi.org/10.1111/j.1365-2044.2004.03741.x

[3] Qian, Y.; Fang, Y. and Gonzalez, J.J.: *Managing information security risks during new technology adoption.*
Computers & Security **31**(8), 859-869, 2012,
http://dx.doi.org/10.1016/j.cose.2012.09.001,

[4] Hadlington, L.: *The "human factor" in cybersecurity: Exploring the accidental insider.* In: McAlaney, J.; Frumkin, L.A. and Benson, V., eds.: *Psychological and Behavioral Examinations in Cyber Security*.
IGI Global, Hershey, 46-63, 2018,
http://dx.doi.org/10.4018/978-1-5225-4053-3.ch003,

[5] Senders, J.W. and Moray, N.: *Human error : cause, prediction, and reduction.*
L. Erlbaum Associates, 1991,

[6] Hollnagel, E.: *Human reliability analysis : context and control.*
Academic Press, London & Toronto, 1993,

[7] Reason, J.T.: *Human error.*
Cambridge University Press, Cambridge, 1990,

[8] Reason, J.: *Human error: Models and management.*
British Medical Journal - BMJ **320**, 768-770, 2000,
http://dx.doi.org/10.1136/bmj.320.7237.768,

[9] Reason, J.: *Human Error.*
The Western Journal of Medicine **172**(6), 393-396, 2000,
http://dx.doi.org/10.1136/ewjm.172.6.393,

[10] Reason, J.; Hollnagel, E. and Paries, J.: *Eurocontrol experimental centre. Revisiting the 'Swiss cheese' model of accidents. EEC Note No. 13/06 Project Safbuild.*
http://www.eurocontrol.int/sites/default/files/library/017_Swiss_Cheese_Model.pdf

[11] Shappell, S.A. and Wiegmann, D.A.: *The Human Factors Analysis and Classification System-HFACS*, 2000,

[12] Balaouras, S. and Cser, A.: *Navigate The Future Of Mobile Security.*
https://www.forrester.com/report/Navigate+The+Future+Of+Mobile+Security/-/E-RES137101, accessed 10th January 2020,

[13] Maxion, R.A. and Reeder, R.W.: *Improving user-interface dependability through mitigation of human error.*
International Journal of Human Computer Studies **63**(1-2), 25-50, 2005,
http://dx.doi.org/10.1016/j.ijhcs.2005.04.009,

[14] Cybersecurity Ventures: *Wi-Fi And Mobile Devices Predicted To Account For 80 Percent Of IP Traffic By 2025*, 2017,
https://cybersecurityventures.com/mobile-security-report-2017 , accessed 10th January 2020,

[15] Check Point: *Mobile Cyberattacks Impact Every Business.*
2017,

[16] Business Advantage Group: *The State of Industrial Cybersecurity.*
2017,

[17] Vanson Bourne: *The CyberArk Global Advanced Threat Landscape Report.*
http://dx.doi.org/10.1016/S1361-3723(18)30050-2,

[18] Shappell, S.A. and Wiegmann, D.A.: *A Human Error Approach to Accident Investigation: The Taxonomy of Unsafe Operation.*
The International Journal of Aviation Psychology **7**(4), 269-291, 1997,
http://dx.doi.org/10.1207/s15327108ijap0704_2,

[19] Norman, D.A.: *The Design of Everyday Things.*
http://faculty.smu.edu/rmason/NormanPOET.html 7/16/2012 , accessed 10th January 2020,

[20] Mhetre, R.S. and Dhake, R.J.: *Using Failure Mode Effect Analysis in a Precision Sheet Metal Parts Manufacturing Company.*
International Journal of Applied Sciences and Engineering Research **1**(2), 302-311, 2012,
http://dx.doi.org/10.6088/ijaser.0020101031,

[21] Johnson, K.G. and Khan, M.K.: *A study into the use of the process failure mode and effects analysis (PFMEA) in the automotive industry in the UK.*
Journal of Materials Processing Technology **139**(1-3), 348-356, 2003,
http://dx.doi.org/10.1016/S0924-0136(03)00542-9,

[22] Mikulak, R.J.; McDermott, R. and Beauregard, M.: *The basics of FMEA. 2nd ed.*
CRC Press, 2011,
http://dx.doi.org/10.1017/CBO9781107415324.004,

[23] Stamatis, D.H.: *Failure mode and effect analysis : FMEA from theory to execution. 2nd ed.*
ASQ Quality Press, 2003.

[24] Marques, L.M.C.: *FMEA-Mobile Phone.*
University of Ljubljana, Ljubljana, 2010,
http://lrss.fri.uni-lj.si/en/teaching/rzd/tutorials/marques2010_FMEA %20- %20Mobile %20Phone.pdf,

[25] Liu, W. and Li, H.: *Impact Analysis of a cellular phone.*
4th ANSA & μETA International Conference, 2011,

[26] Cinque, M. et al.: *How Do Mobile Phones Fail? A Failure Data Analysis of Symbian OS Smart Phones.*
37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, 585-594, 2007, http://dx.doi.org/10.1109/DSN.2007.54,

[27] Vijayalakshmi, K.: *Analysis of Android OS Smart Phones Using Failure Mode and Effect Analysis.*
International Journal of Latest Trends in Engineering and Technology **4**(4), 11-18, 2014,

[28] Tech Times: *New Android Smartphones Found To Be Already Infected By Malware: Are You At Risk?*
http://www.techtimes.com/articles/201326/20170312/new-android-smartphones-found-to-be-already-infected-by-malware-are-you-at-risk.htm, accessed 10th January 2020,

[29] Osborn, A.F.: *Applied imagination : principles and procedures of creative problem-solving.* 3rd rev. ed.
Charles Scribner's Sons, 1979,

[30] Ványi, G. and Pokorádi, L.: *Sensitivity analysis of FMEA as possible ranking method in risk prioritization*.
UPB Scientific Bulletin, Series D: Mechanical Engineering **80**, 165-176, 2018,

[31] Holicza, P. and Kadëna, E.: *Smart and Secure? Millennials on Mobile Devices.*
Interdisciplinary Description of Complex Systems **16**(3-A), 376-383, 2018, http://dx.doi.org/10.7906/indecs.16.3.10.