

Univerzita Pardubice  
Fakulta ekonomicko-správní

**Návrh diskrétně událostního modelu**

Bc. Eva Kmoníčková

Diplomová práce

2011

Univerzita Pardubice  
Fakulta ekonomicko-správní  
Akademický rok: 2010/2011

## ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Bc. Eva KMONÍČKOVÁ**  
Osobní číslo: **E07539**  
Studijní program: **N6209 Systémové inženýrství a informatika**  
Studijní obor: **Regionální a informační management**  
Název tématu: **Návrh diskrétně událostního modelu**  
Zadávací katedra: **Ústav systémového inženýrství a informatiky**

### Z á s a d y p r o v y p r a c o v á n í :

Předpokládaným výstupem diplomové práce bude popis a definice diskrétně událostního modelu.

Vytvoření standartních příkladů diskrétně událostního modelu ve vybraném prostředí.

Návrh a analýza příkladu diskrétně událostního modelu z oblasti veřejné správy.

Rozsah grafických prací:

Rozsah pracovní zprávy:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

NOVÁK, Jiří, et al. **Základy informatiky: počítačové modelování v Matlabu**. 1. vyd. Praha : Česká technika - nakladatelství ČVUT, 2005. 170 s. ISBN 80-01-03308-2.

NOSKIEVIČ, Petr. **Modelování a identifikace systémů**. Ostrava : Montanex, 1999. 276 s. ISBN 80-7225-030-2.

ŠULC, Bohumil, VÍTEČKOVÁ, Miluše. **Teorie a praxe návrhu regulačních obvodů**. 1. vyd. Praha : Vydavatelství ČVUT, 2004. 333 s. ISBN 80-01-03007-5.

Vedoucí diplomové práce:

  
**doc. Ing. Jiří Křupka, Ph.D.**

Ústav systémového inženýrství a informatiky

Datum zadání diplomové práce:

**4. října 2010**

Termín odevzdání diplomové práce:

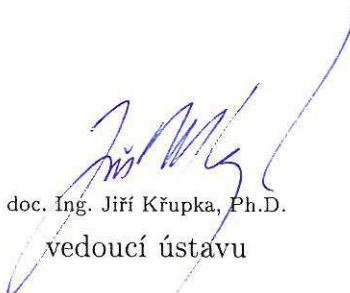
**6. května 2011**



doc. Ing. Renáta Myšková, Ph.D.

děkanka

L.S.

  
doc. Ing. Jiří Křupka, Ph.D.

vedoucí ústavu

V Pardubicích dne 4. října 2010

Prohlašuji:

Tuto práci jsem vypracovala samostatně. Veškeré literární prameny a informace, které jsem v práci využila, jsou uvedeny v seznamu použité literatury.

Byla jsem seznámena s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích dne 27. 6. 2011

Eva Kmoníčková

## **Poděkování:**

Děkuji vedoucímu své práce doc. Ing. Jiřímu Křupkovi, PhD. z Ústavu systémového inženýrství a informatiky, Fakulta ekonomicko-správní, Univerzita Pardubice za jeho odborné a věcné rady a přátelský přístup.

## **ANOTACE**

Diplomová práce popisuje prostředí tvorby diskrétně událostního modelu. Model klasifikace události, systému vyrozumění a varování na jaderné elektrárně je zpracován v prostředí programu MATLAB&Simulink. Tvorba modelu je realizována nástrojem pro tvorbu diskrétně událostních modelů Stateflow. Vytvořený model demonstruje přehledné použití hierarchických stavových automatů pro návrh chování diskrétně událostních modelů.

## **KLÍČOVÁ SLOVA**

Diskrétně událostní systém, modelování, simulace, Stateflow, Hierarchický stavový automat,

## **TITLE**

Building a Discrete-Event model

## **ANNOTATION**

This Thesis describes building interface of discrete-event modelling. Model of classification and notification and information system for nuclear power station is built in MATLAB&Simulink and its discrete-event modelling tool Stateflow. The created model demonstrates a clear use of statecharts for the design of discrete-event models.

## **KEYWORDS**

Discrete-event system, modeling, simulation, Stateflow, statechart

# Obsah

<b>ÚVOD .....</b>	<b>12</b>
<b>1 POPIS PROBLEMATIKY DISKRÉTNĚ UDÁLOSTNÍCH SYSTÉMŮ .....</b>	<b>14</b>
1.1 PŘÍKLADY UŽITÍ DISKRÉTNĚ UDÁLOSTNÍCH SYSTÉMŮ .....	17
1.1.1 <i>Systémy hromadné obsluhy</i> .....	17
1.1.2 <i>Počítačové systémy</i> .....	19
1.1.3 <i>Komunikační systémy</i> .....	19
1.1.4 <i>Výrobní systémy</i> .....	20
1.1.5 <i>Dopravní systémy</i> .....	21
1.2 FORMY POPISU DISKRÉTNÍCH SYSTÉMŮ .....	22
<b>2 STATEFLOW POPIS PROSTŘEDÍ.....</b>	<b>24</b>
2.1 HIERARCHICKÉ STAVOVÉ AUTOMATY.....	24
2.2 ZÁKLADNÍ PRVKY STATEFLOW.....	25
2.2.1 <i>Grafické objekty Stateflow</i> .....	26
2.2.2 <i>Negrafixké objekty Stateflow</i> .....	28
2.3 POSTUP TVORBY MODELU VE STATEFLOW.....	29
2.4 ALGORITMUS FUNGOVÁNÍ STATEFLOW .....	31
2.4.1 <i>Zpracování události</i> .....	31
2.4.2 <i>Vstup do stavu</i> .....	31
2.4.3 <i>Spuštění aktivního stavu</i> .....	31
2.4.4 <i>Opuštění aktivního stavu</i> .....	32
2.4.5 <i>Spuštění skupiny přechodů</i> .....	33
2.4.6 <i>Mechanismus okamžitého ukončení</i> .....	34
<b>3 MODEL ELEKTRONICKÉHO ZABEZPEČENÍ DOMU.....</b>	<b>36</b>
3.1 POPIS BLOKOVÉHO SCHÉMATU MODELU .....	37
3.1.1 <i>Subsystem HOLD</i> .....	38
3.1.2 <i>Stavový diagram Stateflow</i> .....	38
<b>4 MODEL ŘEŠENÍ MIMOŘÁDNÝCH UDÁLOSTÍ V JADERNÉ ELEKTRÁRNĚ .....</b>	<b>41</b>
4.1 POPIS KLASIFIKACE MIMOŘÁDNÉ UDÁLOSTI V JADERNÉ ELEKTRÁRNĚ.....	41
4.2 POPIS SYSTÉMU VYROZUMĚNÍ A VAROVÁNÍ.....	45

4.3	NÁVRH MODELU ŘEŠENÍ MIMOŘÁDNÝCH UDÁLOSTÍ V JADERNÉ ELEKTRÁRNĚ .....	49
4.3.1	<i>Stavový diagram Stateflow</i> .....	51
4.3.2	<i>Realizace modelu</i> .....	59
	<b>ZÁVĚR</b> .....	<b>62</b>
	<b>POUŽITÁ LITERATURA</b> .....	<b>64</b>
	<b>SEZNAM PŘÍLOH</b> .....	<b>I</b>



## Seznam obrázků

OBRÁZEK 1 – PRINCIP MODELOVÁNÍ A SIMULACE [3].....	15
OBRÁZEK 2 - DISKRÉTNĚ UDÁLOSTNÍ SYSTÉM [VLASTNÍ].....	16
OBRÁZEK 3 - STRUKTURA JEDNODUCHÉHO SHO [5].....	17
OBRÁZEK 4 - MODEL SHO POČÍTAČOVÉHO SYSTÉMU [5].....	19
OBRÁZEK 5 - MODEL PRO VÝROBNÍ SYSTÉM [5].....	20
OBRÁZEK 6 - KŘÍŽOVATKA SE SEMAFOREM – MODEL PRO DOPRAVNÍ SYSTÉM [5].....	21
OBRÁZEK 7 - STATEFLOW JAKO NÁSTROJ MATLABU [9].....	23
OBRÁZEK 8 – GRAFICKÉ ZNÁZORNĚNÍ PRVKŮ STATEFLOW [9].....	25
OBRÁZEK 9 - AKCE VE STAVECH A PŘECHODECH [11].....	27
OBRÁZEK 10 - ZÁKLADNÍ SCHÉMA TVORBY MODELU V PROSTŘEDÍ STATEFLOW [9].....	29
OBRÁZEK 11 – SKUPINY PŘECHODŮ [10].....	32
OBRÁZEK 12 - MECHANISMUS PŘEDČASNÉHO UKONČENÍ [10].....	34
OBRÁZEK 13 – MODEL ELEKTRONICKÉHO ZABEZPEČENÍ DOMU [VLASTNÍ].....	37
OBRÁZEK 14 - BLOK HOLD [VLASTNÍ].....	38
OBRÁZEK 15 - STATEFLOW MODEL - ELEKTRONICKÁ ZABEZPEČOVACÍ SIGNALIZACE [VLASTNÍ].....	39
OBRÁZEK 16 - SCHÉMA OCHRANNÝCH BARIÉR JADERNÉ ELEKTRÁRNY [14].....	42
OBRÁZEK 17 - SCHÉMA JADERNÉ ELEKTRÁRNY [14].....	44
OBRÁZEK 18 - PRINCIPIELNÍ SCHÉMA SYSTÉMU VYROZUMĚNÍ A VAROVÁNÍ [VLASTNÍ – INSPIROVÁNO [17]].....	48
OBRÁZEK 19 - MODEL ŘEŠENÍ MIMOŘÁDNÝCH UDÁLOSTÍ V JADERNÉ ELEKTRÁRNĚ [VLASTNÍ] .....	49
OBRÁZEK 20 – SUBSYSTÉM BLOKU I/O BOX [VLASTNÍ].....	51
OBRÁZEK 21 – STATEFLOW MODEL - SYSTÉM VYROZUMENÍ A VAROVÁNÍ [VLASTNÍ].....	52
OBRÁZEK 22 - STATEFLOW EXPLORER [VLASTNÍ].....	53
OBRÁZEK 23 - STAV_REAKTOR [VLASTNÍ].....	54
OBRÁZEK 24 - STAV ING [VLASTNÍ].....	55
OBRÁZEK 25 - STAV VYROZUMENÍ [VLASTNÍ].....	58
OBRÁZEK 26 - PORUCHA POTRUBÍ [VLASTNÍ].....	59
OBRÁZEK 27 - MIMOŘÁDNÁ UDÁLOST 3. STUPNĚ [VLASTNÍ].....	60

## **Seznam tabulek**

TABULKA 1 - KLASIFIKACE MIMOŘÁDNÝCH UDÁLOSTÍ [VLASTNÍ] .....	45
--	----

## Seznam zkratek

CPU	-	Procesor ( <i>Central Processing Unit</i> )
ČR	-	Česká republika
ČRo	-	Český rozhlas
ČT	-	Česká televize
DES	-	Diskrétně událostní systém ( <i>Discrete Event System</i> )
EZS	-	Elektronická zabezpečovací signalizace
GŘ HZS ČR	-	Generální ředitelství Hasičského záchranného sboru České republiky
HZS	-	Hasičský záchranný sbor
INES	-	Mezinárodní stupnice hodnocení závažnosti jaderných událostí ( <i>The International Nuclear Event Scale</i> )
IZS	-	Integrovaný záchranný systém
KŠ	-	Krizový štáb
KÚ	-	Krajský úřad
MAAE	-	Mezinárodní agentura pro atomovou energii
MU	-	Mimořádná událost
MV	-	Ministerstvo vnitra
OO	-	Objektové orientování ( <i>Object-Oriented</i> )
OPIS	-	Operační a informační středisko
ORP	-	Obec s rozšířenou působností
OÚ	-	Obecní úřad
SHO	-	Systémy hromadné obsluhy ( <i>Queueing System</i> )
SÚJB	-	Státní úřad pro jadernou bezpečnost
ZHP	-	Zóna havarijního plánování

## Úvod

Základním cílem této práce je navrhnout a analyzovat diskrétně událostní model z oblasti veřejné správy. Veřejná správa poskytuje širokou škálu témat vhodných pro tvorbu modelů diskrétních událostí. Volba oblasti byla inspirována aktuálními tématy dnešní doby, mezi která patří bezpečnost jaderných elektráren.

Téma jaderné energetiky je v poslední době velmi skloňováno ve všech médiích po celém světě a stále častěji i na vládní úrovni. Evropská unie chce do konce roku 2011 otestovat všechny jaderné elektrárny na území EU a postupně se k testování připojuje i řada států mimo EU. Přičemž například Francie přislíbila uzavřít elektrárny, které testem neprojdou. V německém parlamentu je ke schválení připraven zákon, který má ukončit provoz všech jaderných elektráren na území státu do roku 2022. Tento dlouhodobě nedůvěřivý pohled na jadernou energetiku eskalovala jaderná krize v Japonsku, kterou dne 11. 3. 2011 odstartovalo zemětřesení doprovázené vlnou tsunami.

