

Осигуряване на качеството на сигналноохранителна и пожароизвестителна техника

Теодор Петков ¹⁾, Георги Дюкенджиев ²⁾

¹⁾ ТУ- София, МФ, катедра "Прецизна техника и уредостроене",
София 1000, бул."Кл. Охридски"8, totmana@abv.bg

²⁾ ТУ- София, МФ, катедра "Прецизна техника и уредостроене",
София 1000, бул."Кл. Охридски"8, duken@tu-sofia.bg

Резюме: Основен фактор за качеството е изследването на потенциалния риск при производство и експлоатация на техническите системи и техните модули, което е включва нормативна база, методология и представа.

В работата е извършен обзор на европейските норми – директиви и хармонизирани стандарти за сигналноохранителна и пожароизвестителна техника, които включват изисквания и тестови процедури към елементите и системите. Разгледана е методика за управление на риска – установяване на обстоятелства, определяне на критерии за риск, идентификация и оценяване на риска, анализ и преценяване на риска, въздействие върху риска, наблюдение и преглед.

Ключови думи: сигналноохранителна техника, пожароизвестителна техника, анализ на риска.

1. Нормативна база

Европейските норми за сигналноохранителна техника въвеждат строги изисквания и тестови процедури на елементите в една сигналноохранителна система. С цел да се гарантира високо качество на произвежданите в Европа електронни охранителни системи Европейският комитет по стандартизация в електротехниката (CENELEC) въвежда редица стандарти, които заедно със съществуващи национални стандарти се прилагат в областта. Стандартите въвеждат ясна категоризация на видовете охранителни средства, в зависимост от степента на опасност в съответната зона и методите за тяхното тестване.

При производство и експлоатация на сигналноохранителни системи и техните модули, те трябва да отговарят на изискванията на следните нормативни документи:

89/106/ЕЕС – Директива на съвета от 21 декември 1988 година относно законовите, подзаконовите и административни разпоредби на държавите членки по отношение на строителните продукти.

1999/5/ЕС – Директива на Европейския парламент и на Съвета от 9 март 1999 година

относно радионавигационното оборудване и далекосъобщително крайно оборудване и взаимното признаване на тяхното съответствие.

2004/108/ЕС – Директива на Европейския парламент и на Съвета от 15 декември 2004 година относно електромагнитната съвместимост.

2006/95/ЕС – Директива на Европейския парламент и на Съвета от 12 декември 2006 година за сближаване на законодателствата на държавите членки относно електрически съоръжения, предназначени за използване при някои ограничения на напрежението.

EN 50130 - 4: 2000/A1: 2000+A2 - Алармени системи. Част4: Електромагнитна съвместимост. Стандарт за група изделия: Изисквания за устойчивост на съставни части на пожароизвестителни системи, алармени системи срещу проникване и социални алармени системи [2006]

EN 50131-1 – Алармени системи. Системи против проникване и нападение. Част1: Изисквания към системите [2006]

EN 50131-1:2006/A1 – Алармени системи. Системи против проникване и нападение. Част1: Изисквания към системите [2009]

EN 55022 – Устройства за обработка на информацията. Характеристики на радиочестотно смущаващо въздействие.

Гранични стойности и методи за измерване (CISPR 22:2005, с промени) [2006]

EN 55022:2006/A1 – Устройства за обработка на информацията. Характеристики на радиочестотно смущаващо въздействие. Гранични стойности и методи за измерване (CISPR 22:2005, с промени) [2007]

EN 60950 - 1 - Устройства/съоръжения за информационни технологии. Безопасност. Част1: Общи изисквания. (IEC 60950-1:2001, с промени) [2001]

EN 60950 - 1:2006/A1 – Устройства/съоръжения за информационни технологии. Безопасност. Част1: Общи изисквания. (IEC 60950-1:2005/A1:2009) [2010]

EN 60950 - 1:2006/A11:2009+A12 – Устройства/съоръжения за информационни технологии. Безопасност. Част1: Общи изисквания [2011]

EN 61000-3-2 – Електромагнитна съвместимост (EMC). Част 3-2: Гранични стойности. Гранични стойности за излъчвания на хармонични съставлящи на тока (входен ток на устройства/съоръжения до и включително 16A за фаза) (IEC 61000-3-3:2005) [2006]

EN 61000-3-3 – Електромагнитна съвместимост (EMC). Част 3-3: Гранични стойности. Определяне на граничните стойности на измененията на напрежението, флукуациите на напрежението и фликера в обществени мрежи ниско напрежение за устройства с входен ток 16A за фаза, които не подлежат на условно свързване (IEC 61000-3-3:2008) [2008]

EN 54-5 – Пожароизвестителни системи. Част5: Топлинни пожароизвестители. Пожароизвестители точков тип.

