
# Simulace v bezpečnostní problematice inteligentních budov

**Simulace slouží obecně k poznávání simulovaného objektu, jeho vlastností a chování, čímž nám podává důležité informace jak didaktického charakteru, tak i pro podporu rozhodování. Před samotným aktem simulace je třeba vytvořit věrnou kopii objektu, již označujeme jako model. Ačkoliv jsou tvorba modelu a celkový proces simulace zpravidla časově i finančně náročné činnosti, v konečném důsledku pomáhá simulování zvýšit efektivnost a zpravidla i snížit náklady na simulovanou činnost. Díky jejich variabilitě simulátory - jak se říká objektům sloužícím k simulaci - nepopiratelně patří do tématiky nasazení bezpečnostních i jiných prvků v inteligentních budovách.**

Tento článek poukazuje na možný potenciál využití simulací při projektování bezpečnostních systémů a slouží k obecnému představení této problematiky.

## Základní pojmy

Model (Modus = lat. obraz) – zjednodušená (generalizovaná) reprezentace svého originálu. Kopíruje zejména pro simulaci důležité vlastnosti originálu.
Modelování – proces tvorby modelu. Zkoumání vlastností originálu a jejich aplikace na model.
Operátor – osoba řídící přípravu a vlastní průběh simulace.
Originál (Originalis = lat. původní) – původní předmět s plnou varietou vlastností. Výsledkem napodobení originálu je model.
PIR (z angl. Passive Infra-Red) – často nasazovaný prvek zabezpečení. Detekce narušitele je založena na vyhodnocení změny tepelného záření v chráněném prostoru.
Projektování zabezpečovacího systému – soubor činností projektanta vedoucí k vytvoření návrhu zabezpečovacího systému.
Prvky zabezpečovacího systému – všechna zařízení sloužící k zabránění penetrace objektu, případně její detekci a indikaci přítomnosti narušitele.
Simulace – proces, při kterém je vytvořeného modelu užito pro poznání originálu.
Subjekt – tvůrce/uživatel modelu či účastník simulace.
Trigger (z angl.) – událost vyvolaná předem definovanou podmínkou.
Zabezpečovací systém – množina systémů sloužící k zabránění penetrace objektu, případně její detekci a indikaci přítomnosti narušitele.

## Současná situace projektování bezpečnostních systémů

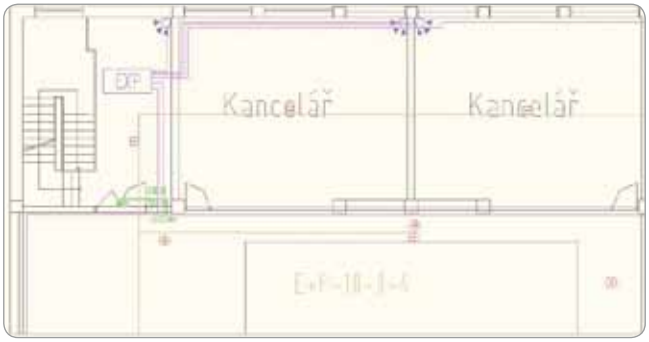
Standardem v projektování budov, zahrad a místností je vytvoření budoucího modelu, jenž umožňuje navrhnout možnosti, jež následně zákazník schvaluje. Výběrovým kritériem je v tomto případě především použitelnost (praktičnost), vzhled a samozřejmě finanční stránka.

Jako kontrast pak působí projektování bezpečnostních systémů, jakožto činnost notně podceňovaná. Jednou ze současných praxí (zejména u menších zakázek) je příchod bezpečnostního technika, který dle svého úsudku rozmístí zabezpečovací prvky, jejichž množství a kvalita závisí zejména na finančních možnostech zákazníka. Je pak na zvážení každého jedince, zda hodnotí druhou variantu - projektovou kancelářskou činnost - jako přístup s kvalitnějším výstupem. Tento často praktikovaný způsob naopak postrádá zhodnocení skutečné situace na místě, projektant má k dispozici pouze omezené informace o objektu.

V obou výše zmíněných případech je rozhodovací fázi zaměřené na rozmístění bezpečnostních prvků dáván pouze omezený prostor. Negativním výstupem této snahy tak mohou být nesprávná nasazení bezpečnostních prvků, které mohou snižovat jejich funkčnost a tím vést k nedostatečnému zabezpečení či častým falešným poplachům.

