FAILURE MODES AND EFFECTS ANALYSIS – FMEA

NELI A. ARABADZHIEVA – KALCHEVA, TSVETOSLAV S. TSANKOV

ABSTRACT: *Failure Modes and Effects Analysis (FMEA) is a method of finding a mechanism for detecting failures, the causes of failures, ways to prevent failures and / or mitigate their effects on the system, and the likely consequences of these failures.*

The example presented in the report demonstrates the application of Analysis of the types of failures and their consequences in a particular case of "Failure of a computer network in a company". Possible risks, selected by experts, are presented in a systematic way in tabular form. Based on the results of applied quantitative assessments, measures for overcoming the risk and application of methods for risk prevention have been identified.

KEYWORDS: *Failure Modes and Effects Analysis, FMEA, risk management, risk assessment, risk analysis, risk assessment methods.*

DOI: https://doi.org/10.46687/MT22NEL

АНАЛИЗ НА ВИДОВЕТЕ ОТКАЗИ И ПОСЛЕДСТВИЯТА ОТ ТЯХ

НЕЛИ А. АРАБАДЖИЕВА – КАЛЧЕВА, ЦВЕТОСЛАВ С. ЦАНКОВ

АБСТРАКТ: *Анализ на видовете откази и последствията от тях (Failure Modes and Effects Analysis – FMEA) е метод за намиране на механизъм за откриването на отказите, причините причиняващи възникването им, начините за предотвратяване на отказите и/или смекчаване на въздействията им върху системата, както и вероятните последици от тези откази.*

Представеният в доклада пример демонстрира приложение на Анализ на видовете откази и последствията от тях при определен казус „Срив на компютърна мрежа във фирма“. Систематизирано в табличен вид са изложени възможни рискове, подбрани от експерти. Въз основа на резултати от приложени количествени оценки са набелязани мерки за преодоляване на риска и прилагане на методи за предотвратяване на риска.

1 Въведение

Управлението на риска е процес на идентифициране на опасностите, свързани с даден продукт или процес, оценка на свързаните рискове, контролиране на тези рискове и мониторинг. Оценяването на риск може да се извършва с различни методи, в зависимост от същността и сложността на проблема, както и от наличието на подходящи експерти. В Стандарт 31010 [1] е представено приложение на редица методи, с конкретни позовавания на други международни стандарти, в които концепцията и прилагането на методите са описани в по-големи потребности. Един от изложените методи е Анализ на видовете откази и последствията от тях (Failure Modes and Effects Analysis – FMEA).

2 Анализ на видовете откази и последствията от тях (Failure Modes and Effects Analysis – FMEA)

Анализ на видовете откази и последствията от тях (Failure Modes and Effects Analysis – FMEA) е един от първите методи за изследване на риска и е разработен около петдесетте години на миналия век, използван за разрешаване на проблеми възникнали във военни съоръжения. FMEA е методология, разработена за първи път за системни инженери, която

изследва потенциални повреди в продукти или процеси и която може да се използва за оценка на приоритетите за управление на риска за смекчаване на известни уязвимости на заплахите [2]. Прилагането на метода FMEA позволява да се открият потенциалните източници на грешки и техните последици върху качествените характеристики на системата възможно най-рано, с цел те да се минимизират [3]. Методът изисква много внимателно разглеждане на всички компоненти на една система с цел идентифициране на отказите и последствията от тях. Той може да се използва за оценка на риска както с качествена, така и с количествена оценка на оценяваната система, както на етап проектиране, така и на етап експлоатация. Методът е лесен за приложение, който може да се проведе от един експерт или от екип от експерти, които трябва много добре да познават анализираната система. Резултатите се обобщават в работни листове (карта за оценка на риска), съдържанието на които зависи от конкретния анализ.

В алгоритъма на този инструмент е от съществено значение да се разгледа важността на всеки риск чрез стойност на риска. Изчисляването на приоритета на потенциалния риск RPN (Risk Priority Number), което е полуколичествена мярка на критичността, се получава чрез умножение на числата от скалите на ранговете (обикновено между 1 и 10) за тежестта от отказа, вероятността за поява на отказа и възможността за разкриване на проблема (1).

$$RPN = S * O * D \quad (1)$$

Където S – тежест, O – вероятност за поява, D – вероятност за разкриване

Всеки отказ може да има различни последствия, различна вероятност за откриване и различно ниво на тежест. Въз основа на това се прави индивидуална оценка в зависимост от тежестта на съответния отказ (Таблица 1), от вероятността за поява на риска (Таблица 2) и вероятността за разкриване на риска (Таблица 3).

