

Charakteristika falešných poplachů z hlediska příčin vyvolání a popis možných řešení (2)

Možnosti řešení falešných poplachů [1]

Možností řešení falešných poplachů existuje mnoho. Avšak ne každá možnost je sama o sobě účinná, a proto je vhodné užít kombinaci následujících možností pro odhalení, snížení či eliminaci falešných poplachů.

Ověřování

Ověřování je obecný název pro mnohé používané techniky, které umožní DPPC určit, zda se jedná o falešný poplach. Ověřování pomáhá bezpečnostním agenturám reagovat pouze na situace, kdy se jedná o skutečný poplach. Signály odesílané ze střežených objektů jsou vyhodnocovány v DPPC s cílem potvrdit nebo popřít detekovaný poplach.

Standardní ověřování

Standardní ověřování je metoda DPPC, pomocí níž ověřují (při odeslání poplachové zprávy), zda se jedná o falešný poplach. Standardní ověřování se provádí prostřednictvím telefonického hovoru, audio ověřování nebo jinými elektronickými metodami.

Rozšířené ověřování

Rozšířené ověřování je metoda DPPC, pomocí níž ověřují, že se v zabezpečených objektech neděje žádná mimořádná situace. Provádí se prostřednictvím důkladnějších postupů, jako je kombinace alespoň dvou metod, jako jsou ověření telefonickým hovorem na alespoň dvě čísla, živé audio ověřování a video ověřování, jiné prostředky nebo kombinace těchto postupů.

Metody ověřování

Metod ověřování falešných poplachů se v bezpečnostním průmyslu užívá mnoho. Ne každá metoda je však sama o sobě účinná a proto je vhodné užít kombinaci těchto metod pro spolehlivější ověřování.

Ověření voláním

Po odeslání poplachové zprávy na DPPC vyškolený operátor telefonicky kontaktuje uživatele PZTS, aby si ověřil, zda se nejedná o falešný poplach.

Neexistuje žádná záruka, že uživatel bude moci určit, zda se jedná o falešný poplach nebo střežený objekt napadl „šikovný zloděj“. Tato technologie je spolehlivá pro snižování falešných poplachů pouze v případě, že uživatel sám vygeneroval poplach a je si toho vědom.

Video ověřování

Po odeslání poplachové zprávy DPPC přepne na video spojení, které je ve střeženém objektu realizováno prostřednictvím kamery. Vyškolený operátor v DPPC určí na základě živého vysílání z kamery, zda se jedná o falešný poplach nebo o skutečné narušení střeženého objektu.

Tento typ ověřování je poměrně nákladný a neexistuje žádná záruka, že operátor spolehlivě určí příčinu vyhlášení poplachu.

Audio ověřování

Audio ověřování funguje na podobném principu jako video ověřování. Po obdržení poplachové zprávy se operátor spojí telefonicky se střeženým objektem a na základě zvuků v objektu určí, zda se

jedná o falešný poplach (ticho = falešný poplach, hlas = skutečný poplach).

Stejně jako u video ověřování, je tato metoda poměrně nákladná a neexistuje žádná záruka spolehlivého určení falešného poplachu.

Křížová detekce (Cross zoning)

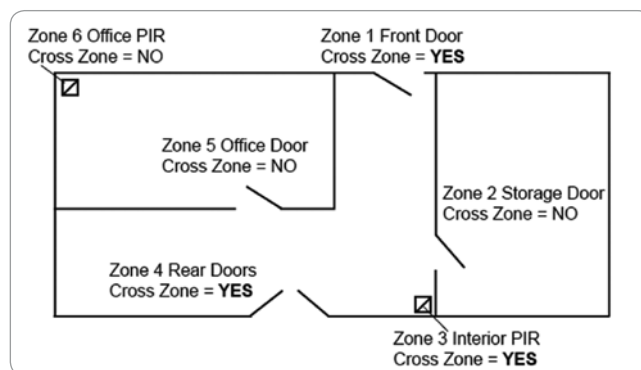
Tato metoda se považuje za jednu z neúčinnějších, co se týče eliminace falešných poplachů. Pokud je aplikována křížová detekce, poplachová zpráva se odešle na DPPC pouze tehdy, když jedna nebo více zón (detektorů) detekuje poplach během nadefinované doby.