## Projektování bezpečnostních systémů z pohledu simulace

Z pohledu simulací lze na oba výše popsané přístupy k projektování bezpečnostních systémů pohlížet jako na jakýsi myšlenkový model, který vzniká v hlavě technika (projektanta), na jehož základě následně vytváří varianty, z nichž nakonec vybírá tu nejlepší [1]. Pakliže bychom však měli zhodnotit kvalitu simulačního procesu, k získanému výstupu byl užit ten nejprostší typ simulace, jehož výsledek může na stupnici kvality nabývat jak kladných, tak i záporných hodnot.




**Obr. Část příkladového bezpečnostního projektu**

Do vlastního procesu simulace v tomto případě vstupují veličiny jako schopnosti technika/projektanta, jeho aktuální rozpoložení, množství času, kterým disponuje a další, na první pohled místy až malicherné, přesto velmi podstatné, proměnné. Jelikož však proces zabezpečení objektu slouží k naprosto serióznímu účelu, jímž je návrh systému, jenž chrání život, zdraví a majetek vlastníka (zákazníka), nebylo by vhodné použít seriózní postupy, jimiž by se zkvalitnil vlastní proces projektování?

## Možnosti propojení procesu simulace a projektování

Jak již bylo v úvodu článku předesláno, jednou z přidaných hodnot procesu projektování za využití simulátorů je zkvalitnění rozhodovacího procesu a zvětšení šance, že zákazníkem vynaložené finance nevyjdou vniveč, leč budou správně zacíleny. Zejména seriózní firmy zabývající se bezpečnostním průmyslem by měly zvážit možné propojení svých činností s procesem simulace.

Vlastní implementace simulačního procesu však není jednoduchá, základním kamenem úrazu je neexistence kvalitního simulátoru, jehož vývoj by musel být zafinancován. V úvahu připadají jak 2D simulátory, tak i 3D simulátory.

## 2D simulátory

Představa o vhodném simulátoru může začít u jednoduchých 2D simulátorů, v nichž by zabezpečovací prvky měly vymezen detekční rádius a v závislosti na výběru typu prvku, vložením jeho parametrů získaných například z oficiální dokumentace a umístěním do půdorysu objektu by šlo jednoduše zabezpečit pokrytí vymezeného prostoru.

Na první pohled rozumná a finančně relativně nenáročná úvaha však skýtá řadu nevýhod. Jednou z nich je fakt, že charakteristika prvků ve 2D prostředí není pro účely projektování dostatečná. Plazící se narušitel nemusí být zabezpečovacím prvkem zachycen, stejně jako je možno případná nášlapná zařízení v podlaze jednoduše překročit, což je v podobném simulátoru jen těžko simulovatelné.

## 3D simulátory

Přejděme tedy k otázce 3D simulátorů. Ideálním typem simulátorů pro fázi projektování jsou virtuální simulátory, tedy simulátory virtuální reality, v nichž je možno testovat rozmístění bezpečnostních prvků ve virtuálním prostředí. [2]

Ačkoliv se vytvoření podobného simulátoru může zdát jako problém, v povědomí široké veřejnosti se jistě nachází spousta existujících adeptů, na nichž by se dalo stavět. Jedná se zejména o 3D akční hry, v nichž se již v základu často objevují velice kvalitní a v tomto směru velmi použitelné editory pro vlastní tvorbu a návrh. Mezi další „pro“ při využití těchto her je třeba zmínit i velice dobré grafické zpracování a zpravidla kvalitně vyladěné ovládání.

Důležitým faktorem pro úspěšnou simulaci a pro získání co nejhodnotnějších výsledků je vytvoření přesného modelu místnosti, potažmo celé budovy i s přilehlým okolím, se zaimplementováním všech důležitých vlastností objektů, zejména pak rozměrů místnosti, jejího půdorysu a vybavení, což již editory v dnešních herních simulátorech umožňují.

**Obr. Grafika současných herních simulátorů [3]**

Ideálním řešením při tvorbě vhodného simulátoru by tedy bylo vytvoření jakési nástavby na již existující simulátor (hru), investice do vývoje by tak nebyly natolik markantní. Vytvoření důležitých zabezpečovacích prvků pro potřeby simulace je pak především otázkou 3D modelování, přičemž zhotovení vhodného 3D modelu na zakázku je otázkou několika málo tisíc dolarů.