V České republice jsou v provozu dvě jaderné elektrárny, jaderná elektrárna Dukovany, kde kontrola z Mezinárodní agentury pro atomovou energii konstatovala v červnu letošního roku vysoký standard bezpečnosti a jaderná elektrárna Temelín. Temelínská elektrárna má nyní v provozu dva jaderné bloky a do roku 2025 je plánovaná dostavba dalších dvou. Proti této plánované výstavbě se v pravidelných intervalech zvedá vlna protestů zejména v sousedních zemích. Česká vláda je ale pevně rozhodnuta elektrárnu rozšířit na čtyři původně projektované jaderné bloky. Češi jsou jedni z největších příznivců využívání jaderné energie ze všech obyvatel Evropské unie.

Ačkoli se odborníci na jadernou energetiku shodují v názoru na vysokou míru bezpečnosti českých jaderných elektráren, nehoda v japonské Fukušimě prokázala, že havarijní stav může nastat z nejrůznějších příčin. Právě proto je nezbytné, aby byla velmi obezřetně zajišťovaná havarijní připravenost vzniku mimořádné události na jaderné elektrárně.

Téma bezpečnosti jaderných elektráren je inspirací pro tuto práci, která si klade za cíl navrhnout a analyzovat příklad diskrétně událostního modelu z oblasti veřejné správy. Před samotnou tvorbou modelu je nezbytné důkladně analyzovat mimořádné události na české jaderné elektrárně z pohledu toku informací v případě vzniku nehody. Diskrétně událostní model by měl zaznamenat všechny orgány, které mají být o vzniku

nehody informovány, včetně posledního nejdůležitějšího článku, kterým jsou občané. Model klasifikace mimořádných událostí a následný systém vyrozumění a varování by měl být zpracován ve vybraném prostředí vhodném pro tvorbu diskrétně událostních systémů.

Práce by měla zahrnovat i stručné představení diskrétně událostních systémů včetně popisu prostředí jejich tvorby. Měl by zde být popsán a vypracován i standardní příklad diskrétně událostního modelu. Hlavním cílem této práce by měla být tvorba vlastního diskrétně událostního modelu z prostředí veřejné správy. Tento model by měl být vytvořen na základě reálných podkladů, které bude nutné nejprve podrobně analyzovat a popsat a následně zpracovat ve vybraném simulačním prostředí.

# 1 Popis problematiky diskrétně událostních systémů

Tvorba diskrétně událostního modelu je spojena s mnoha pojmy z oblasti modelování a simulace. Mezi tyto základní termíny patří pojmy systém, model, simulace a modelování a mnoho dalších termínů. Některé pro tuto práci podstatné pojmy jsou popsány, tak jak uvádí odborná literatura [1] [2] [3]:

- \* **Systém** je soubor elementárních částí, prvků systému, které mají mezi sebou určité vazby. Toto vzájemné propojení množiny prvků tvořící systém by mělo směřovat k dosažení cílového stavu.

- \* **Model** je napodobenina systému jiným systémem. Model rovná se reprezentace znalostí.

Modely se dle charakteru procesu dělí na deterministické, kdy v modelu nejsou zahrnuty náhodné veličiny a stochastické, u kterých se v modelu nachází alespoň jeden prvek s nedeterministickým chováním tedy mající náhodný charakter.

Modely lze dělit také dle způsobu zachycení časového faktoru na spojitě, diskrétní a kombinované. Spojité modely jsou takové, kde všechny prvky modelu mají spojitě chování. Modely diskrétního charakteru zahrnují pouze prvky s diskrétním chováním a u kombinovaných modelů se nacházejí prvky se spojitým i diskrétním chováním.

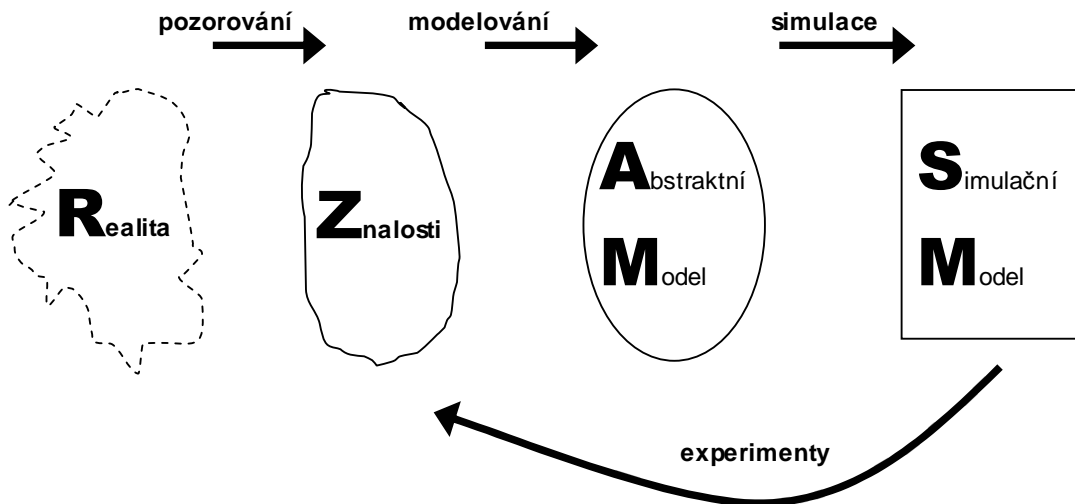
- \* **Modelování** je vytváření modelů systému, modelovat lze jen to co je známé a popsitelné. Podstatou modelování je náhrada zkoumaného systému jeho modelem, jejímž cílem je získat pomocí pokusů s modelem informaci o původním zkoumaném systému.

- \* **Simulace** je metoda získávání nových znalostí o systému experimentováním s jeho modelem.

**Shannon:** Simulace je proces tvorby modelu reálného systému a provádění experimentů s tímto modelem za účelem lepšího pochopení chování studovaného systému či za účelem posouzení různých variant činnosti systému.

- \* **Simulační model** je dynamický model, v němž dochází k výskytu jevů ve stejném pořadí jako v modelovaném systému.

- \* **Princip modelování a simulace** - cílem je získat nové znalosti o modelovaném systému. Obrázek 1 nastiňuje základní principy modelování a simulace, je zde znázorněno, jak se široká a často těžko uchopitelná realita přemění v simulační model.

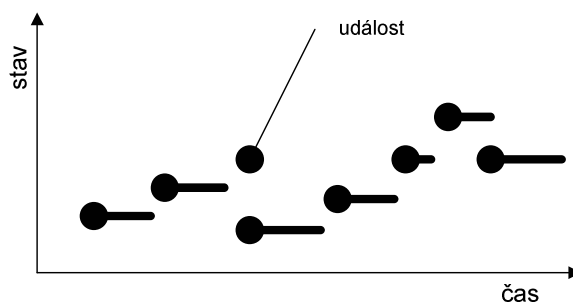


Obrázek 1 – Princip modelování a simulace [3]

- \* **Čtyři základní etapy modelování a simulace [3]:**
  1. **Vytvoření abstraktního modelu.** Během první fáze modelování a simulace dochází k formulaci zjednodušeného popisu zkoumaného systému abstrahujícího od všech nedůležitých skutečností vzhledem k cíli a účelu modelu.
  2. **Vytvoření simulačního modelu.** Simulační model je vytvořen pomocí programového vybavení, kdy se abstraktní model zapíše ve formě programu.
  3. **Simulace.** K experimentování s reprezentací simulačního modelu dochází ve třetí etapě modelování a simulace.
  4. **Analýza a interpretace výsledků.** Poslední etapa je určena k ověřování správnosti modelu.

## Diskrétní simulace

Stav modelu systému se v diskrétní simulaci mění jen v konečně mnoha okamžicích během konečného časového intervalu. Změna hodnot stavových veličin může nastat jen v konečné množině časových okamžiků. V těchto okamžicích pak nastávají tzv. události (*events*). Tyto změny jsou elementární a okamžité (s nulovou dobou trvání). [4]



Obrázek 2 - Diskrétně událostní systém [vlastní]

Událost – *event* tedy nastává v určitém časovém okamžiku a vyvolává přechod mezi stavy systému neboli změnu stavu (Obrázek 2). Událostí může být současné splnění několika podmínek

**Časem řízené systémy** jsou takové systémy, kde při každé změně času je vybrána událost, která vyvolá změnu stavu systému. Může být vybrána i „nulová“ událost, která stav nemění.

**Událostmi řízené systémy** jsou systémy, kde pro každou událost je definován samostatný proces, který definuje okamžiky nastoupení události. Změna stavu je dána kombinací těchto asynchronních procesů, jak znázorňuje Obrázek 2.

Diskrétně událostní systém *A Discrete Event System (DES)*

**Diskrétně událostní** systém je charakterizován třemi základními vlastnostmi, kterými jsou, stavový prostor definovaný jako diskrétní množina, událostmi řízené přechody mezi stavy a základní pravidlo diskrétně událostních systémů, kdy mezi dvěma souslednými událostmi nedochází k žádným změnám v systému.



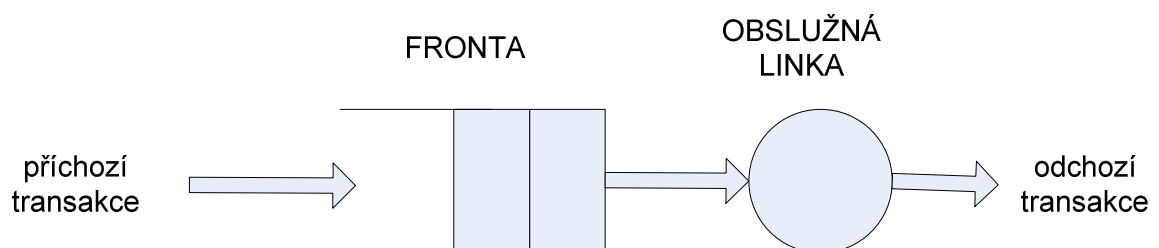
## 1.1 Příklady užití diskrétně událostních systémů

Příklady diskrétně událostních systémů se nacházejí v reálném životě i běžné praxi nejen inženýrské. V následujících pěti kapitolách jsou tyto příklady využití diskrétně událostních systémů popsány a graficky vyobrazeny.

### 1.1.1 Systémy hromadné obsluhy

Systémy hromadné obsluhy SHO (Queueing System) jsou systémy obsahující zařízení, která poskytují obsluhu transakcím. Typický SHO, jehož ukázka je na Obrázku 3, obsahuje tři základní elementy [3] [5]:

- \* **Transakce** odpovídající procesům v diskrétní simulaci a popis jejich příchodu. Transakce bývají často označovány jako zákazníci, zákazníkem (transakcí) pak může být člověk (např. čekající v bance nebo na autobusové zastávce), zprávy přenášené komunikačním médiem, požadavky, úkoly nebo transakce prováděné v počítačových systémech, výrobní součástky nebo auta v silniční síti.
- \* **Obslužné linky a popis obsluhy.** Příkladem obslužné linky jsou lidé (např. bankovní úředníci, pokladní,...), komunikační kanály užívané pro přenos zpráv, procesor, stroje užívané ve výrobních systémech, semaforey atd.
- \* **Fronty** různých typů představují prostor, kde dochází k čekání. Viditelným příkladem jsou například fronty v bance, supermarketu nebo na pásu obslužné linky. Nicméně fronty se velmi často tvoří také v komunikačních kanálech nebo počítačových systémech, kde jsou transakce umístěny do front.



Obrázek 3 - Struktura jednoduchého SHO [5]

Vznik teorie SHO je spojen s dánským matematikem A. K. Erlangem, který v roce 1908 řešil problém změřený na zkrácení čekací doby vyřizování telefonních hovorů. Celé studium SHO vzniklo díky omezenosti počtu obsluhujících jednotek, které jsou

k dispozici. Pokud by obsluha byla neomezená, nedocházelo by k žádným frontám a čekání. [2]

Při simulaci se sleduje informace o časovém průběhu transakce procházející systémem, doby čekání ve frontách a zatížení obslužných linek. Simulací se odhalují zdržení a optimalizuje výkon. [3]

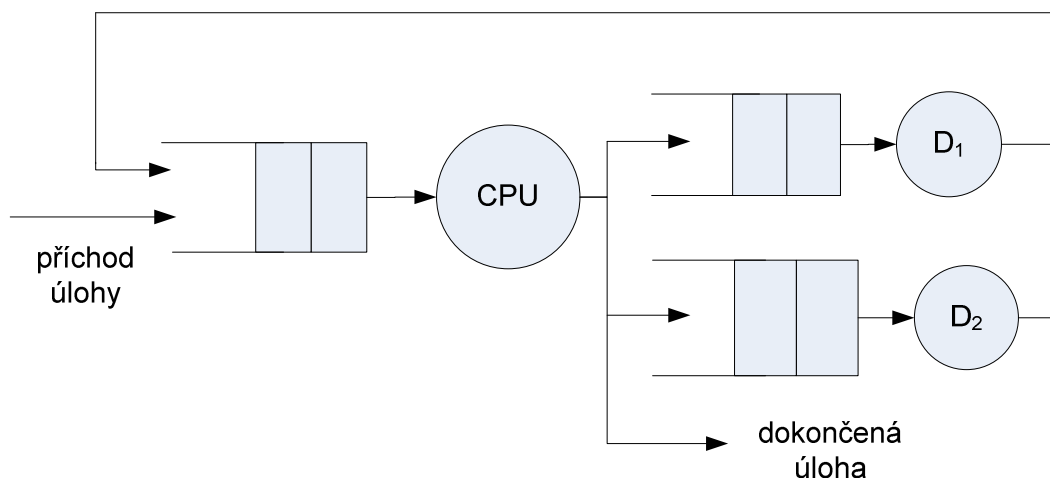
Mezi nezbytné charakteristiky SHO patří definování kapacity front a pravidla pro chování fronty [5]:

- \* Kapacita front je maximální počet zákazníků, kteří mohou být umístěni do aktuálního prostoru určeného pro čekání.
- \* Pravidla pro chování fronty určují, který zákazník čekající ve frontě má být obslužen. Nejjednoduššími pravidly jsou FIFO (first-in first-out), kde zákazníci mají být obsluženi v pořadí, v jakém přišli a opačný přístup LIFO (last-in first-out), kdy k obsluze odchází z fronty naposledy přijatý požadavek. Dalšími přístupy jsou SIRO (service in random order) obsluha zákazníků v náhodném pořadí, PŘI pravidlo značí třídění obsluhy zákazníků podle priorit a pravidlo GD (genera discipline), které zastupuje obecný řád fronty.