EN 54-7 – Пожароизвестителни системи. Част7: Димни пожароизвестители. Пожароизвестители точков тип, използващи разсеяна светлина, пропускана светлина или йонизация [2001]

EN 54-7:2000/A1 – Пожароизвестителни системи. Част7: Димни пожароизвестители. Пожароизвестители точков тип, използващи разсеяна светлина, пропускана светлина или йонизация [2002]

EN 300 220-3 V1.1.1 – Електромагнитна съвместимост и въпроси на радиоспектъра (ERM). Радиосъоръжения с малък обseg на действие. Радиосъоръжения за използване в честотния обхват от 25 Mhz до 1000 Mhz обхващаи нива на изходна мощност до 500 mW. Част3: Хармонизиран стандарт от Директивата за радиосъоръжения и крайни далекосъобщителни устройства (R&TTED) [2002]

EN 301 489-3 V1.2.1 - Електромагнитна съвместимост и въпроси на радиоспектъра (ERM). Стандарт за електромагнитна съвместимост (EMC) на радио съоръжения и служби. Част3: Специфични условия за устройства с малък обseg на действие (SRD), работещи на честоти между 9 Khz и 40 Ghz.[2002]

2. Изисквания и тестови процедури

С цел да се гарантира високо качество на произвежданите в Европа електронни охранителни системи, преди няколко години Европейският комитет по стандартизация в електротехниката (CENELEC) въведе стандарта EN 50131. Очаква се EN 50131 постепенно да замени съществуващите национални стандарти в Европа и да се прилага в европейските държави, в които понастоящем няма утвърден стандарт в областта. Стандартът въвежда ясна категоризация на видовете охранителни средства, в зависимост от степента на опасност в съответната зона и методите за тяхното тестване. EN 50131 въвежда изисквания и тестови процедури за елементите в една сигнално-охранителна система.

Тестове за устойчивост на външни влияния.

EN 50131 дефинира различията в изискванията към всеки сензор в една система за сигнално-охранителна техника и специфицира съответните методи за изпитване. Една част от изпитанията засягат устойчивостта на външни влияния на различните средства за охрана и сигнализация и вероятността да подават фалшиви сигнали при определени условия.

Чрез серия от тестове се проверява устойчивостта им на въздушен поток, радиация от инфрачервени източници и микровълнови смущения, предизвикани от луминесцентни осветители.

При годните за сензори въздушният поток, преминаващ пред датчика, под никаква форма не предизвиква сигнал за тревога. Също така, излъчването на светлина в работния диапазон на инфрачервен сензор от близък светлинен източник, например автомобилните фарове или микровълнови сигнали от луминесцентни лампи, не трябва да бъде отчетено от детектора като евентуална опасност и да предизвиква сигнализация.

Симулирано проникване в помещение.

Отделен тест включва серия критерии, които следва да бъдат покрити от определен детектор, отнасящи се до скоростта на движение и позицията на нарушителя. Този тест е познат като „Симулиране на проникване в помещение“. За целите на теста се избира обект, висок между 160 и 185 см, с тегло 70 кг (± 10 кг) и облекло, което излъчва повече от 80% топлина от повърхността си с дължина на вълната между 8 и 14 микрометра. По време на теста се измерва разликата между температурата на обекта и температурата на въздуха в среда, през която той е преминал. Специфичното в измерването е, че се набляга върху измерването на определени зони от тялото на обекта и пространството, близо до тях – глава, гърди, длани, колене и стъпала, за да се постигне по-голяма точност в резултатите.