Tato metoda umožňuje jakoukoli kombinaci bezpečnostních prvků. Například se může „křížit“ PIR detektor a s ním dva jiné PIR detektory, dveřní kontakt s mikrovlnným detektorem atd.

Nastavení křížové detekce se provádí při prvotním programování ústředny. Pro správnou funkčnost se při programování musí dbát na správné nastavení „swinger bypass“ (vyřazení zóny), včasnému varování na klávesnici a hlavně nastavení časového zpoždění mezi jednotlivými zónami (detektory) při narušení. Obvykle se zpoždění nastavuje mezi 1 až 250 sekundami.

Pokud je PZTS zastřežen a dojde k narušení (detekci) ve střežené oblasti, ústředna začne vydávat akustickou signalizaci (zvonění, siréna), že došlo k narušení zóny (detektoru) a začne odpočítávat naprogramovaný čas zadaný při instalaci (1 až 250s). Pokud během této doby nenastane další narušení (detekce), ústředna odešle chybnou zprávu o zóně (detektoru). Poplachová zpráva je odeslána na DPPC, pokud je během odpočítávání opakovaně narušena původní narušená zóna (detektor) nebo další zóny (detektory).

Níže je uveden obrázek pro typické použití křížové detekce.



Obr. 1 Schéma komerční budovy [5]

Ve schématu této malé komerční budovy (Obr. 1.) je uvedeno, že je zabezpečena pomocí dveřních kontaktů a PIR detektoru. Dveřní kontakty „Front door“, „Rear doors“ a pohybový detektor „Interior PIR“ jsou naprogramovány do „Křížové detekce“.

Pachatel po překonání „Front nebo Rear doors“ spustí akustický signál (siréna, zvonění). Ústředna začne odpočítávat naprogramovaný čas. Pokud jej do této doby detekuje „Interior PIR“, odešle se na DPPC poplachová zpráva, že byl objekt narušen.

Pokud dveřní kontakty způsobují falešné poplachy kvůli větru nebo problémy s elektroinstalací, ústředna spustí akustický signál (po naprogramovanou dobu) a na DPPC je odeslána pouze chybná zpráva. Obdobnou funkčnost má i PIR, pokud detekuje pohyblivost rostliny, hmyz atd.

Vstupní a výstupní zpoždění

Vstupní a výstupní zpoždění jsou funkce ústředny, které řeší problémy falešných poplachů při zastřežení a odstřežení PZTS.

Vstupní zpoždění znamená čas na odstřežení systému, než systém vyhlásí poplach (v případě, že je uživatel systémem detekován). Výstupní zpoždění znamená čas, který má uživatel na opuštění objektu po zastřežení. Pokud uživatel nestihne opustit objekt během doby zpoždění, systém vyhlásí poplach. Doba vstupního a výstupního zpoždění lze nastavit libovolně. Záleží na uživateli, kolik času potřebuje na opuštění objektu či odstřežení svého poplachového zabezpečovacího systému. Samozřejmě, že čas na zastřežení, či odstřežení nesmí být příliš dlouhý (maximálně 45 sekund), aby nedošlo k překonání systému pachatelem.

Vynechání zóny (Swinger zone bypassing)

Tato funkce umožňuje ústředně vynechat (ignorovat) zónu v případě, že daná zóna odešla během nadefinovaného časového období určitý počet falešných poplachů.

Pokud je naprogramována tato funkce, ústředna monitoruje, kolikrát daná zóna detekuje poplach a zároveň toto číslo (počet detekcí) porovnává s číslem, které naprogramoval technik při instalaci pro odpojení zóny. Když je tento počet dosažen, ústředna automaticky vynechá (ignoruje) zónu.

Vynechaná zóna se zpětně aktivuje resetem (klávesnicí či na dálku) nebo pokud nedetekuje falešné poplachy po dobu jedné hodiny.

Vynechání zóny je ideální používat v prostředích, kde je systém vystavován velkému působení okolních vlivů, což zapříčiňuje četné falešné poplachy.