Množina událostí pro systém SHO je  $E = \{\text{příchod transakce, odchod transakce}\}$ .

Jako stav systému v čase  $t$  je obvykle uvažována délka fronty v čase  $t$ , někdy se zavádí konvence, že je započten i právě obsluhovaný zákazník. Stavový prostor je množina přirozených čísel  $X = \{0, 1, 2, \dots\}$ . [5]

### 1.1.2 Počítačové systémy



Obrázek 4 - Model SHO počítačového systému [5]

V typickém počítačovém systému jsou úlohy zákazníkem soupeřícím o zdroje, kterými může být procesor (CPU) nebo jiné periferie (tiskárny, disky, atd.).

Pro počítačový systém na Obrázku 4 je množina událostí  $E = \{a, d, r_1, r_2, d_1, d_2\}$  kde [5]:

- $a$       příchod nové úlohy z vnějšího prostředí,
- $d$       odchod obsloužené úlohy,
- $r_1, r_2$    směrování úlohy obsloužené na CPU k obsluze na disku  $D_1$  nebo  $D_2$ ,
- $d_1, d_2$    směrování úlohy obsloužené diskem k obsluze na CPU.

Stavový vektor se skládá z délek jednotlivých front  $x = [x_{CPU}, x_1, x_2]^T$  a stavový prostor je  $X = \{(x_{CPU}, x_1, x_2) | x_{CPU}, x_1, x_2 \geq 0\}$ .

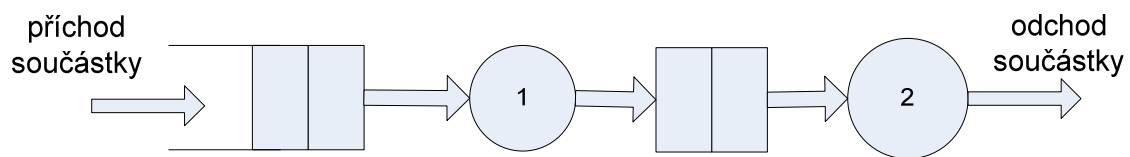
### 1.1.3 Komunikační systémy

Zákazníkem komunikačního systému jsou zprávy, datové pakety nebo telefonní hovory. Základní úlohou v komunikačních systémech jsou dva účastníci předávající si zprávy, které mají přenést přes společné přenosové médium. Médium se může nacházet ve třech stavech – volné médium (I), médium, po kterém probíhá přenos jedné zprávy (T) a stav média, které přenáší více zpráv (C). Stavy, ve kterých se může nacházet účastník, jsou volný (I), přenášející zprávu (T) nebo čekající na možnost odeslat zprávu (W). [5]

Stavový prostor je potom  $X = \{(x_{CH}, x_A, x_B) \mid x_{CH} \in \{I, T, C\}, x_A \in \{I, T, W\}, x_B \in \{I, T, W\}\}$ , a množina událostí je  $E = \{a_A, a_B, t_A, t_B, t_{CH}\}$ , kde [5]:

- $a_A, a_B$  představuje příchod zprávy pro odeslání k účastníkovi,
- $t_A, t_B$  je zahájení přenosu zprávy účastníkem,
- $t_{CH}$  je ukončení přenosu zprávy.

#### 1.1.4 Výrobní systémy



Obrázek 5 - Model pro výrobní systém [5]

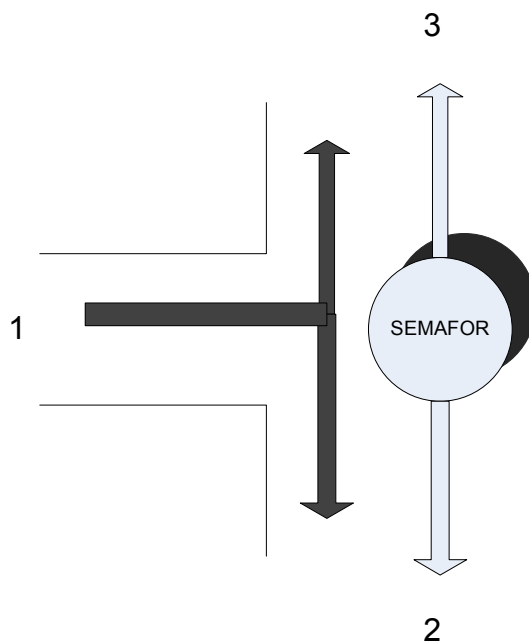
Zákazníkem ve výrobním systému jsou součástky soupeřící o různá výrobní zařízení. Fronty mají většinou konečnou délku, což způsobuje blokování obslužných zařízení. Model výrobního systému je znázorněn na Obrázku 5.

Množina událostí je  $E = \{a, c_1, d_2\}$  kde [5]:

- $a$  příchod nové součástky z vnějšího prostředí,
- $c_1$  dokončení operace na stroji,
- $d_2$  odchod výrobku ze stroje 2.

Stavový vektor tvoří počty čekajících výrobků  $x = [x_1, x_2]^T$ , stavový prostor je  $X = \{(x_1, x_2) \mid x_1 \geq 0, x_2 \in \{0, 1, 2, 3, B\}\}$ , kde stav  $B$  označuje situaci, kdy je stroj 1 blokován (stroj 2 pracuje a jeho fronta je plná, přičemž stroj 1 dokončil operaci).

### 1.1.5 Dopravní systémy



Obrázek 6 - Křižovatka se semaforem – Model pro dopravní systém [5]

V dopravní síti využívají dopravní prostředky nejrůznějších obsluh (obslužných linek) jako jsou semaforey, mýtné brány nebo obecně prostory silnic. Obrázek 6 ukazuje jednoduchou T-křižovatku, kterou lze zobrazit jako DES.

Řízení na této křižovatce zajišťují semaforey, kdy při zelené mají dovolen provoz auta ve směru (2,3) a (3,2) a při červené (1,2) a (1,3).

Množina událostí je potom  $E = \{a_{12}, a_{13}, a_{23}, a_{32}, d_{12}, d_{13}, d_{23}, d_{32}, g, r\}$ , kde [5]:

$a_{12}, a_{13}, a_{23}, a_{32}$  představuje příjezd vozidla ke křižovatce pro jednotlivé směry,

$d_{12}, d_{13}, d_{23}, d_{32}$  značí opuštění křižovatky v daném směru,

$g, r$  jsou změny signalizace (*green, red*).

Stavový prostor pak bude  $X = \{(x_{12}, x_{13}, x_{23}, x_{32}, y) \mid x_{12}, x_{13}, x_{23}, x_{32} \geq 0, y \in \{G, R\}\}$ .

## 1.2 Formy popisu diskrétních systémů

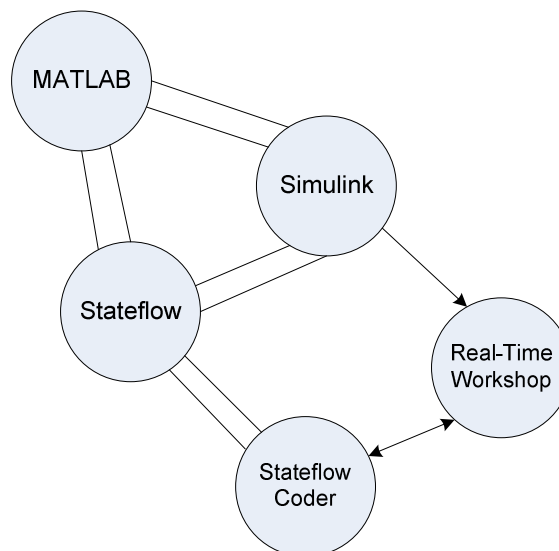
Pro popis diskrétně událostních systémů existuje celá řada simulačních programovacích jazyků. Většina běžně užívaných DES softwarů byla od poloviny devadesátých let zakládána na objektově orientovaném (OO) programování, a vybavena grafickým uživatelským rozhraním, které usnadňuje tvorbu a následnou vizualizaci modelu. Tyto jazyky používají přesně definované události, které způsobují změnu stavu modelu. Součástí těchto jazyků bývá popis struktury systémů hromadné obsluhy. [5]

### Diskrétní simulační jazyky

Programů běžně používaných pro simulaci diskrétních událostí existuje celá řada, patří mezi ně například: EXTEND, GASP, SLAM, SIMPRO využívaný ve společnosti Škoda Auto, GPSS, SIMAN/ARENA, SIMSCRIPT, SIMULA SIMEVENTS nebo STATEFLOW, posledních šest uvedených jazyků je podrobněji představeno níže.

- \* **GPSS (Genera Purpose Simulation System)** - první implementace amerického jazyka GPSS zaměřeného na simulaci systému hromadné obsluhy, se datuje od roku 1961, jde tedy o celosvětově první jazyk určený pro diskrétní simulaci. Algoritmus se vyjadřuje pomocí určitého počtu bloků daného typu. [5] [6]
- \* **SIMAN/ARENA** – Simulační jazyk SIMAN (SIMulation Analysys) by vytvořen na začátku 80. let dvacátého století. Arena je novější verze umožňující grafickou tvorbu modelů a animaci průběhu simulace. [5]
- \* **SIMSCRIPT** – Tato rodina jazyků vznikla v USA v roce 1963. Nejnovější verze SIMSCRIPT III, je dostupná přes CACI Products Company. Všeobecné využití a volně dostupná verze tohoto programu zajišťuje jeho oblíbenost při modelování systémů, které není nutné charakterizovat výhradně pomocí SHO. Používá entity a jejich atributy, metodu proměnného časového kroku. [5]
- \* **SIMULA** - První objektově orientovaný jazyk SIMULA 67 byl poprvé oficiálně uveden v roce 1967 v Norsku. Všechny moderní programovací práce jsou založeny na principech objektově orientovaného programování poprvé zavedených definicí jazyka SIMULA, který se ale prakticky neuplatnil mimo akademické prostředí. Autoři jazyka získali v roce 2002 prestižní ocenění za to, že návrhem a implementací jazyka Simula vytvořili základ objektově orientovaného programování. [7]

- \* **SIMEVENTS** – SimEvents je zakotven v programu MATLAB a jeho nadstavbě Simulink, ten rozšiřuje o nástroje pro simulace systémů diskrétních událostí. SimEvents dovoluje vyvíjet modely systémů s takovými proměnnými, jako je zahlcení, kolize zdrojů, zpoždění procesů a podobně. SimEvents je dostupný jako součást programu MATLAB od společnosti TheMathWorks, Inc. [8]
- \* **STATEFLOW** - stejně jako SimEvents je plně integrován do výpočetního prostředí MATLAB & Simulink, jak lze vidět z Obrázku 7. Diagramy Stateflow mohou reprezentovat událostmi řízené chování simulovaného systému přímo ve schématech Simulinku. Interakcí těchto dvou nástrojů lze simulovat jak spojité procesy, tak chování logiky událostmi řídicího systému, který tyto procesy ovládá, a to vše prostřednictvím intuitivního grafického uživatelského rozhraní. [8] [9]



**Obrázek 7 - Stateflow jako nástroj MATLABu [9]**

Model systému diskrétních událostí zpracovaný v této diplomové práci využívá k simulaci prostředí MATLAB & Simulink a jeho nástroje Stateflow.