Таблица 1. Стойности за тежест (S)

Ефект	**Стойност**	**Критерии**
Няма ефект	1	Няма ефект.
Много малък	2-4	Грешка, която може да доведе до объркване, забавяне или леко увреждане на системата.
Среден	5-7	Грешка, която може да доведе до умерено увреждане на системата.
Висок	8-10	Грешка, която може да доведе до голямо увреждане на системата.

Таблица 2. Стойности за вероятност за поява (O)

Ефект	**Стойност**	**Критерии**
Почти никога	1	Инцидентът почти никога няма да се случи.
Малко вероятен	2-4	Малко вероятно е инцидентът да се случи.
Вероятен	5-7	Инцидентът е вероятно да се случи.
Много вероятен	8-10	Много голяма е вероятността инцидентът да се случи.

Таблица 3. Стойности за вероятността за разкриване (D)

Ефект	**Стойност**	**Критерии**
Сигурен	1	Сигурно е, че вероятността да се случи инцидент ще бъде разкрита.
Умерен	2-4	Умерена вероятност да се разкрие инцидента.
Малък	5-7	Ниска вероятност да се разкрие инцидента.
Незначителен или почти никакъв	8-10	Надеждността да се разкрие вероятността даден инцидент да се случи е недоказана или не се знае. Липсват всякакви методи за разкриване на вероятността даден инцидент да се случи и дори няма планове за това.

Класифицирането на риска се извършва в степени (Таблица 4).
Висок риск: RPN > 125. Тези рискове, оказват най-голямо влияние върху качеството и заради тях се прави изследване чрез планиран експеримент.
Среден риск: 42 ≥ RPN ≥ 125. Тези рискове оказват влияние върху качеството на системата.
Нисък риск: RPN < 42. Тези рискове не оказват съществено влияние върху системата, някои заради малко влияние, други заради лесна откриваемост.

Таблица 4. Ниво на риска

Ниво на риска	**Стойност на изчисления риск**	**Категория, наименование**	**Възможни действия**
I	RPN < 42	Нисък риск Допустим риск, под нивото на приемливия риск	Допуска се да не се предприемат действия.
II	42 ≥ RPN ≥ 125	Среден риск Ниво на приемливия риск	Допуска се да не се предприемат действия. Препоръчително се предприема наблюдение и/или въздействие
III	RPN > 125	Висок риск Ниво над приемливия риск	Задължително се предприема наблюдение и въздействие

Въз основа на данните от четирите таблици: Таблица 1, Таблица 2, Таблица 3 и Таблица 4 се попълва карта за оценка на риска (Таблица 5) от специалист или специалисти, експерти в съответната област. В тази карта се описват очакваните рискове (колона 2), задават се стойности на S, O и D (колони 3, 4 и 5) въз основа на критериите описани в съответните таблици. В колона 6 се нанася стойността на RPN, получена чрез формула (1). В колона 7 се вписва нивото на риска в зависимост от получената стойност на RPN и въз основа Таблица 4.

Таблица 5. Карта за оценка на риска

Задача:													
Изготвил:													
№	**Описание на риска**	**S**	**O**	**D**	**RPN**	**Ниво на риска**	**Методи за недопускане/ предотвратяван на риска (отстраняване на причина)**	**Мерки за преодоляване на риска (отстранява-не на следствие)**	**Sн**	**Oн**	**Dн**	**RPNн**	**Ниво на риска**
1.	**2.**	**3.**	**4.**	**5.**	**6.**	**7.**	**8.**	**9.**	**10.**	**11.**	**12.**	**13.**	**14.**
1													
2													
…													

След анализиране на всяка стойност на RPN в таблица 5, в колона 8 се описват мерките за недопускане на риска или мерките за предотвратяване, или намаляване на риска от възникване на отказ, т.е. стремежът е да се отстрани причината за възникване на отказ. В колона 9 се записват мерките за преодоляване на риска, т.е. това са мерките свързани с отстраняването на следствието от отказа. В колони 10, 11 и 12 се задават нови стойности на

S, O и D именувани Sн, т.е. S ново, Oн, т.е. O ново и Dн, т.е. D ново, въз основа на предвидените мерки описани в колони 8 и 9. В колона 13 се изчислява приоритета на риска на RPN след предприетите действия – RPNн, т.е. RPN ново. След сравняване на първоначалните стойности на RPN от колона 6 и крайните стойности на RPN, т.е. RPNн от колона 13, може да се заключи за ефективността на избраната стратегия. В последната колона се вписват новите нива на риск. Анализът на картата разкрива критичните числа (т.е. високите нива на риск), в резултат на което е необходимо да се избягват критичните събития и се вземат мерки за предотвратяване и преодоляване на риска.