“Anti-masking” тестове на детектори

Стандартът описва подробно реакцията на годеи за детектор при опит да бъде “маскиран” от нарушителите, с цел да се повлияе на работата му. Познатите като “anti-masking” тестове проверят функционирането на сензори, които са били покрити с определен материал, спрей или са били дезактивирани по друг начин. При това положение, в рамките на 180 секунди от появата на дезактивиращ метод, сензорът трябва да изпрати “anti-masking” сигнал,

който да се излъчва постоянно през определен интервал до отстраняване на проблема. При провеждането на тестовете за покриване на лещата на сензора със спрей или лак се спазват определени условия, които се доближават максимално до подобни реални ситуации. Например пръскането трябва да е неравномерно и да продължава не повече от 2 секунди, а лакът да се нанася с един замах на четката. Сред материалите, използвани в “anti-masking” тестовете, са черна хартия, листов алуминий, акрил, самозалепващ се прозрачен винил, полиуретанов спрей и други, имащи достатъчно голям размер, за да възпрепятстват работата на сензора. Ако при два от три опита изпитваният детектор не успее да генерира алармен сигнал, то той не подлежи на сертификация по EN 50131.

Тестването - в независими лаборатории.

За да може стандартът да бъде утвърден във всички европейски държави и продуктите да са с гаранитрано качество, важно е те да бъдат изпитвани в независими лаборатории. Това означава, че цялата охранителна индустрия, от производителите и инсталаторите до крайните клиенти, би имала основание да се довери на качеството и функционалните характеристики на сертифицираните продукти. Поради тази причина много международно признати тестови лаборатории, като например CNPP във Франция, VDS в Германия и ANPI в Белгия, вече изпитват продукти за сигурност, според изискванията на EN 50131.

За момента, има разработени стандартизационни изисквания и тестови процедури за алармени системи (EN 50131-1), пасивни инфрачервени детектори (EN 50131-2-2), пасивни IR/микровълнови детектори (EN 50131-2-4), алармени панели (EN 50131-3), предупредителни устройства (EN 50131-4), безжични връзки за алармени системи (EN 50131-5-3) и захранвания (EN 50131-6). Комбинираните PIR/ултразвукови детектори (TS 50131-2-5) са в процес на подготовка да бъдат публикувани като EN - стандарти.

3. Анализ на риска.

Организациите, независимо от техния вид и големина са изправени пред вътрешни и външни фактори и влияния, които създават неувереност дали и кога ще постигнат своите цели. Влиянието на тази неопределеност по отношение на постигането на целите на дадена организация представлява т.нар. "риск".

Всички дейности на една организация съдържат рискове. Организациите управляват риска, като го идентифицират, анализират и след това се преценяват необходимостта от изменение чрез въздействие върху риска, за да се удовлетворят критериите за риск.

Обмен на информация и консултиране

Обменът на информация и консултирането с вътрешните и външни заинтересовани страни трябва да се осъществява на всички етапи от процеса на управление на риска. Планове на обмен на информация и консултиране трябва да се създават на ранен етап. Тези планове трябва да се разглеждат въпроси, отнасящи се до самия риск, до причините за риска, последствията (ако те са известни), и до взетите мерки за въздействието върху риска.

Установяване на обстоятелства

Външните обстоятелства са външната среда, в която организацията се стреми да постигне своите цели. Много е важно да се разбират външните обстоятелства, за да се гарантира, че целите и интересите на външните заинтересовани страни са взети предвид при създаването на критерии за риск. Външните обстоятелства се основават на обстоятелствата извън организацията, от изискванията на нормативните актове и на заинтересованите страни.

Вътрешните обстоятелства са вътрешната среда, в която организацията се стреми да постигне своите цели.

Установяване на обстоятелства, свързани с процеса на управление на риска

Обстоятелствата, свързани с процеса на управление на риска, се променят в зависимост от потребностите на

организацията. Те може да включват, без да се ограничават до:

- определянето на общите и конкретните цели за управление на риска;
- определянето на отговорности;
- определянето на степента и обема от предприемани дейности;
- определянето на взаимовръзките между проекти, процеси или дейности на организацията;
- определяне на методи за оценяване на риска;
- определянето на метода за оценяване на постиженията и ефикасността;
- идентифицирането и определянето на решения;
- идентифицирането на областта на приложение или организационната рамка за необходими изследвания, техния обхват и цели, както и необходимите ресурси за тяхното изпълнение.