## 2 Stateflow popis prostředí

Simulační vývojové prostředí Stateflow využívá Harelovu grafickou notaci založenou na koncepci hierarchických stavových automatů. Stateflow umožňuje navrhnout hierarchický stavový automat schopný komunikovat se simulačním modelem vytvořeným v prostředí Simulink. Stateflow díky přehledné struktuře vnořených stavů hierarchického stavového automatu umožňuje úsporný, přehledný a přirozený zápis modelu. [10] [11]

### 2.1 Hierarchické stavové automaty

V roce 1987, během práce na informačním systému izraelského letectva, vytvořil David Harel koncept hierarchických stavových automatů. Ačkoli je tento koncept přes dvacet let starý, je stále užitečný, a nachází uplatnění v praktické implementaci do řady vývojových nástrojů. [11]

Hierarchický stavový automat využívá k uchování kontextu aplikace přehlednou strukturu vnořených stavů, kde jsou jasně viditelná kritéria přechodů mezi stavy. Kontextově závislé odezvy na přicházející zprávy pak vyjadřují reakce daného stavu na příslušnou zprávu, jasně viditelná kritéria přechodů mezi stavy a následné reakce na změnu stavu. Hierarchický stavový automat reaguje na přijetí události změnou některých uživatelských prvků, přepsáním vstupů modelů nebo naopak čtením jeho výstupů, popřípadě může dojít ke změně kontextu aplikace. Soustředěním všech obslužných akcí vázaných na jeden stav, na jedno místo v kódu zpřehledňuje návrh a umožňuje snadnou změnu struktury stavového automatu. [10] [11]

Hierarchické stavové automaty vznikly rozšířením konečných stavových automatů o vnořené stavy, paralelismus a další prvky. Hierarchie stavů zaručuje, že každý stav nadřazený aktivnímu stavu, musí být také aktivní. Pojem paralelních stavů umožňuje uchování informace o nezávislých subsystémech zároveň. To vše umožňuje úsporný, přirozený a velmi přehledný zápis.[11]

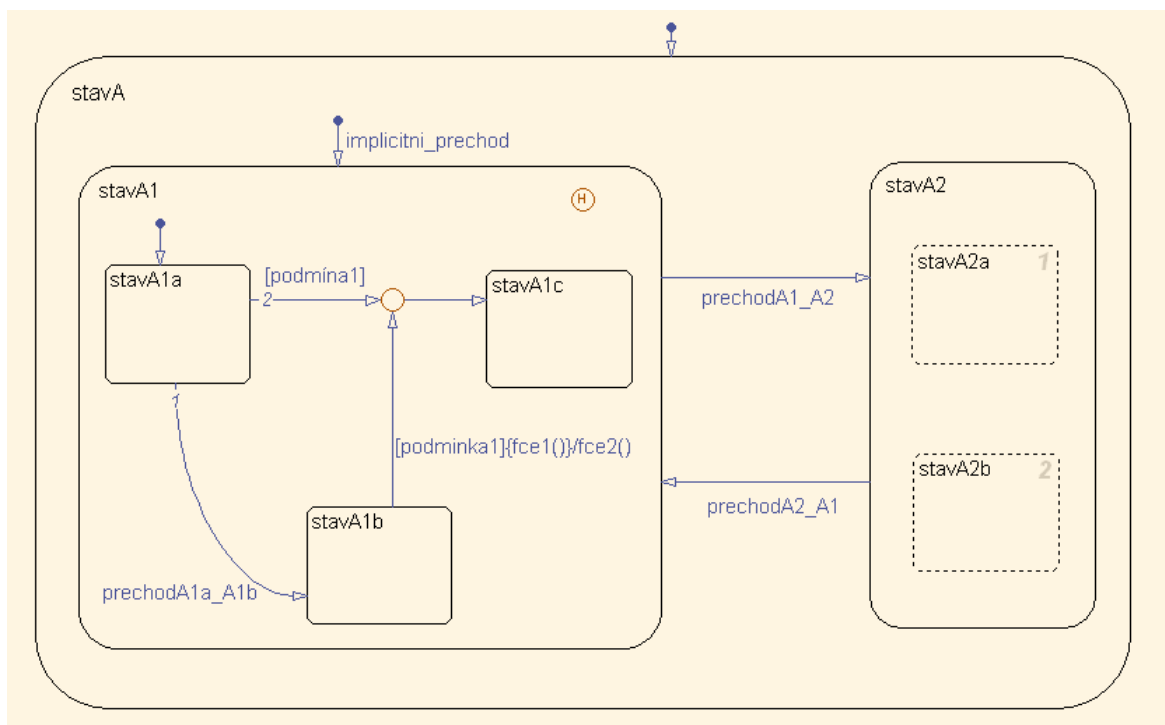
Hierarchické stavové automaty využívají syntézu Moorova a Mealyho přístupu, což umožňuje definovat akce, kterými automat aplikaci řídí jak na úrovni stavů, tak na přechodech mezi nimi. Stavové automaty Moorova typu mají výstupní hodnotu závislou jen na předchozím stavu. Kdežto Stavové automaty Mealyho typu jsou obecnější



a jejich výstupní hodnota je na rozdíl od Moorova automatu závislá jak na předchozím stavu, tak i a vstupních symbolech. Hierarchické stavové automaty pak díky syntéze těchto přístupů mohou obsahovat podmínky na přechodech a akce jak na přechodech (při kladném vyhodnocení podmínky nebo během samotného provádění přechodu) tak ve stavech (při stupu nebo opuštění stavu nebo během samotného provádění stavu). [10] [12]

## 2.2 Základní prvky Stateflow

Objekty Stateflow lze dělit na grafické a negrafické. Mezi grafické objekty patří stav, přechod, implicitní přechod, uzel, spojka, historie, box a funkce. Obrázek 8 zachycuje základní grafické objekty Stateflow. Negrafické prvky jsou zaznamenány ve Stateflow Exploreru, tyto objekty nemají svého grafického zástupce. Mezi negrafické objekty Stateflow se řadí data, události a cílové objekty (metody). [9]



Obrázek 8 – Grafické znázornění prvků Stateflow [9]

## 2.2.1 Grafické objekty Stateflow

Základními stavebními kameny Stateflow jsou stavy a přechody. Stavy reprezentují situace, ve kterých se může modelovaný systém nacházet a ve Stateflow jsou zastoupeny obdélníkem se zaobleným rohem a názvem v levém horním rohu. Přechody jsou zobrazeny jako šipky mezi stavy a reprezentují možná schémata změny stavů. [9] [10]

**Stavy** (*states*) popisují mód událostmi řízeného systému a reprezentují situace, ve kterých se může modelovaný systém nacházet. Stavy jsou hierarchické (rodič a synové) a sourozenecké stavy pak mohou být vůči sobě v poměru exkluzivním (OR) nebo paralelním (AND, čárkovaný okraj obdélníku). Součástí stavů může být akce jako [9] [10]:

- \* *Entry action* je vykonána při vstupu do stavu.
- \* *During actin* je vykonávána periodicky jakmile je stav aktivní.
- \* *Exit action* je vykonána při opuštění stavu.
- \* *On-event action* je vykonána v případě, že je přijata specifická událost a stav je aktivní.

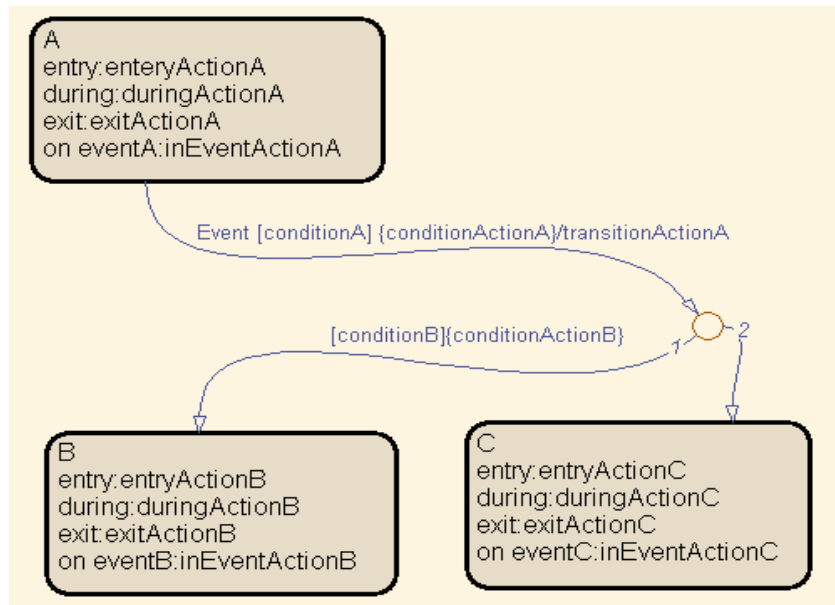
Jednotlivé akce ve stavech jsou znázorněny na Obrázku 9.

Hierarchie určuje stavům následující vlastnosti [10]:

- \* Stav, který je aktivní, má vždy aktivního i svého rodiče.
- \* Stav, který není aktivní, nesmí mít aktivního potomka.
- \* Aktivní stav s potomky musí mít aktivní právě jeden exkluzivní podstav.
- \* Aktivní stav s potomky musí mít aktivní všechny paralelní podstavy.

Změny stavů jsou znázorněny pomocí **přechodů** (*transitions*), které začínají a končí ve stavech, popřípadě spojkách. Přechody mohou obsahovat [10]:

- \* *Condition* je podmínka, která musí být splněna, aby bylo možné použít daný přechod.
- \* *Condition action* je vykonávaná jakmile je podmínka vyhodnocena jako pravda.
- \* *Transitin action* je vykonána ve chvíli, kdy je přechod skutečně vykonáván.
- \* *Event triggers* je seznam událostí, které mohou způsobit přechod po tomto stavu. Pokud na přechodu není definovaná žádná událost, může být použit s libovolnou událostí. Přechodové akce zobrazuje a popisuje Obrázek 9.



**Obrázek 9 - Akce ve stavech a přechodech [11]**

Za předpokladu aktivního stav A jsou provedeny následující akce. Při události Event je testována podmínka přechodu ConditionA. Pokud je tato podmínka pravdivá je vykonána akce ConditionActionA a testována platnost podmínky ConditionB. V případě, že je podmínka pravdivá provede se ConditionActionB, přechod se stane platným a je uskutečněna přechodová akce transitionActionA. Následně je deaktivován stav A a zároveň s tím proběhne exitActionA, je aktivován stav B a provedena vstupní akce entryActionB. Pokud podmínka ConditionB nebyla splněna, je aktivován stav C.

**Implicitní přechody** (*default transition*) určují, který z exkluzivních (OR) stavů má být aktivován při vstupu do jejich rodiče. Mohou stejně jako obyčejné přechody obsahovat podmínku, podmínkovou nebo přechodovou akci a seznam událostí. Implicitní přechody se zobrazují šipkou vycházející z puntíku umístěného v rodičovském stavu. [9] [10]

Mezi další grafické prvky stavových diagramů Stateflow patří spojky a historie.

**Spojky** (*junctions, connective junctions*) jsou místem rozhodování systému. Znázorňují se kolečkem, které může soužit jako zdroj nebo cíl přechodů. Spojky slouží ke zjednodušení grafického znázornění diagramu, umožňují totiž snížení počtu přechodů. Pomocí spojek lze graficky vyjádřit složitější algoritmus rozhodování například cyklus. [11]

**Historie** (*history junction*) je speciálním druhem spojky, která zaznamenává naposledy aktivní stav. Historie zajišťuje, že při aktivaci stavu, ve kterém je umístěna, bude vždy aktivován ten potomek, který byl aktivní v době, kdy byl stav opuštěn. Graficky je historie znázorněna jako kolečko s písmenem „H“ ve prostřed. [10]

**Boxy** (*boxes*) jsou grafické objekty Stateflow sloužící k organizaci jednotlivých bloků. Boxy jsou zobrazeny pomocí obdélníku s názvem v levém horním rohu. Pomocí boxů lze graficky oddělit jednotlivé celky Stateflow diagramu. [9]

**Grafická funkce** (*graphical functions*) je grafický objekt zahrnující funkci. Tento objekt je plnohodnotným zaznamenáním funkce stejně jako v prostředí MATLAB. Grafické zobrazení poskytuje jednoduchý zápis a možnost umístění funkce přímo ve Stateflow modelu spolu s diagramy, které tyto funkce vykonávají. To vše umožňuje snadnou tvorbu, přístup a správu funkce. [9]

## 2.2.2 Negrafické objekty Stateflow

V Stateflow Exploreru lze navíc definovat události, data a cílové objekty. Tyto atributy mají platnost rovnu stavu, ve kterém jsou definovány, a všem stavům vnořeným. Jsou-li definovány na úrovni celého Stateflow diagramu, je jejich platnost rozšířena i na okolí a dají se tak použít ke komunikaci s okolními objekty. [9]

**Události** (*events*) jsou pojmenované signály, které řídí běh Stateflow diagramu. Události jsou distribuovány po aktivních stavech, které na jejich základě provádějí akce. Události ale nejsou graficky znázorněné ve Stateflow diagramu, k jejich tvorbě a úpravě se užívá Stateflow Explorer. Události mohou být definovány v každé úrovni diagramu a mají stejné vlastnosti jako signál [9]:

- \* Lokální pro Stateflow diagram.
- \* Vstupem pro Stateflow diagram z modelu Simulink.
- \* Výstupem ze Stateflow diagramu do modelu Simulink.
- \* Vyslané do externí oblasti mimo Stateflow a Simulink.
- \* Zasláné z externího zdrojového kódu mimo model Stateflow a Simulink.