Podkladový simulátor by měl navíc pokud možno již v základu obsahovat funkci detekce pohybu, vizuální detekce a audio detekce.

## Detekce pohybu

Po funkční stránce nám na mysl ihned vyvstanou známé, již implementované prvky v podobě automatických střílen sloužících k detekci a zneškodnění nepřátel. Tyto by bylo možno pomocí relativně jednoduché úpravy změnit například v PIRy, na něž by byl nastaven pro případ detekce osoby trigger, kterým by byl spuštěn na místo obvyklé střelby poplach. Podobně jednoduchou úpravou by bylo možno nášlapné miny transformovat v nášlapné detektory, apod.

## Vizuální detekce

Rovněž oblast kamerových systémů je ve virtuální realitě velmi dobře zvládnuta. Prvky nejen že detekují pohyb a jsou schopny narušitele sledovat, obraz z kamery je navíc možno zobrazovat na virtuální obrazovce. V současnosti již, dovoluji si říci, vysoká umělá inteligence virtuálních osob zcela pokrývá otázku detekce narušitele náhodným kolemjdoucím či sousedem.

## Audio detekce

Detekce zvuků je dnes již naprosto standardní funkcí ve virtuální simulaci. Nepřítele můžete například přepadnout ze zálohy a odstranit jej metodou nablízko, pokud se však nechováte dostatečně tiše, tento si vás včas všimne a může reagovat. Narušitel tak může být detekován na základě jeho hlasitého projevu způsobeného ať už překonáváním mechanických zábranných prostředků, tak i neopatrným pohybem po objektu, apod.

## Simulační proces

Představme si situaci, kdy je již vytvořen funkční 3D simulátor s vlastnostmi, jaké byly popsány v předchozí kapitole a přejděme k simulačnímu procesu. Tento sestává ze tří hlavních částí, a to z přípravy simulace, vlastního pokusu o penetraci a zhodnocení simulace.

## Fáze přípravy

K vlastnímu procesu virtuální simulace směřuje přípravná fáze skládající se z definování objektu – tedy jeho topologie a počtu vstupů se zaměřením na atypické tvary místností, rozmístění předmětů, šířky stěn a dalších důležitých parametrů – a jeho následné vymodelování v editoru simulátoru operátorem.

Dalším krokem je strategické rozmístění prvků zabezpečení ve vymodelovaném objektu, což je činnost, kterou vykonává operátor (projektant) na základě vlastního zvážení a vlastních zkušeností. Ideální situací je vytvoření více variant alespoň dvěma projektanty, což by vedlo k možnosti jejich následného srovnání, přičemž varianty by se logicky lišily v rozmístění prvků, jejich typech a celkové ceně provedení každého návrhu.

Poslední krok přípravné fáze spočívá v přiřazení charakteristik v předchozím kroku vybraným prvkům. Důležité charakteristiky jsou například zorný úhel, vzdálenost snímání, pravděpodobnost detekce a další. Pro ideální volbu je vhodné pro vymodelovaný objekt vytvořit více variant zabezpečení.


**Obr. Simulační proces**

## Fáze simulace

Simulační proces řídí subjekt simulace. Ovládáním virtuální osoby v simulátoru se může opakovaně pokoušet o vstup do modelovaného objektu a prověřovat tak kvalitu rozmístění zabezpečovacích prvků. Výhodou virtuální simulace je možnost editace tohoto rozmístění i v samotném průběhu simulace, pakliže toto přijde operátorovi vhodné.

Při vlastní simulaci se navíc nemusíme omezit pouze na penetrační testy jednou osobou. Již v přípravné fázi je možno definovat počet osob, jež se budou o narušení objektu pokoušet. Každou z těchto osob pak může ovládat jiný subjekt simulace, přičemž subjekty mohou navzájem kooperovat, čímž se simulační proces ocitá na zcela jiné úrovni věrnosti napodobení reálné situace.

## Fáze vyhodnocení

Cílem zabezpečení objektu je minimalizace šance na vniknutí narušitele a v případě jeho vniku jeho včasná detekce. Hodnocenými parametry simulace z tohoto pohledu by tedy mohly být:

- Doba mezi započetím pokusů narušitele o vstup do objektu a úspěšným vstupem,
- doba mezi úspěšným vstupem narušitele do objektu a jeho detekcí,
- doba mezi zmocněním se věci narušitelem a jeho opuštěním objektu.