Определяне на критерии за риск

Организацията трябва да определи критерии, позволяващи да се оцени значимостта на риска. Някои критерии може да бъдат наложени или да произтичат от задълженията за спазване на изискванията от нормативни актове или на други изисквания, които организацията е приела да спазва. Критериите за риск трябва да бъдат в съответствие с политиката за управление на риска на организацията, да бъдат определяни в началото на всеки процес на управление на риска и непрекъснато трябва да бъдат прегледвани.

Оценяване на риска

Оценяването на риска е цялостният процес на идентификация, анализ и преценяване на риска. ISO/IEC 31010 дава указания за методите за оценяване на риска.

Идентификация на риска

Организацията трябва да идентифицира източниците на риск, областите на въздействие, събитията (включително измененията на обстоятелствата), както и техните причини и потенциални последствия. Този етап има за цел да се състави изчерпателен списък на рискове, основани на тези събития, които могат да

провокират, подбудят, задържат, отстранят, ускорят или забавят постигането на целите. Важно е да се идентифицират рисковете, свързани не само с една възможност. Идентификацията трябва да включва рисковете, чиито източник е или не е под контрола на организацията, дори когато източникът или причината за риска може да не са очевидни. Идентификацията на риска трябва да включва проверка на влиянието от конкретни последствия, включително странични и натрупващи се влияния. Необходимо е също да се провери широк спектър от последствия, дори когато източникът или причината за риска може да не са очевидни. Трябва да бъдат проучени всички значителни причини и последствия. При идентифицирането на риска от съществено значение е използваната информация да бъде постоянно актуализирана. При идентифицирането на риска трябва да участва персоналят, който притежава съответните опит и познания.

Анализ на риска

Анализът на риска осигурява входни данни за преценяването на риска и за вземането на решения относно необходимостта от въздействие върху риска.

Анализът на риска включва отчитането на причините и източниците на риск, на техните положителни и отрицателни последствия и на възможността тези последствия да настъпят. Факторите, които влияят върху последствията и тяхната възможност, трябва да бъдат идентифицирани. Рискът се анализира чрез определяне на последствията и тяхната вероятност, както и чрез други характеристики на риска. Дадено събитие може да има многобройни последствия и да повлияе на няколко цели.

При анализа трябва да се отчита достоверността при определянето на нивото на риска и на неговата чувствителност спрямо предварителните условия и допускания и ефикасно да се съобщава на вземащите решения и при необходимост на другите заинтересовани страни. Трябва да бъдат определяни фактори като различие на

мнения между експертите, неопределеност, наличност, качество, количество и валидност на подходящата информация или гаранции на моделирането.

Анализът на риска може да бъде извършван на различни нива на подробност в зависимост от риска, целта на анализа и информацията, данните и наличните ресурси. Анализът може да бъде качествен, полукачествен, количествен или комбинация от трите в зависимост от обстоятелствата.

Последствията и тяхната възможност може да бъдат определени чрез моделиране на последиците от събитие или съвкупност от събития, или чрез екстраполация на експериментални проучвания или на налични данни.

Преценяване на риска

Преценяването на риска включва сравняване на нивото на риска, опеределено по време на процеса на анализ на риска с критериите за риск, разработени по време на установяването на обстоятелствата. На базата на това сравняване е възможно да се проучи необходимостта от въздействие върху риска.

Решенията трябва да отчитат разширените обстоятелства, свързани с риска, и да включват съображенията относно допустимостта на риска, създаден в страни, различни от организацията, които имат ползи от риска. Решенията трябва да се вземат, като се спазват изискванията на нормативните актове и други изисквания.

Въздействие върху риска

Въздействието върху риска може да включва избор и внедряване на една или повече възможности за изменение на риска. Веднъж внедрено, въздействието върху риска поражда или изменя средствата за управление на риска. Въздействието върху риска включва повтарящ се процес за:

- оценяване на въздействието върху риска;
- решение дали остатъчният риск е допустим;
- когато не е допустим - ново въздействие върху риска;
- оценяване на ефикасността.