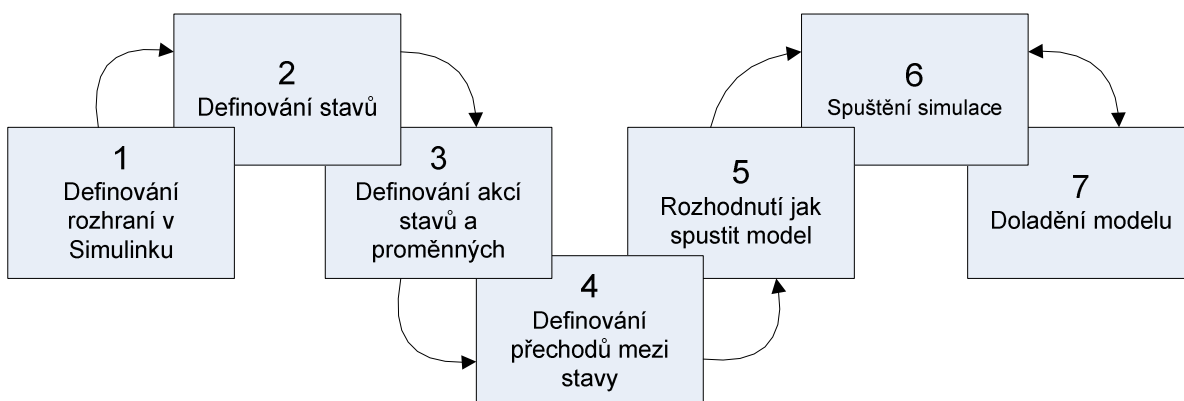
**Data** (*data*) jsou proměnné, které jednotlivé stavy vlastní. Data stejně jako události nemají grafickou notaci a jsou definovány ve Stateflow Exploreru, kde atribut *Scope* definuje, zda data jsou [9]:

- \* Lokální pro Stateflow diagram.
- \* Vstupem pro Stateflow diagram z modelu Simulink.
- \* Výstupem ze Stateflow diagramu do modelu Simulink.
- \* Dočasná data.
- \* Data definovaná v uživatelském prostředí MATLAB.
- \* Konstantní data.
- \* Vyslané do externí oblasti mimo Stateflow a Simulink.
- \* Zasláné z externího zdrojového kódu mimo model Stateflow a Simulink.

**Cílové objekty** (*target objects*) se využívají ke spuštění Stateflow pokud je vytvořen Stateflow automat. Tedy v případě, že Stateflow automat obsahuje všechny Stateflow diagramy v modelu Simulink. Cílové objekty jsou užívány zejména ke komunikaci s okolními objekty. [9]

### 2.3 Postup tvorby modelu ve Stateflow

Tvorbu modelu Stateflow lze rozčlenit do sedmi základních úloh, jak je zobrazeno na Obrázku 10. Postup tvorby modelu jde krok po kroku až do fáze šest – spuštění simulace, kde je nutné několikrát zopakovat fáze spuštění simulace a vyladění modelu, dokud nebude model odpovídat požadovanému chování. [9]



Obrázek 10 - Základní schéma tvorby modelu v prostředí Stateflow [9]

## **1. Definování rozhraní v prostředí Simulink**

V prvním kroku je nezbytné určit, jaké hodnoty mají být na vstupu modelu Stateflow a jaké budou požadované výstupy do Simulinku.

## **2. Definování stavů**

Během tvorby jednotlivých stavů modelu je nutné uvažovat jejich hierarchii a správně stavy strukturovat. V tomto kroku dochází i k dekompozici stavů, nastavení exkluzivních OR a paralelních AND stavů.

## **3. Definování proměnných**

Po fázi definování stavů přichází rozhodnutí, zda mají být ve stavech definovány aktivity typu entry, during, exit nebo on event. Navíc je nezbytné definovat proměnné jednotlivých stavů, k čemuž slouží nástroj Stateflow Explorer.

## **4. Definování přechodů mezi stavy**

V další fázi tvorby modelu Stateflow je nezbytné definovat přechody mezi stavy. Každý přechod potom spojuje jeden stav s druhým vždy v jednom směru a může být nositelem podmínek a akcí. Navíc je v této fázi třeba definovat implicitní přechody na každém stupni hierarchie OR stavů pro upřesnění, který z exkluzivních stavů má být aktivován jako první při vstupu do jejich rodiče.

## **5. Rozhodnutí jak spustit model**

Model je po svém spuštění neaktivní. Je nutné definovat, jak má být model Stateflow spuštěn. Stateflow model lze spustit třemi možnými impulzy, pomocí signálu, s použitím jiného modelu Stateflow nebo pomocí implicitních přechodů.

## **6. Spuštění simulace**

V této fázi je model dokončený, integrovaný do prostředí Simulink a připravený k simulaci. Během simulace se na modelu animuje jeho chování v čase. Animace zvýrazňuje vykonávání jednotlivých stavů a přechodů.

## **7. Vyladění modelu**

Při vyladění modelu je možné sledovat tok dat a detekovat chyby díky uživatelsky přívětivému prostředí Stateflow Debugging, které poskytuje diagnostickou pomoc.

[9]

## **2.4 Algoritmus fungování Stateflow**

### **2.4.1 Zpracování události**

Model je po svém vytvoření neaktivní a je nutné definovat mu výchozí pozici pro zpracování události. K tomu slouží implicitní přechody, které určují kořenový stav s implicitní událostí. Následně se buď neděje nic, pokud je příjemce události neaktivní. Nebo je spuštěn stav, ve kterém je tato událost definována, pokud je aktivní. [10]

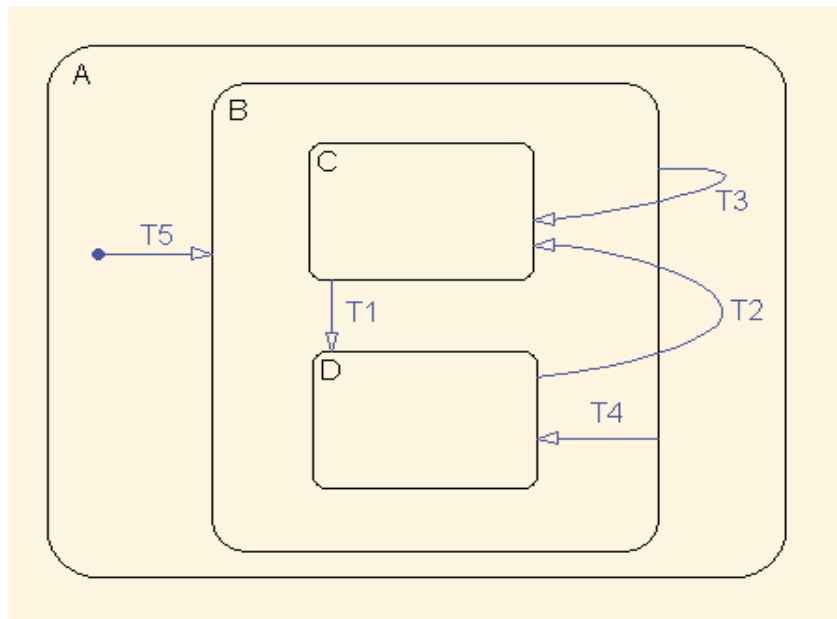
### **2.4.2 Vstup do stavu**

1. Pouze první čtyři kroky tohoto algoritmu se provedou na stavu, jehož rodič není aktivní.
2. U paralelních stavů je provedena kontrola aktivity sourozenců s vyšší prioritou. Pokud tyto sourozenecké stavy nejsou aktivní, postupně podle priority se do nich vstoupí. Prioritu jednotlivých stavů určuje jejich umístění v modelu shora dolů a zleva doprava, priorita je zobrazena pomocí číselných hodnot v pravém horním rohu stavů.
3. Stav je označen za aktivní.
4. Následně se provede vstupní akce, je-li ve stavu definována.
5. Pokud má stav své potomky, proběhne do nich vstup:
  - a. Stav s definovanou historií vstoupí do podstavu dle informací z historie.
  - b. Pokud stav historii nemá, provede se spuštění skupiny implicitních přechodů stavu.
  - c. Pokud je vztah potomků paralelní, provedou se na nich postupně dle jejich priority kroky 1-5 tohoto algoritmu.
6. Je-li stav paralelní, provede se postupně vstup do sourozenců a nižší prioritou.
7. Pokud rodič tohoto stavu není zároveň rodičem cesty, po které bylo do tohoto stavu vstoupeno, provedou se na něm kroky 6 a 7 tohoto algoritmu. [10]

### **2.4.3 Spuštění aktivního stavu**

1. Prvním krokem je spuštění skupiny vnějších přechodů stavů.
2. Pokud mezi vnějšími přechody stavu byla nalezena platná cesta, algoritmus zde končí.

3. V dalším kroku se provede průběžná aktivita stavu. Pokud je definována i akce vázaná na událost bude vykonána.
4. Následně dojde ke spuštění všech vnitřních přechodů stavu (Obrázek 11).
5. Algoritmus zde končí, pokud byla nalezena platná cesta ve vnitřních přechodech stavu.
6. Pokud není nalezena platná cesta z předchozího kroku, zaktivní se potomci tohoto stavu. Jsou-li potomci stavu paralelní, spuštění proběhne dle jejich priorit. [10]



**Obrázek 11 – Skupiny přechodů [10]**

Přechody lze rozdělit do tří skupin, implicitní, vnitřní a vnější. Přechody T1 a T2 jsou vnějšími přechody stavu C. Stav B má vnější přechod T3 a vnitřní T4. Implicitním přechodem stavu A je přechod T5. Rodičem přechodů T2 a T3 je stav A. [10]

#### 2.4.4 Opuštění aktivního stavu

1. U paralelních stavů dochází nejprve ke kontrole, zda jsou i bratrské stavy neaktivní. Pokud je některý bratr s nižší prioritou aktivní, provede se na něj opuštění stavu, opuštění se provádí podle priorit stavů od nejnižší po nejvyšší.
2. Dalším krokem je opuštění stavu u potomků v pořadí od nejnižší po nejvyšší prioritu.
3. Pokud je ve stavu definována výstupní akce dojde k jejímu vykonání.
4. Následně je stav označen za neaktivní. [10]



## 2.4.5 Spuštění skupiny přechodů

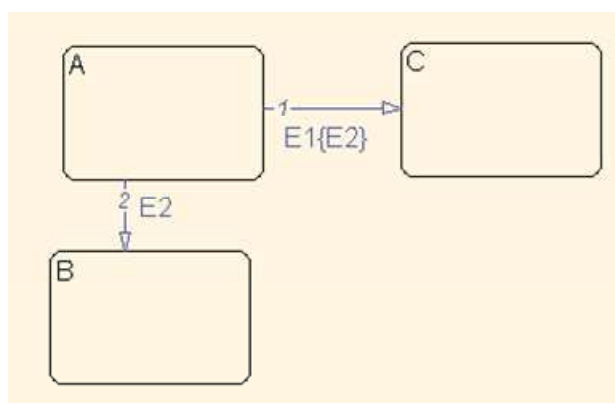
1. Seřazení přechodů se stejným počátkem dle důležitosti. Toto pořadí určují následující pravidla (pořadí dle důležitosti):
  - \* Přechody, jejichž cílový stav nebo spojka jsou umístěny výše v hierarchii stavů.
  - \* Přechody obsahující seznam událostí (*event triggers*) a podmínku zároveň.
  - \* Přechody obsahující seznam událostí.
  - \* Přechody obsahující podmínku.
  - \* Ostatní přechody – pořadí poté určuje fyzické umístění na zdroji, ve směru hodinových ručiček.
2. Výběr, v pořadí důležitosti, dalšího přechodu.
3. Testování platnosti přechodu – kontrola pravdivosti podmínky přechodu. Následné provedení podmínkové akce, pokud je specifikována.
4. Při neplatnosti přechodu následuje bod 2.
5. Směřuje-li přechod do stavu.
  - \* Z dosud vybraných přechodů se vytvoří cesta – nejsou testovány další přechody.
  - \* Deaktivují se stavy, které jsou přímými potomky rodiče vytvořené cesty.
  - \* Provedení přechodové akce posledního přechodu cesty.
  - \* Vstoupení do cílového stavu.
6. Je-li cílem přechodu historie – vstoupí se do stavu určeného historií.
7. Pokud cílem přechodu je spojka bez následných přechodů nebo historie, algoritmus končí. Nedochozí k opuštění nebo aktivování stavů.
8. Jestliže cílem je spojka s následnými přechody, dojde k provedení prvního kroku algoritmu spuštění přechodů.
9. Dojde-li k neúspěšnému otestování všech přechodů ze spojky, opakuje se algoritmus od druhého kroku. Neúspěšný konec algoritmu nastane po neúspěšném otestování všech přechodů výchozí skupiny. [10]

## 2.4.6 Mechanismus okamžitého ukončení

V každém okamžiku běhu automatu musí platit tři základní podmínky – invarianty:

- \* Aktivní stav musí mít aktivního i svého rodiče.
- \* Stav s exkluzivními potomky nesmí mít aktivní více než jeden podstav.
- \* Je-li aktivní paralelní stav, musí mít aktivní také všechny své sourozence s vyšší prioritou.