Анализ на видовете откази и последствията от тях (Failure Modes and Effects Analysis – FMEA) е приложен в конкретен казус: „Срив на компютърна мрежа във фирма. След създаване на нова инфраструктура на IT системите, мрежата се е сринала 5 пъти, вследствие на което инфраструктурата се е реорганизирала 2 пъти.“

Таблица 6. Карта за оценка на риска на конкретен казус „Срив на компютърна мрежа във фирма“

Задача: След създаване на нова инфраструктура на IT системите, мрежата се е сринала 5 пъти, вследствие на което инфраструктурата се е реорганизирала 2 пъти. Да се изготви оценка на риск чрез метода Анализ на видовете откази и последствията от тях (Failure Modes and Effects Analysis – FMEA). Изчисляване на приоритета на риска преди и след предприети действия – RPN и RPNн (RPN ново)													
Изготвил:													
№	**Описание на риска**	**S**	**O**	**D**	**RPN**	**Ниво на риска**	**Методи за недопускане/ предотвратяване на риска (отстраняване на причина)**	**Мерки за преодоляване на риска (отстраняване на следствие)**	**Sн**	**Oн**	**Dн**	**RPNн**	**Ниво на риска**
1.	**2.**	**3.**	**4.**	**5.**	**6.**	**7.**	**8.**	**9.**	**10.**	**11.**	**12.**	**13.**	**14.**
1	Срив на мрежата	10	7	3	210	III	Диагностика на мрежата	Установяване на връзка с мрежов доставчик	10	6	2	120	II
2	Отпадане на компютър от мрежа	7	3	3	63	II	Диагностика на мрежата	Добавяне на компютър в мрежата	7	2	1	14	I
3	Възникване на грешки при диагностика	7	9	9	567	III	Връзка със специалист занимаващ се с диагностика	Използване на по-надеждни и бързи програми за диагностика	7	4	4	112	II
4	Загуба на информация	8	4	6	192	III	Използване на криптиран канал	Повторно изпращане на информация	8	3	5	120	II
5	Неясен хардуерен проблем	8	6	8	384	III	Необходима диагностика	Разрешаване на проблем от специалист	8	4	4	128	III

Анализът на картата за оценка на риска на конкретния казус (Таблица 6) показва, че след прилагане на мерки за преодоляване на риска и прилагане на методи за недопускане и предотвратяване на риска четири от възможни пет риска са намалили нивата си. В последната колона, се забелязва, че е останал само един риск (Неясен хардуерен проблем) от висока степен, със стойност по-голяма от 125. Резултатите показват, че е ефективна избраната стратегия.

3 Заключение

Анализ на видовете откази и последствията от тях (Failure Modes and Effects Analysis – FMEA) е метод за намиране на механизъм за откриването на отказите, причините причиняващи възникването им, начините за предотвратяване на отказите и/или смекчаване на въздействията им върху системата, както и вероятните последици от тези откази.

Представеният в доклада пример демонстрира приложение на Анализ на видовете откази и последствията от тях (Failure Modes and Effects Analysis – FMEA). На определените от IT експерти рискове е приложена количествена оценка. Систематизирано в табличен вид са набелязани мерки за преодоляване на риска и методи за недопускане и предотвратяване на риска, които нагледно представят ефективността на метода.

ЛИТЕРАТУРА:

[1] Международна организация по стандартизация, БДС EN ISO 31000:2011 Управление на риска. Принципи и указания., 2011, София, БИС

[2] Reddy V, Vijayakumar Gangadharappa H V, Shashikanth D Risk assessment by using failure mode effective analysis(FMEA) tool: an overview. World J Pharm Res 4(3): 567–574, (2015)

[3] Carlson, C., Understanding and Applying the Fundamentals of FMEAs. Tucson (Arizona): 2014 Annual RELIABILITY and MAINTAINABILITY Symposium, (2014)