Školení a vzdělávání

Rozhodující metodou jakéhokoli snížení falešných poplachů je školení a vzdělávání uživatelů PZTS už jen z toho důvodu, že většina falešných poplachů vzniká uživatelskou chybou (neznalost systému, zapomenuté heslo atd.). Právě školení a vzdělávání poskytuje uživateli a bezpečnostní agentuře pevný základ k zamezení falešných poplachů.

V zahraničí dokonce vznikají tzv.on-line kurzy, kde se uživatelé mohou seznámit s informacemi týkající se správného užívání PZTS a jak správně postupovat při signalizaci poplachu. Také bezpečnostní agentury, které se zabývají problematikou falešných poplachů, pořádají školení přístupné všem zájemcům.

Zařízení vhodné k odhalení, snížení či eliminaci falešných poplachů [1]

V dnešní době existují zařízení a softwarové programy, které nejenže dokáží falešný poplach odhalit, ale také pomocí moderních technologií eliminovat a tím zabránit odeslání falešné poplachové zprávy na DPPC.

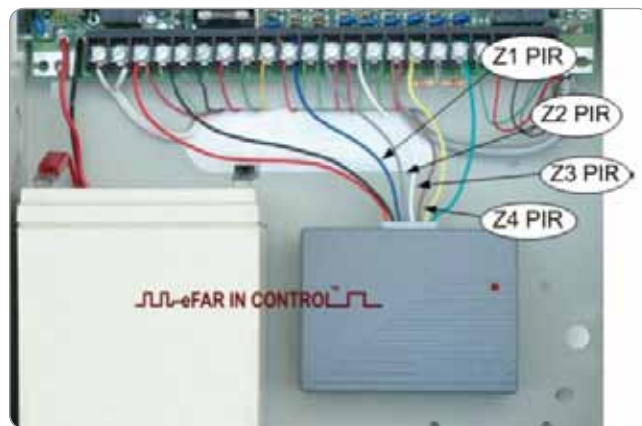
Detektory jsou již „chytřejší“ a mohou přesně vyhodnotit skutečné hrozby a minimalizovat falešné poplachy. Pracují na tzv. multikriteriálním zpracování signálu jako polarita, strmost, velikost signálu atd., které vyhodnocují mikroprocesory. Mikroprocesory následně rozhodnou na základě uložené databáze možných způsobů narušení, zda se jedná o falešný poplach či nikoliv.

eFAR 100

Modul eFAR100 je vyroben za účelem odhalení a následnému snížení nebo dokonce eliminování falešných poplachů, které pocházejí z detektorů pohybu. DPPC uvádí, že 25 až 30% falešných poplachů denně způsobí pohybové detektory. Po instalaci eFAR 100 došlo ke snížení falešných poplachů o více než 90%.

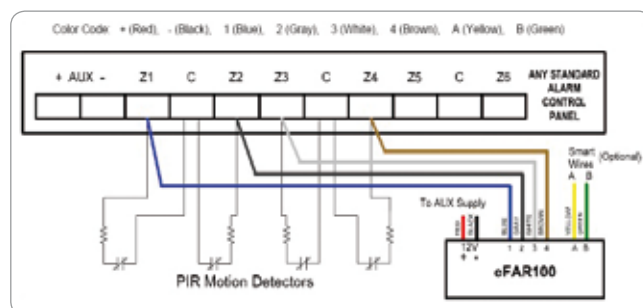
eFAR100 využívá DVC (Digital Verification Control) technologii pro snížení nebo zabránění falešných poplachů. Tato technologie vyhodnocuje poplašné signály PIR detektorů ve všech zónách pomocí funkcí Single, Multiple zone verification atd. Potlačuje

signály, které vyhodnotí jako falešný poplach a na ústřednu odešle pouze signály, které znamenají narušení střeženého objektu.