Po provedení každé akce je nutné zkontrolovat, zda nedošlo k situaci, kdy by pokračování ve vykonávaném algoritmu vedlo ke kolizi vůči výše uvedeným invariantům, názorně tuto situaci ukazuje Obrázek 12. V takovém případě je třeba provést mechanismus okamžitého ukončení algoritmu (*early return logic*). [10]



**Obrázek 12 - Mechanismus předčasného ukončení [10]**

Jakmile je stav A aktivní, pak při vyvolání události E1 se vyvolá přechod a spustí podmínková akce vyvolávající událost E2. Ze stavu A pak může být vystoupeno po vyvolání přechodu do stavu B a aktivace stavu B. Tím je ukončeno zpracování události E2 a algoritmus se vrací ke zpracování události E1. To není možné, protože dalším krokem je opuštění stavu A, který už ale není aktivní a navíc spuštění stavu C, což by porušilo jeden z invariantů. [10]

Mechanismy kontroly okamžitého ukončení po provedených akcích jsou následovné:

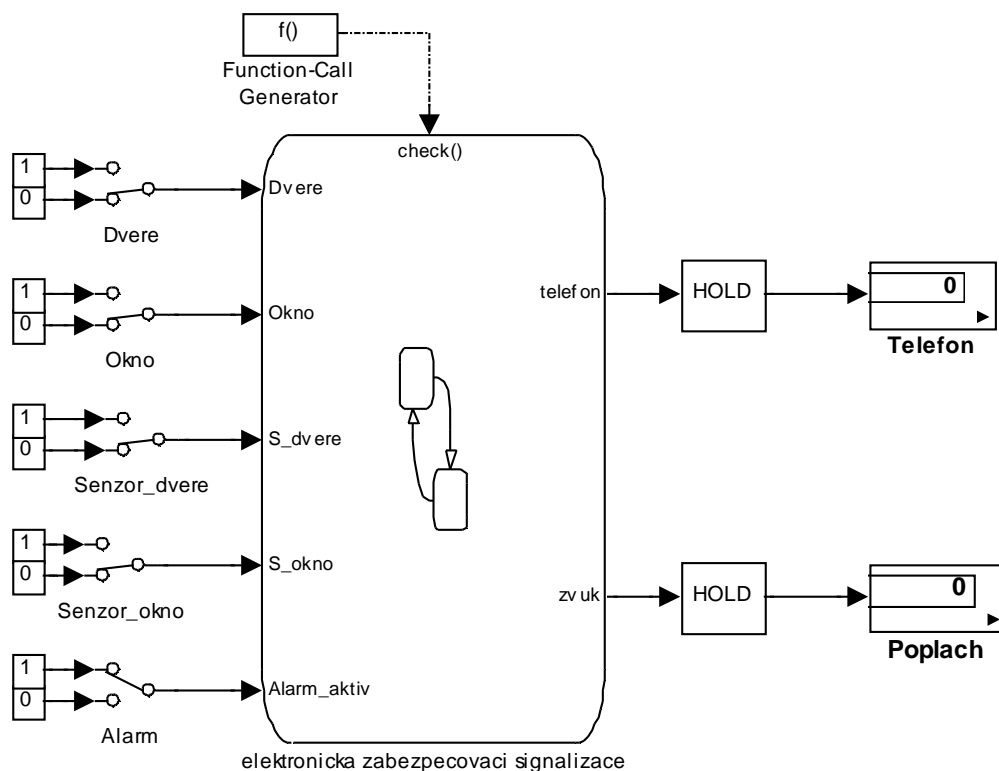
- \* Vstupní akce stavu – není-li stav aktivní okamžitě po vykonání vstupní akce stavu, neproběhnou žádné další kroky algoritmu vstupu do stavu.
- \* Výstupní akce stavu – není-li stav aktivní okamžitě po vykonání výstupní akce, neproběhnou žádné další kroky algoritmu výstupu ze stavu.

- \* Průběžná aktivita stavu a akce vázaná na událost – není-li stav aktivní okamžitě po vykonání některé z těchto akcí, nejsou vykonány žádné další kroky algoritmu spuštění aktivního stavu.
- \* Podmínková akce na přechodu – není-li zdrojový stav zkoumané cesty aktivní okamžitě po vykonání podmínkové akce (u implicitních přechodů se zkoumá aktivita rodiče cesty), nejsou vykonány žádné další kroky algoritmu spuštění skupiny přechodů.
- \* Akce přechodu – není-li aktivní rodič přechodové cesty nebo má aktivní podstavy okamžitě po vykonání akce přechodu, neproběhnou žádné další kroky algoritmu spuštění skupiny přechodů. [10]

### 3 Model elektronického zabezpečení domu

Běžnou součástí vybavení domů a bytů se staly důmyslné systémy jejich zabezpečení. K základním a nejčastěji užívaným zabezpečovacím mechanismům patří kvalitní zámky, odolné bezpečnostní vstupní dveře nebo ochranné folie na sklech oken domů. Systémy elektronické zabezpečovací signalizace (EZS) se postupem času staly oblíbenou a hojně využívanou součástí vybavení domů a bytů. Zařízení slouží především jako varovný a ochranný prvek daného prostoru před narušením pomocí jednotlivých čidel propojených v jeden funkční celek.

Model elektronického zabezpečení domu, vytvořený v prostředí programu MATLAB, je standardním příkladem diskrétně událostního modelu znázorňující elektronický zabezpečovací systém. Detektory zabezpečovacího systému hlídají okolí dveří a oken, a mechanické poškození dveří a oken. Pokud je alarm zapnut a dojde k narušení okolí, automaticky se spustí siréna, ohlašující možný pokus o proniknutí do chráněného prostoru domu. V případě, že dojde i k mechanickému poškození dveří nebo oken jako je rozbití skla, páčení zámku nebo jinému hrubému zásahu, bude spuštěna siréna a následně informována bezpečnostní agentura a předem navolená osoba nebo osoby pomocí SMS zprávy.



Obrázek 13 – Model elektronického zabezpečení domu [vlastní]

### 3.1 Popis blokového schématu modelu

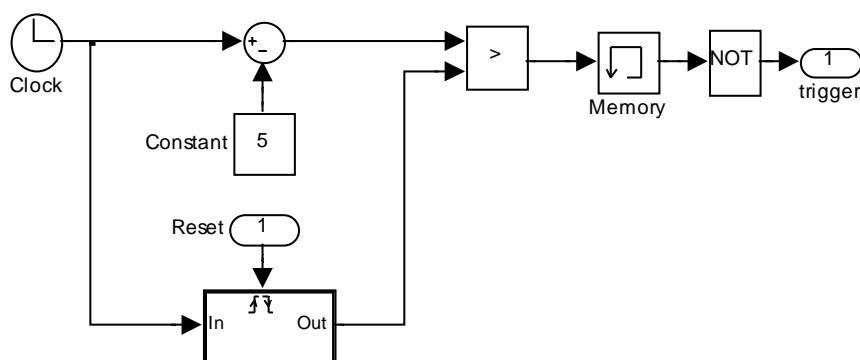
Celkový systém elektronického zabezpečení pracuje na základě vstupních hodnot od senzoru oken, senzoru dveří, dveřního kontaktu, okenního kontaktu a samotného alarmu. Na základě těchto vstupů stavový diagram vytvořený v prostředí Stateflow vyhodnotí stav narušení hlídaného objektu a aktivuje poplašné zařízení, popřípadě doplní aktivaci sirény o rozeslání varovné SMS zprávy. Celé schéma systému je patrné z Obrázku 13. Vstupní hodnoty pro stavový diagram (blok „elektronicka zabezpecovaci signalizace“) jsou typu Boolean, neboť celý systém pracuje na rozhodovací úrovni 0/1. Výstupní hodnoty (telefon, zvuk) mají charakter pulzního signálu, který je způsoben iteračním krokem výpočtu modelu.

Iterační krok výpočtu modelu má za následek nepřetržitého střídání hodnot 0/1 na výstupních hodnotách telefon a poplach. Proto byly vytvořeny bloky HOLD (Obrázek 13), které tuto vlastnost odstraňují. Blok Function-Call Generátor je využit k definování

iteračního kroku pro model Stateflow, kterému poskytuje vstupní hodnotu vzorkovacího času 0.05.

### 3.1.1 Subsystem HOLD

V subsystému HOLD dochází k převodu pulzního signálu na konstantní signál 0 nebo 1 (Obrázek 14). Hodinový signál odpovídající simulačnímu kroku zajišťuje v subsystému blok Clock. Vstupem do subsystému je pulzní signál z modelu Stateflow, který po přivedení na Trigger s každou hranou (rostoucí i klesající) upraví signál na právě běžící časovou hodnotu.

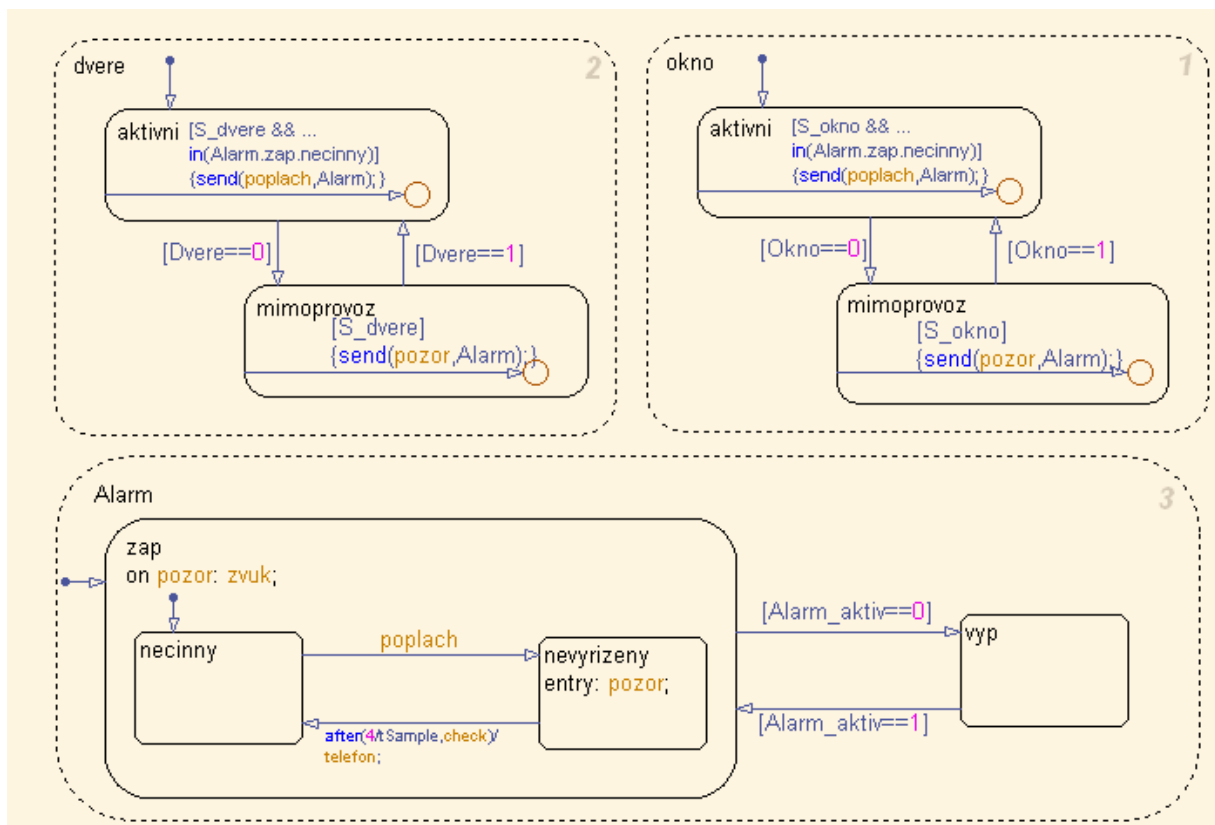


Obrázek 14 - Blok HOLD [vlastní]

Při porovnání výstupu z Triggeru a hodinového signálu (poníženého o konstantu 5), dojde k vyřešení problému s pulzním signálem od Stateflow diagramu. Zvolená konstanta 5 odpovídá podmínce, která říká, že ponížený hodinový signál musí být menší, než je požadovaná časová prodleva signálu telefon nebo poplach.

### 3.1.2 Stavový diagram Stateflow

Model Stateflow v sobě zahrnuje 3 paralelní stavy – stavy Dveře a Okno, které jsou identické a kontrolují, zda byla porušena bezpečnost domu, a stav Alarm, který vyhodnocuje informace od stavu Dveře a Okno a řídí spuštění varovné sirény popřípadě rozeslání SMS zpráv (Obrázek 15).



Obrázek 15 - Stateflow model - elektronicka zabezpecovaci signalizace [vlastní]

**Stav Dveře a Okno** zpracovávají signály ze spínačů Dvere (Okno) a S\_Dvere (S\_Okno) a zahrnují shodnou logiku upozornění. Vždy, když je proměnná S\_Dvere (S\_Okno) aktivní, je vysílána událost stavu alarm. O tom, jaká událost bude vysílána, je rozhodováno ve dvou exkluzivních podstavech – aktivní nebo mimoprovoz.