Nezanedbatelným parametrem hodnocení návrhu je cena navrhovaného řešení. V tomto kroku by tedy byla provedena kalkulace všech variant a následné srovnání. Po kvalitním prověření všech návrhů je možno jednoduše vybrat ten nejvhodnější, popřípadě udělat zákazníkovi nabídku s možnou prezentací kdy si tento, na základě vlastního rozhodnutí, zvolí lepší variantu.

## Další možnosti využití virtuálních simulátorů

Výše popsaný simulátor by nemusel být úzce zaměřen pouze na projektování bezpečnostních systémů, ale bylo by jím možné pokrýt celou řadu činností spojených s bezpečnostní problematikou objektů. Na následujících řádcích jsou uvedeny některé z možných aplikací.

Obdobou výše popsaného postupu simulace projektování by bylo možno testovat již existující zabezpečení. Účelem takovýchto testů by mohlo být kupříkladu potvrzení či vyvrácení podezření na nedostatečné zabezpečení objektu. Dosavadní nízké nároky pojišťoven na zabezpečení objektů mohou být v budoucnu zvýšeny, popsaný 3D virtuální simulátor by tak mohl být vhodným prostředkem pro testování, zda navrhované/stávající zabezpečení je dostatečné či nikoliv a to jak z pohledu zákazníka, tak z pohledu pojišťoven.

Zcela jiným účelem využití simulátoru by pak mohlo být testování plánů evakuace objektů a to jak při použití ozvučených evakuačních systémů, zhodnocení dostatečnosti kapacity únikových tras, tak i z pohledu značení evakuace a jejího řízení.

Přidáním některých nadstandardních funkcí by se rozrostly možnosti využití simulátoru. Obecně známým problémem výše zmíněného PIR je například citlivost na pohyb záclony či závěsu s vyšší teplotou než okolí, což bývá zpravidla způsobeno kontaktem s topením. I toto by mohl dostatečně kvalitní simulátor zohledňovat a například pomocí automatické funkce vyznačovat v průběhu přípravné fáze ta místa, pro něž umístění detektoru není vhodné. Editor simulátoru by tak pro PIR vyznačil jako nevhodná například místa naproti oken, místa s topením či klimatizací či nestandardní místa s častým pohybem větších zvířat, apod. Vhodná by byla i funkce automatického rozmístění zabezpečovacích prvků s přihlédnutím k předem definované míře pokrytí prostoru. Tato by mohla být závislá na určení priority prostor závislé například na ceně majetku, který obsahují a osobním preferencím zákazníka.

## Závěr

Ačkoliv v současnosti chybí použitelný simulátor pro účely projektování bezpečnostních systémů, díky existenci virtuálních simulátorů obsahujících kvalitní editory a zvládajících techniku detekce pohybu, vizuální detekce i audio detekce není jeho vývoj zcela nemožný a to ani po finanční stránce. Implementace procesu simulace do činnosti firem průmyslu komerční bezpečnosti by mohla vést k tvorbě úspornějších a efektivnějších variant návrhů a ke zvýšení prestiže firmy, jež by simulátor používala a výstupy prezentovala svým zákazníkům. Přidáním nadstandardních funkcí by se rozrostla paleta využití tohoto simulátoru, vznikl by tak multifunkční nástroj pokrývající řadu důležitých činností a usnadňující proces projektování.

Zřejmou překážkou ve vývoji popsaného simulátoru je finanční stránka, zřejmě neexistuje jediný subjekt, který by jej sám zafinancoval. Tento problém by tedy mohl být vyřešen například spolufinancováním projektu více společnostmi či získáním prostředků ze speciálních fondů, například z bezpečnostního výzkumu Ministerstva vnitra České republiky. Dalším krokem v oblasti analýzy možností vývoje simulátoru tedy bude prověření obou výše zmíněných variant financování.

## Zdroje

[1] RYBÁR, Mikuláš. Modelovanie a simulácia vo vojenstve. Bratislava: Vydavateľská a informačná agentúra, Ministerstvo obrany Slovenskej republiky, 2000, 402 s. ISBN 80-88842-34-4.

[2] PELÁNEK, Radek. Modelování a simulace komplexních systémů: jak lépe porozumět světu. Vyd. 1. Brno: Masarykova univerzita, 2011, 233 s. ISBN 978-80-210-5318-2.

[3] BOHEMIA INTERACTIVE STUDIO, screenshot z válečného simulátoru Arma2.

**Ing. Petr Svoboda**

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