Obr. 2 Zapojení eFAR 100 [6]

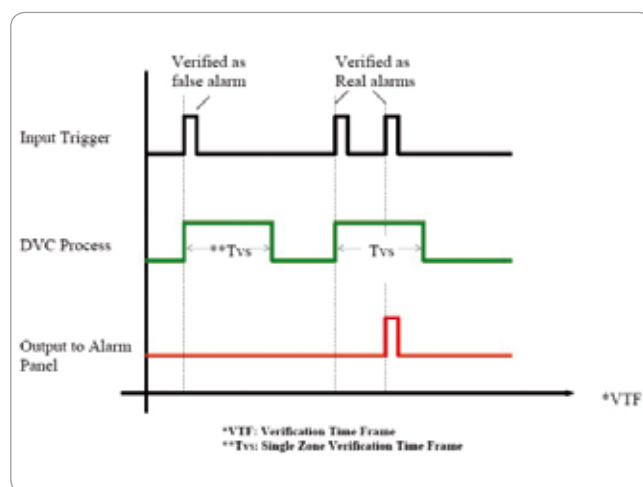
Modul dokáže pracovat až se čtyřmi PIR zónami. Nevyžaduje žádné programování. Automaticky rozpozná, o jaký typ smyčky se jedná (NC, EOL, EOLR, atd.)



Obr. 3 Schéma zapojení EOLR smyčky [6]

Single zone verification

Ústředna vyhlásí poplach pouze v případě, pokud v jedné zóně dojde k druhé detekci do 14,2 sekund nebo do 38,2 sekund (Tvs) od první detekce (čas si zvolí uživatel). Tvs je stanoven v těchto časech, protože pokud se jedná o skutečné napadení, PIR detektor detekuje narušitele dvakrát během několika sekund. Tento modul umožňuje i nastavení na 3 detekce do 42,6 sekund nebo do 114,6 sekund.

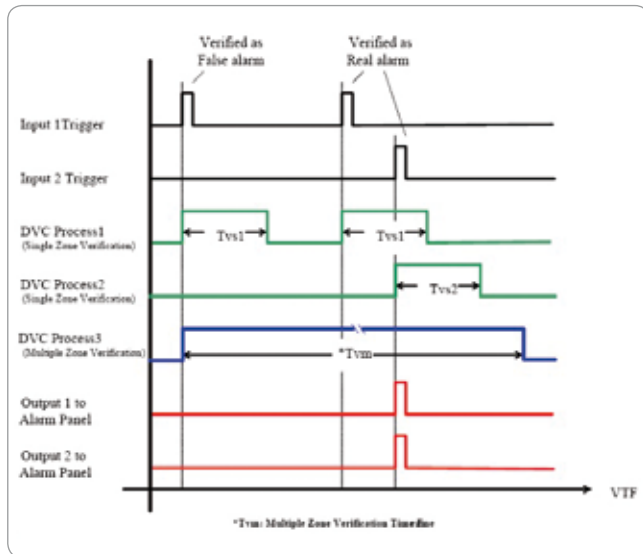


Obr. 4 Princip Single zone verification [7]

Když eFAR obdrží signál první detekce, začne danou zónu ověřovat. Pokud během Tvs neregistruje další detekci, modul tuto detekci vyhodnotí jako falešný poplach a ústředna poplach nevyhlásí. Pokud během Tvs nastane další detekce, eFAR ověří, že se jedná o skutečný poplach a ústředna jej vyhlásí.

Multiple zone verification

Ústředna vyhlásí poplach pouze v případě, pokud ve dvou a více různých zónách dojde k druhé detekci během 300 sekund (T_{vm}) od první detekce. Funkce single a multiple zone verification fungují na podobném principu jako křížová detekce.



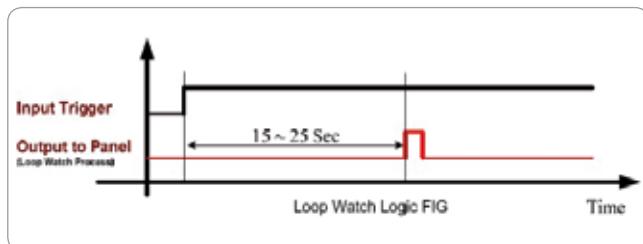
Obr. 5 Princip Multiple zone verification [7]

Když eFAR obdrží první detekci, spustí Single i Multiple zone ověřování. Pokud neobdrží další detekci v časovém rozmezí T_{vs} a T_{vm} , eFAR vyhodnotí poplach jako falešný a ústředna nevyhlásí poplach. Pokud od stejné zóny, v časovém rozmezí T_{vs} , přijme další detekci vyhodnotí jej jako poplach (viz Single zone verification). Ústředna vyhlásí poplach také v případě, že obdrží detekci z jiné zóny během časového rozmezí T_{vm} . Z tohoto důvodu musí být časové rozmezí T_{vm} delší než T_{vs} .