- \* **Mimoprovoz** je stav, kdy nedošlo k mechanickému poškození dveří (oken), neboli vstupní hodnota Dvere (Okno) je nastavena na 0, ale senzory S\_Dvere (S\_Okno) zaznamenaly pohyb – hodnota 1. V tomto případě dochází k vyslání události pozor stavu alarm a je spuštěna siréna.
- \* **Aktivní** stav vysílá alarmu událost poplach a zaktivňuje stav necinny v případě, že proměnné Dvere (Okno) i S\_Dvere (S\_okno) jsou nastaveny na hodnotu 1.

**Stav Alarm** kontroluje vstupní hodnotu Alarm, pokud ta je nastavena na 0 nachází se ve stavu vyp a výstupem celého modelu je pak nulová hodnota pro telefon i poplach. V případě že je Alarm zapnut zpracovává události vyslané ze stavu Dvere (Okno), kterými jsou poplach nebo pozor.

- \* **Událost Pozor** aktivuje výstupní signál zvuk. Tedy jakmile je Alarm aktivní a je mu vysílána událost Pozor, dojde ke spuštění sirény.

- \* **Událost Poplach** mění stav Alarm zap z necinny na nevyrizeny, kde je nadále spuštěna siréna. Pokud nedojde k vnějšímu zásahu do systému a nedojde ke změně na vstupních hodnotách, pak po definovaném časovém zpoždění 4s ( $4/t_{\text{Sample}}$ ) dojde k aktivaci výstupní události telefon. Zde je časová prodleva za zvukovým signálem, pro případ kdy ke spuštění poplachu dojde omylem. Tato časová prodleva byla již zmíněna při popisu bloku HOLD.



## 4 Model řešení mimořádných událostí v jaderné elektrárně

Celosvětově je asi 14% elektřiny vyrobeno ve 443 jaderných reaktorech a předběžně se ve světě uvažuje o vybudování dalších 324 reaktorů. Nejvíce jaderných zdrojů se nachází v USA (104), Francii (58), Japonsku (55), Rusku (32), Jižní Koreji (21), Velké Británii (19), Kanadě (18), Indii (18) a v Německu (17). V průběhu posledních 15 let se výroba elektřiny v jaderných elektrárnách celosvětově zvýšila o více než 660 milionů kWh ročně. Jaderné zdroje současně patří všude ve světě mezi nejlevnější energetické zdroje. Jaderná energetika má vliv na rozvoj ekonomiky a lze předpokládat, že tomu tak bude i v budoucnu. [13]

V České republice jsou v provozu dvě jaderné elektrárny, obě provozuje společnost ČEZ, a.s. Jaderná elektrárna **Dukovany** je první provozovanou jadernou elektrárnou v České republice (od r. 1985) a roční výroba elektrické energie představuje asi 20% celkové spotřeby energie v České republice. Jaderná elektrárna **Temelín** je od jara 2003 největším energetickým zdrojem České republiky a zároveň žhavým tématem týkající se jaderné bezpečnosti v celé Evropě. Proto byl pro potřeby této diplomové práce vybrán model řešení mimořádných událostí na jaderné elektrárně v České republice. [13]

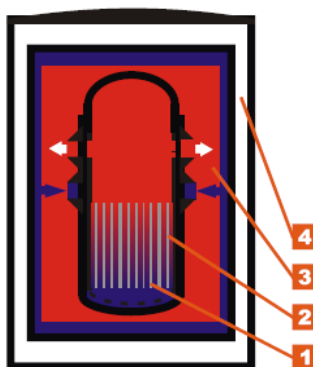
### 4.1 Popis klasifikace mimořádné události v jaderné elektrárně

Právní předpisy definující technický projekt, nároky na výstavbu, konstrukci zajišťují vysoký standard bezpečného provozu jaderných elektráren. Analýzy na českých jaderných elektrárnách prokázaly, že pravděpodobnost vzniku zdraví ohrožující poruchy reaktoru při provozu, je velmi nízká a srovnatelná s nejlepšími jadernými elektrárnami světa. Rizika z provozu těchto elektráren jsou daleko nižší než rizika, kterým je člověk vystaven v každodenním životě a která běžně přijímá. [13]

Základním principem bezpečnosti jaderné elektrárny je zajištění neporušitelnosti ochranných bariér, které brání úniku radioaktivních látek do okolního životního prostředí.

Tyto ochranné bariéry, zobrazeny na Obrázku 16, tvoří [14]:

1. Pevná keramická struktura paliva.
2. Hermetické kovové pokrytí jaderného paliva.
3. Uzavřený primární (jaderný) okruh.
4. Železobetonová ochranná obálka, která hermeticky odděluje primární okruh od životního prostředí.



Obrázek 16 - Schéma ochranných bariér jaderné elektrárny [14]

Jaderné elektrárny mají pro případ, že nastane mimořádná událost mající za následek porušení ochranných bariér, vypracován systém ochranných opatření zaměstnanců a obyvatelstva. Systém havarijní připravenosti jaderné elektrárny je pro prostory elektrárny stanoven Vnitřním havarijním plánem. Ve Vnějších havarijním plánu jaderné elektrárny jsou zahrnuty požadavky na ochranu obyvatelstva a ochranu životního prostředí. Do systému havarijní připravenosti jaderné elektrárny jsou přesně definovaným způsobem zapojeny všechny potřebné složky a zároveň je předem vytvořeno odpovídající technické, personální a kompetenční zázemí. [16]

Scénáře prověřující schopnosti zvládnutí mimořádných situací v jaderných elektrárnách jsou důkladně připravovány a popsány. Na jaderné elektrárně je definován soubor havarijních zásahových úrovní, podle kterých se každé mimořádné události přiřadí některý ze tří základních stupňů. Klasifikace závažnosti mimořádných událostí vychází z požadavků vyhlášky SÚJB č. 318/2002 Sb. v platném znění, s přihlédnutím k doporučením MAAE v dokumentu Generic assesment procedures for determining protective actions during a reactor incident. [16]

### **Klasifikace mimořádných událostí**

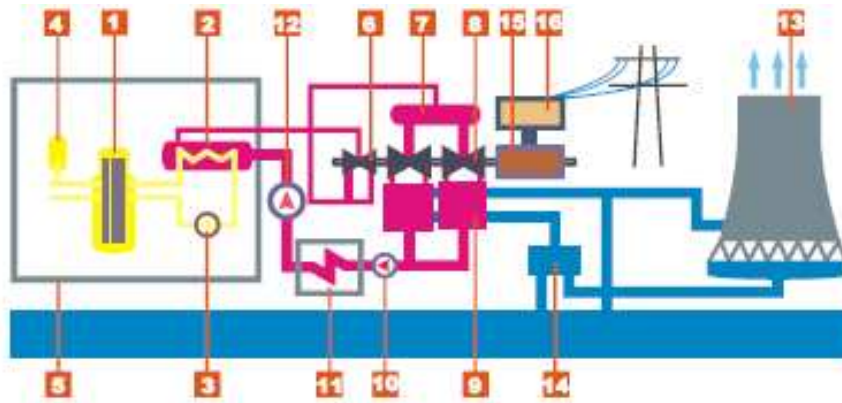
**Mimořádná událost 1. stupně** neboli radiační událost má omezený, lokální charakter. Během radiační události může dojít k nepřipustnému ozáření zaměstnanců popřípadě k nepřipustnému uvolnění radioaktivních látek do prostor zařízení nebo pracoviště. K řešení této mimořádnosti dostačují síly a prostředky obsluhy nebo pracovní směny. [15]

**Mimořádná událost 2. stupně** je nazývána radiační nehodou. Během této události může dojít k nepřipustnému závažnému ozáření zaměstnanců nebo dalších osob nebo k nepřipustnému uvolnění radioaktivních látek do životního prostředí. Tato mimořádnost, nevyžaduje zavádění opatření k ochraně obyvatelstva a životního prostředí. K řešení radiační nehody jsou nezbytné zásahy osoby držitele povolení a ke zvládnutí se popřípadě využívají i síly a prostředky smluvně zajištěné držitelem povolení. [15]

**Mimořádná událost 3. stupně** neboli radiační havárie. Tento nejhorší stupeň mimořádné události nastane v případě, že dojde k nepřipustnému závažnému uvolnění radioaktivních látek v rozsahu, který vyžaduje zavedení neodkladných opatření k ochraně obyvatelstva a životního prostředí. Při vzniku mimořádné události 3. stupně jsou aktivovány nejen zasahující osoby držitele povolení ale i osoby zasahující dle vnějšího havarijního plánu. [15]

### **Konkrétní příklady mimořádných událostí pro model**

Pro potřeby této diplomové práce bylo vybráno pět možných oblastí jaderné elektrárny, kde mohou nastat závažné poruchy celého systému. Tyto oblasti byly vybrány na základě podkladů INES Mezinárodní stupnice hodnocení závažnosti jaderných událostí. Jednotlivé části elektrárny jsou zobrazeny na Obrázku 17 a v popisku jsou zvýrazněna ta zařízení, která jsou dále zapracována v modelu jaderné elektrárny.



Obrázek 17 - Schéma jaderné elektrárny [14]

Primární okruh: 1 – reaktor, 2 – parogenerátor, 3 – hlavní cirkulační čerpadlo, 4 – kompenzátor, 5 – železobetonová ochranná obálka – kontejnment.

Sekundární okruh: 6 - vysokotlaký díl turbíny, 7 – separátor, 8 – nízkotlaký díl turbíny, 9 – kondenzátor, 10 – čerpadlo kondenzátoru, 11 – ohříváče, 12 – napájecí čerpadlo

Terciální okruh: 13 – chladicí věž, 14 – čerpací stanice chladicí vody

Elektrická část: 15 – elektrický generátor, 16 – transformátor

Jedná se o příklady mimořádných událostí na jaderné elektrárně, které se skutečně udály. Jsou to:

- \* Nehoda z ledna 2007 v jaderné elektrárně Sizewell A ve Velké Británii, kde došlo k nehodě na potrubí. Při této havárii nedošlo k významnému ohrožení zaměstnanců ani veřejnosti – v modelu označen jako vstup Potrubí.
- \* Požár na sekundární části jaderné elektrárny Vandellos, Španělsko v roce 1989. Tato nehoda nevedla k úniku radioaktivity do okolí, ani k poškození aktivní zóny reaktoru – v modelu vstup Kondenzátor.
- \* Havárie ve francouzské jaderné elektrárně v Saint Laurent z roku 1980, kdy došlo k poškození aktivní zóny reaktoru – kontejnmentu. V důsledku této havárie vznikla značná škoda na zařízení bez závažného úniku radioaktivních látek mimo elektrárnu – vstupní hodnota Kontejnment.
- \* Těžké poškození aktivní zóny reaktoru na jaderné elektrárně Free Mile Island v roce 1979 USA, jejíž účinky na okolí byly omezené, ale měla velký dopad na vnitřní část elektrárny. Poškození způsobila porucha na hlavním vodním napájecím čerpadle chladicího systému – vstup Čerpadlo pro model řešení mimořádných událostí v jaderné elektrárně.

- \* Nejrozsáhlejší havárie z roku 1986 na černobylské jaderné elektrárně, kdy došlo k přehřátí a následné explozi na čtvrtém reaktoru. Tato exploze měla za následek kontaminaci rozsáhlého území – v modelu vstup Reaktor.

V Tabulce 1 je uvedena klasifikace mimořádných událostí zpracovávaných modelem Stateflow.

**Tabulka 1 - Klasifikace mimořádných událostí [vlastní]**

Stupeň MU	Zařízení jaderné elektrárny
<b>1. stupeň MU</b>	potrubí
<b>2. stupeň MU</b>	kondenzátor, kontejnment
<b>3. stupeň MU</b>	čerpadlo, reaktor

Pokud nastane některá z mimořádných událostí, okamžitě se aktivuje příslušná složka Organizace havarijní obsluhy, jak je popsáno dále v kapitole 4.2 Popis systému vyrozumění a varování.