Възможностите за въздействие върху риска не са непременно взаимно изключващи се или подходящи за всякакви обстоятелства. Тези възможности могат да включват:

- а) не се започва или продължава дейност, която поражда риск,
- б) премахване на източника на риск,
- в) изменение на възможността,
- г) изменение на последствията,
- д) споделяне на риска с други страни,
- е) поддържане на риска, основано на аргументиран избор.

Изборът на най-подходящата възможност за въздействие върху риска включва сравняване на разходите и усилията за внедряване по отношение на получените ползи, отчитайки задълженията, произтичащи от изискванията на нормативните актове и други изисквания като социална отговорност и опазване на околната среда.

Въздействието върху риска може също да породи вторични рискове, които трябва да бъдат разглеждани, оценявани, наблюдавани и преглеждани. Тези вторични рискове трябва да бъдат включени в същия план за въздействие върху риска както за първоначалния риск и не трябва да се разглеждат като нов риск. Връзката между двата риска трябва да бъде идентифицирана и поддържана.

Разработване и внедряване на планове за въздействие върху риска

Целта на планове за въздействие е върху риска е да се документира начина, по който избраните възможности за въздействие върху риска са внедрени. Информацията в плановете за въздействие върху риска включва причините, въздействието върху риска, очакваните ползи, персонала, ресурсите, мярката за успехите и ограниченията, изискванията за наблюдение и отчети, графика и последователността.

Планове за въздействие върху риска трябва да бъдат включени в процесите на управление на организацията и трябва да бъдат съгласувани със съответните заинтересовани страни.

Наблюдение и преглед

Наблюдението и прегледът трябва да бъдат планирани като част от процеса за управление на риска да включват контрол или редовно наблюдение. Този контрол или това наблюдение може да бъдат периодични или според конкретния случай. Отговорностите на организацията за наблюдението и прегледа трябва да бъдат ясно определени. Процесите за наблюдение и за преглед трябва да се прилагат за всички аспекти, свързани с процеса на управление на риска.

4. Заключение

На основата на изискванията в нормативната база и методологията за анализ на риска при осигуряване на качеството на сигналноохранителната и пожароизвестителната техника трябва да се прилагат превантивни методи като FMEA, FTA в комбинация с експериментално изследване на всички етапи от жизнения цикъл – проектиране, производство, експлоатация.

5. Литература

- [1] EN 50131-1 – Алармени системи. Системи против проникване и нападение. Част1: Изисквания към системите, 2006
- [2] ISO/IEC 31010 Управление на риска. Методи за оценяване на риска, 2009

Данни за авторите:

Теодор Лазаров Петков, маг.инж. специалност „Машиностроене и уредостроене“ (2009), ТУ - София, катедра ПТУ, МФ, докторант. Област на научни интереси – метрология и измервателна техника.

Георги Кирилов Дюкенджиев, машинен инженер, специалност “Механично уредостроене” (1981г.). Доктор (1994г.). Доцент (2000), , ръководител катедра “Прецизна техника и уредостроене”, ръководител на СОПКНИ в ТУ – София. Научни области - контролноизмервателна техника, метрология и управление на качеството.

Quality assurance of security and fire alarm equipment

Teodor Petkov ¹⁾, Georgi Dukendjiev ²⁾

¹⁾ TU - Sofia, MF, Department of Precision engineering, Sofia 1000, 8 St. Kl. Ohridsky blvd.,
totmana@abv.bg.

²⁾ TU - Sofia, MF, Department of Precision engineering, Sofia 1000, 8 St. Kl. Ohridsky blvd.,
duken@tu-sofia.bg.

Abstract: The main factor is the quality evaluation of potential risks in production and operation of technical systems and their modules, which include legislation, methodology and means. The work was carried out a review of European standards - Directives and harmonized standards security systems and fire alarm equipment, including requirements and test procedures for components and systems. Presented is the methodology for risk management - identifying circumstances determining the criteria for risk identification and risk assessment, analysis and evaluation of the risk impact on risk monitoring and review.

Key-Words: security systems, fire alarm, quality assurance, risk management