Loop watch function

V případě, že je zóna otevřena či zkratována a zůstane v tomto stavu, eFAR signály potlačí a ústředna nesignalizuje poplach. Zůstávali však zóna otevřená či zkratována delší dobu než 15 sekund, ústředna vyhlásí poplach.

Tato funkce je velice užitečná pro uživatele, kteří nechávají pootevřené dveře a okna. Rovněž je důležitá pro monitorování vadné instalace PIR detektorů (špatný kontakt).



Obr. 6 Princip Loop watch function [7]

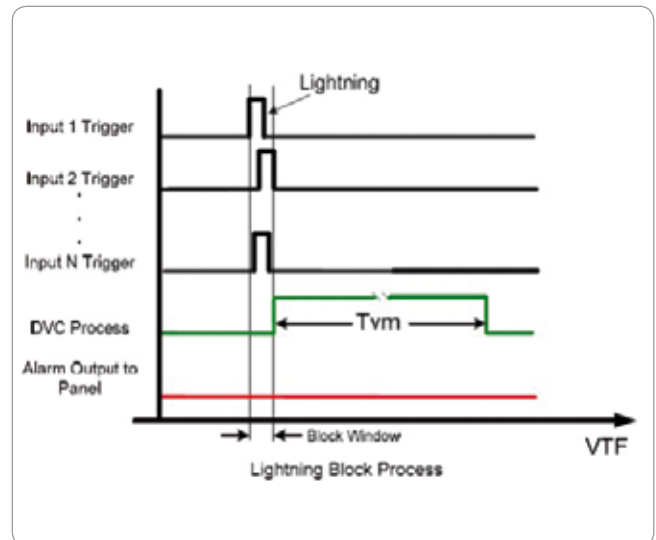
Lightning Block

eFAR100 má schopnost rozpoznat, zda byl (falešný) poplachový signál vytvořen vlivem blesku nebo jiného elektrického rušení. Modul vyhodnotí tento signál společně s ostatními funkcemi DVC. Porovná signál s ostatními funkcemi a podle toho rozhodne, zda se jedná o falešný poplach, či ohrožení objektu.

Silný blesk nebo radiofrekvenční rušení zasahuje většinou do funkce více než dvou zařízení, které jsou v časovém pásmu „Block window“ viz obr. 7.

Tato funkce vychází z úvahy, že je velice nepravděpodobné, aby narušitele detekovaly PIR v krátkém časovém intervalu na několika různých místech současně. Proto pokud eFAR obdrží

hlášení několika PIR detektorů v krátkém časovém rozmezí (Block window), jsou signály potlačeny a nedojde k vyhlášení poplachu.

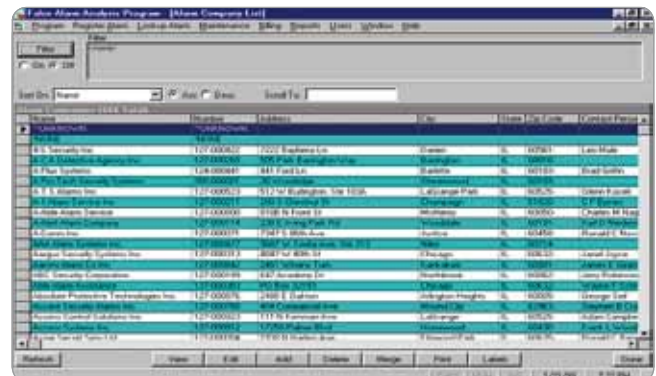


Obr. 7 Princip Lightning block [7]

FAAP (False alarm analysis program)

Jedná se o softwarový program, který byl vytvořen za účelem monitorování a evidování falešných poplachů. Především díky evidenci falešných poplachů má administrátor možnost upozornit zásahovou jednotku, že například za poslední hodinu v daném objektu došlo k deseti poplachům v určitých intervalech, což jsou s velkou pravděpodobností falešné poplachy a výjezd jednotky ke strážnému objektu není nutný.

Další využití je možnost sledování, zda dochází ke snižování falešných poplachů od roku instalace programu do současné nebo budoucí doby a zároveň identifikuje „problémové“ uživatele, jejichž systém je častým zdrojem odesílání falešných poplachů. Těmto uživatelům je následně poskytnuta pomoc v odstranění falešných poplachů.

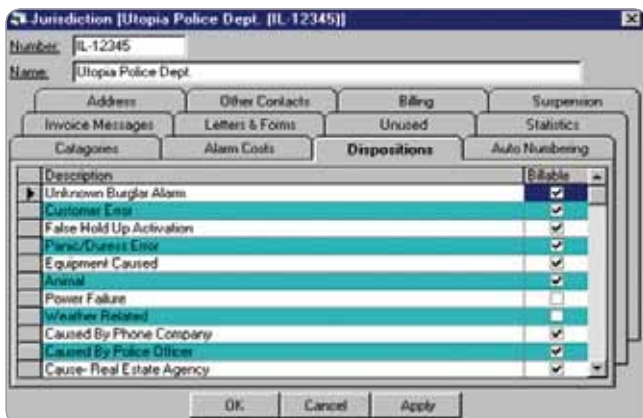


Obr. 8 FAAP [8]

Uživatel při registraci uvádí i název subjektu (police, bezpečnostní agentura), který v jeho objektu instaloval PZTS. To znamená, že program eviduje falešné poplachy jak uživatelům, tak subjektům, což udává jakousi prestiž, kvalitu a spolehlivost služeb subjektů (čím více falešných poplachů, tím klesá kvalita služeb).

Systém také vede evidenci příčin poplachů, na jejichž základě se rozhodne, zda bude poplach uživateli pokutován či nikoliv. Pokud poplach způsobí narušitel, počasí či chyba detektoru, sankce se zpravidla neúčtuje. Pokuty se udělují především za uživatelské chyby (tento program využívají převážně v Kanadě a Americe, kde jsou falešné poplachy uživatelům pokutovány).

Uživatel systému po zadání uživatelského jména a hesla má možnost zjistit, kolik falešných poplachů jeho systém vyhlásil, v jaký čas k poplachu došlo a částku, kterou dluží za vyhlášené falešné poplachy.



Obr. 9 Evidence příčin poplachu [8]

Literatura

- [1] CAHLÍK, Marek. Metodika zjišťování falešných poplachů s využitím moderních technologií. Zlín, 2009. bakalářská práce (Bc.). Univerzita Tomáše Bati ve Zlíně. Fakulta aplikované informatiky
- [2] UHLÁŘ, J. Technická ochrana objektů II. Díl – Elektrické zabezpečovací systémy. Praha : Policejní akademie ČR, 2001. ISBN 80-7251-076-2

- [3] ŠALANSKÝ, Dalibor, HÁJEK, Jan. DEHN: Tipy a triky – Jak uzemnit hromosvod [online]. c1998-2009 [cit. 2009-05-04]. Dostupný z WWW: <<http://elektrika.cz/data/clanky/dehn-tipy-a-triky-jak-uzemnit-hromosvod/view>>.
- [4] ČSN EN 50 131-7 DODATEK A
- [5] Understanding Cross Zoning [online]. 2007 [cit. 2009-05-04]. Dostupný z WWW: <http://www.guardianalarms.net/home_security_manuals/DMP/CROZONE.PDF>.
- [6] EFAR 100 - Installation Instruction [online]. 2006 [cit. 2009-05-04]. Dostupný z WWW: <<http://www.eefar.com/doc/DIG.pdf>>.
- [7] EFAR-Digital Verification Control (DVC) Technology [online]. 2006 [cit. 2009-05-04]. Dostupný z WWW: <<http://www.eefar.com/doc/DPD.pdf>>.
- [8] FAAP manual [online]. c2008 [cit. 2009-05-04]. Dostupný z WWW: <http://siacinc.org/faap_software.aspx>.

Ing. Marek Cahlík

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav bezpečnostního inženýrství
cahlik@fai.utb.cz