## **4.2 Popis systému vyrozumění a varování**

Na základě zhodnocení rozsahu a charakteru vzniklé mimořádné události na jaderné elektrárně je zajištěno varování a vyrozumění dotčených složek systému. Mezi tyto složky jsou řazeni zaměstnanci jaderné elektrárny, vnější orgány státní správy, územní samosprávy a v neposlední řadě i obyvatelstvo. Systém vyrozumění a varování zajišťuje jednak varování obyvatelstva a jednak aktivaci havarijních podpůrných středisek, státní monitorovací sítě a integrovaného záchranného systému. Dokumentace havarijního plánování podrobně zpracovává systém vyrozumění a varování. Základní dokumentaci havarijní připravenosti tvoří Vnitřní havarijní plán a Vnější havarijní plán. [13]

### **Vnitřní havarijní plán**

Vnitřní havarijní plán je dokument jaderných elektráren, schválený Státním úřadem pro jadernou bezpečnost. Plán popisuje zabezpečení základních povinností provozovatele jaderné elektrárny, součástí plánu jsou pokyny k zabezpečení havarijní připravenosti, zajištění ochrany zaměstnanců a dalších osob v areálu jaderné elektrárny v případě mimořádných událostí a zejména v případě vzniku radiační nehody nebo havárie. Vnitřní

havarijní plán je závazný pro zaměstnance jaderné elektrárny a všechny ostatní osoby, které se zdržují v areálu jaderné elektrárny. [13] [16]

### **Vnější havarijní plán**

Vnější havarijní plán je zpracován pro zónu havarijního plánování (ZHP). Velikost ZHP stanovuje Státní úřad pro jadernou bezpečnost na základě analýz scénářů radiologických dopadů neprojektovaných havárií. Vnější havarijní plán je základním dokumentem složek havarijní připravenosti na řešení a realizaci opatření k ochraně obyvatelstva, životního prostředí a majetku v případě klasifikace mimořádné události 3. stupně. V plánu je vymezeno zabezpečení havarijní připravenosti v okolí jaderné elektrárny z hlediska kompetenčních, organizačních, personálních a materiálně technických podmínek. [13] [16]

### **Varování obyvatelstva**

Systém vyrozumění a varování zabezpečuje včasné varování obyvatelstva v případě mimořádných událostí na jaderné elektrárně, které by mohly vést k úniku radioaktivních látek do životního prostředí. K varování obyvatelstva dochází bezprostředně po vyhlášení vzniku MU 3. stupně. Varování obyvatelstva se provádí spuštěním sirén v ZHP a současně s tím je zabezpečeno odvysílání audiovizuálních kazet v České televizi a Českém rozhlase s předem nahranými informacemi o vzniku radiační havárie a s pokyny o provedení neodkladných ochranných opatření pro obyvatelstvo. Na tyto informace navazují přímé televizní a rozhlasové vstupy orgánů státní správy s oznámením o zavedení příslušných následných opatření a jejich popis. [13] [16]

Součástí systému varování je havarijní příručka poskytující základní informace pro činnost obyvatelstva v případě vyhlášení radiační havárie a jednotlivých ochranných opatření. Příručka je distribuována do všech domácností v ZHP jaderné elektrárny. Příručka pro roky 2010 a 2011 je volně dostupná na internetu.

### **Principiální schéma systému vyrozumění a varování**

Jednotlivé orgány dotčené při vzniku mimořádné události jsou zaznamenány na Obrázku 18. Informovanost se liší podle rozsahu mimořádné události. Diagram informovanosti byl vypracován na základě podkladů dostupných od společnosti

ČEZ., a.s., SÚJB a jednotlivých integrovaných záchranných systémů dotčených krajů a obcí. Zapracovány byly údaje ze scénářů průběhu cvičení ZÓNA v letech 2002 až 2010, kde jsou podrobně zaznamenány jednotlivé postupy řešení mimořádných událostí.

### **Mimořádná událost 1. stupně**

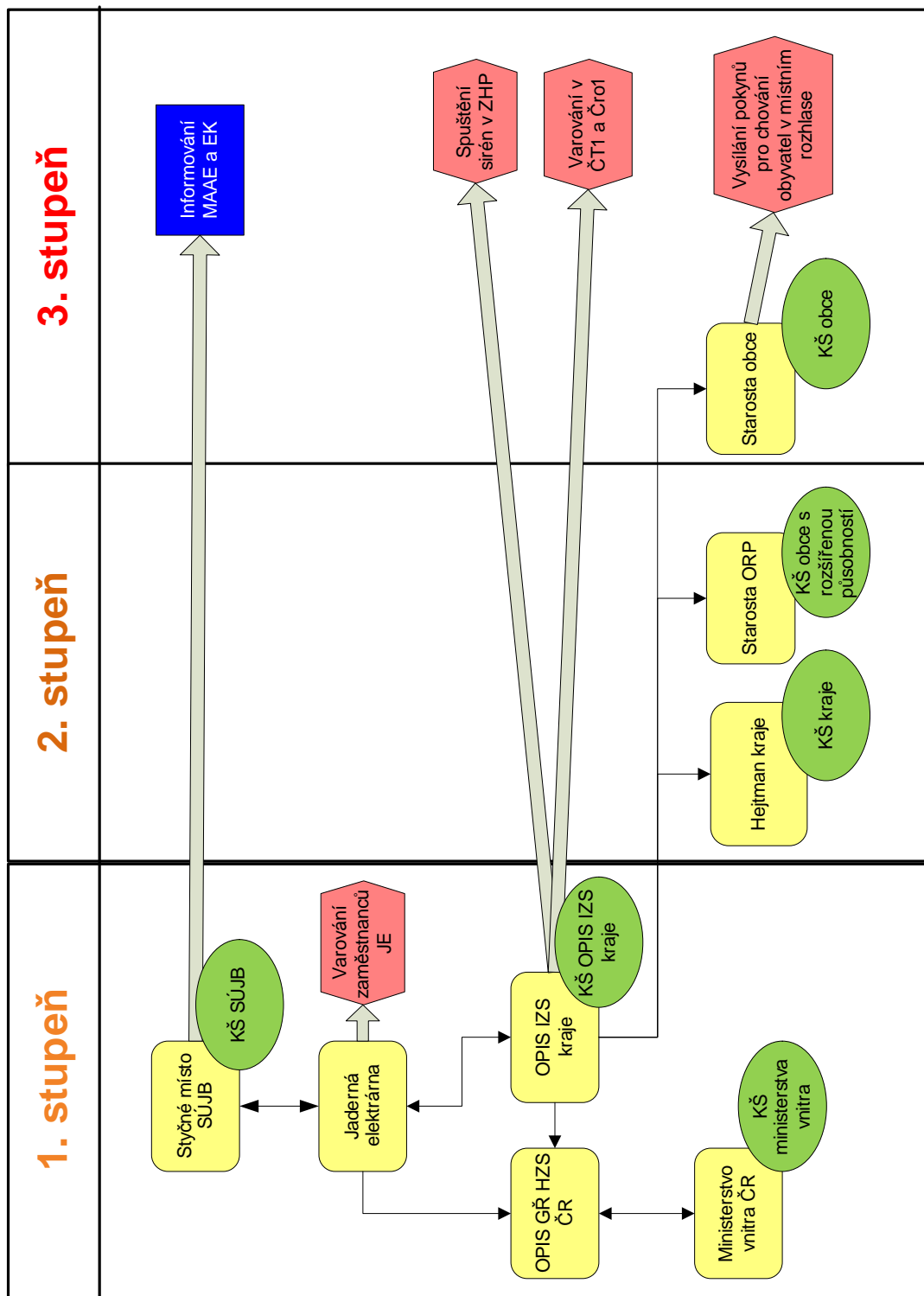
Zřizovatel jaderné elektrárny prostřednictvím směnového inženýra neprodleně informuje o vzniku MU 1. stupně Státní úřad pro jadernou bezpečnost, OPIS IZS příslušného kraje a OPIS HZS GŘ ČR. O vzniku radiační události jsou informováni také zaměstnanci a další osoby v areálu jaderné elektrárny upoutávacím gongem a následným hlášením v provozním rozhlase. Případně mohou být k varování v areálu elektrárny použity hlasité dorozumívací stanice, telefony nebo vnitřní (objektové) sirény a majáky. Styčné místo SÚJB pak ihned po obdržení zprávy o vzniku MU svolává krizový štáb, stejně tak i OPIS IZS kraje. OPIS GŘ HZS ČR informuje o vzniklé události ministerstvo vnitra, kde je svolán krizový štáb.

### **Mimořádná událost 2. stupně**

V případě, že dojde ke vzniku události druhého stupně, ať již nenadále nebo rekvalifikací ze stupně číslo jedna, rozšíří směnový inženýr tuto informaci stejným orgánům, jako v případě stupně prvního. Postup jednotlivých orgánů je stejný jako v případě prvního stupně MU, jen OPIS IZS kraje předá tuto informaci i hejtmanovi kraje a starostům ORP v zóně havarijního plánování. Hejtman kraje bezprostředně svolá krizový štáb kraje, stejně tak i starostové obcí s rozšířenou působností zahájí činnost krizových štábů.

### **Mimořádná událost 3. stupně**

Vyhlásí-li směnový inženýr MU 3. stupně, budou neprodleně informováni všechny orgány havarijní odezvy. Styčné místo SÚJB svolá svůj krizový štáb a odešle zprávu o vzniklé havárii evropské komisi a mezinárodní agentuře pro atomovou energii. OPIS IZS kraje svolá svůj krizový štáb, a neprodleně informuje hejtmana kraje, starosty ORP i jednotlivých obcí. OPIS IZS kraje také zajistí aktivaci sirén v ZHP a odvysílání varovné informace v Českém rozhlase a České televizi. Starostové obcí svolají krizové štáby a zajistí vysílání pokynů v místním (obecním) rozhlase. Na všech úrovních orgánů havarijní odezvy budou svolány krizové štáby.

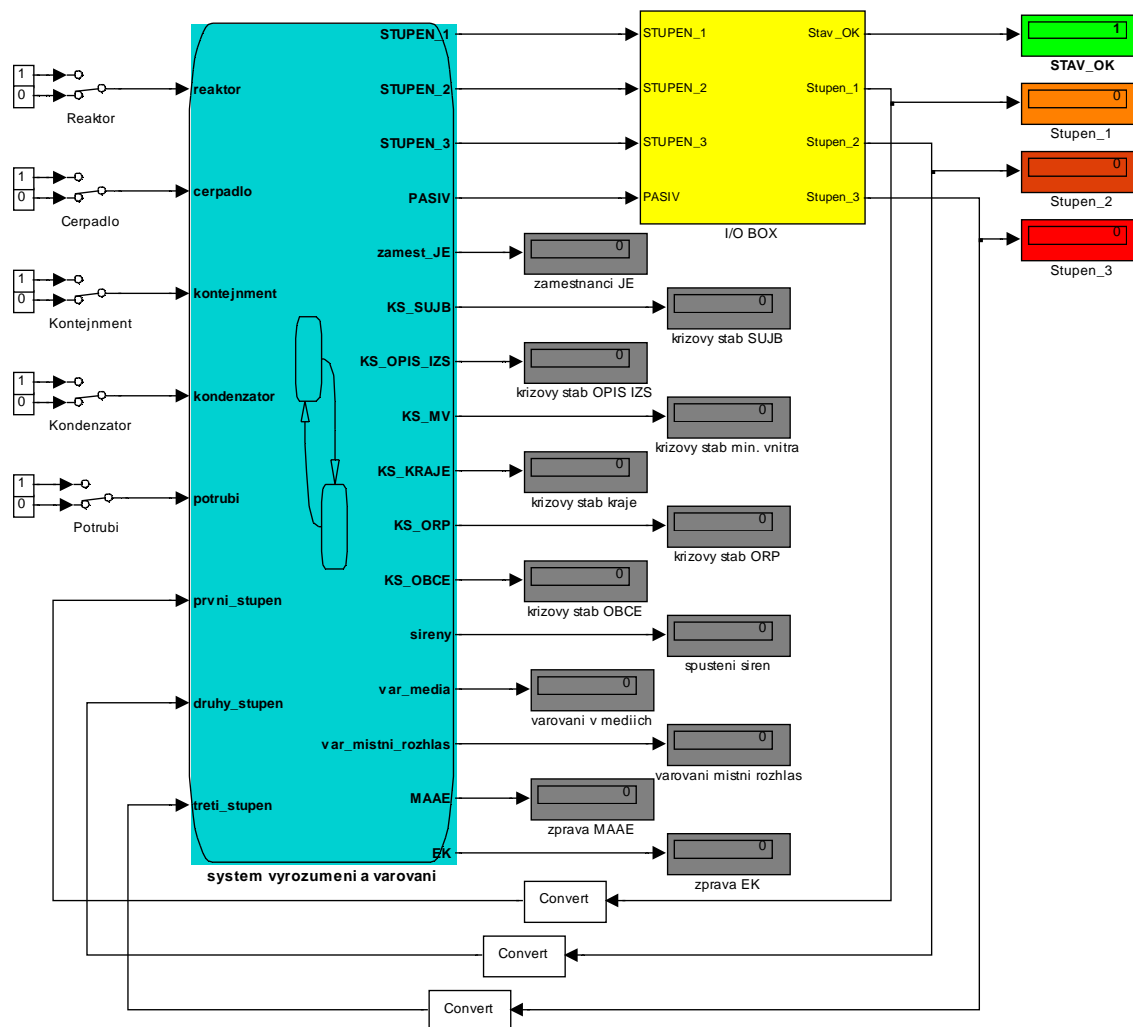


Obrázek 18 - Principiální schéma systému vyzoomění a varování [vlastní – inspirováno [17]]



## 4.3 Návrh modelu řešení mimořádných událostí v jaderné elektrárně

Model řešení mimořádných událostí v jaderné elektrárně je vytvořen v prostředí programu MATLAB & Simulink s využitím knihovny Stateflow k simulaci diskretních událostí. Celý model znázorňuje Obrázek 19. Model byl pro potřeby popisu rozdělen do tří hlavních oblastí, kterými jsou – Bezpečnostní systém (vstupní hodnoty), Stavový diagram Stateflow (stavy jednotlivých částí) a Zpracování signálu (subsystém I/O BOX).



Obrázek 19 - Model řešení mimořádných událostí v jaderné elektrárně [vlastní]

### Bezpečnostní systém

Rozsah mimořádné události ovlivňuje pět základních částí jaderné elektrárny, tato zařízení jsou vstupem do stavového diagramu, který vyhodnocuje běh celé elektrárny. Konkrétně

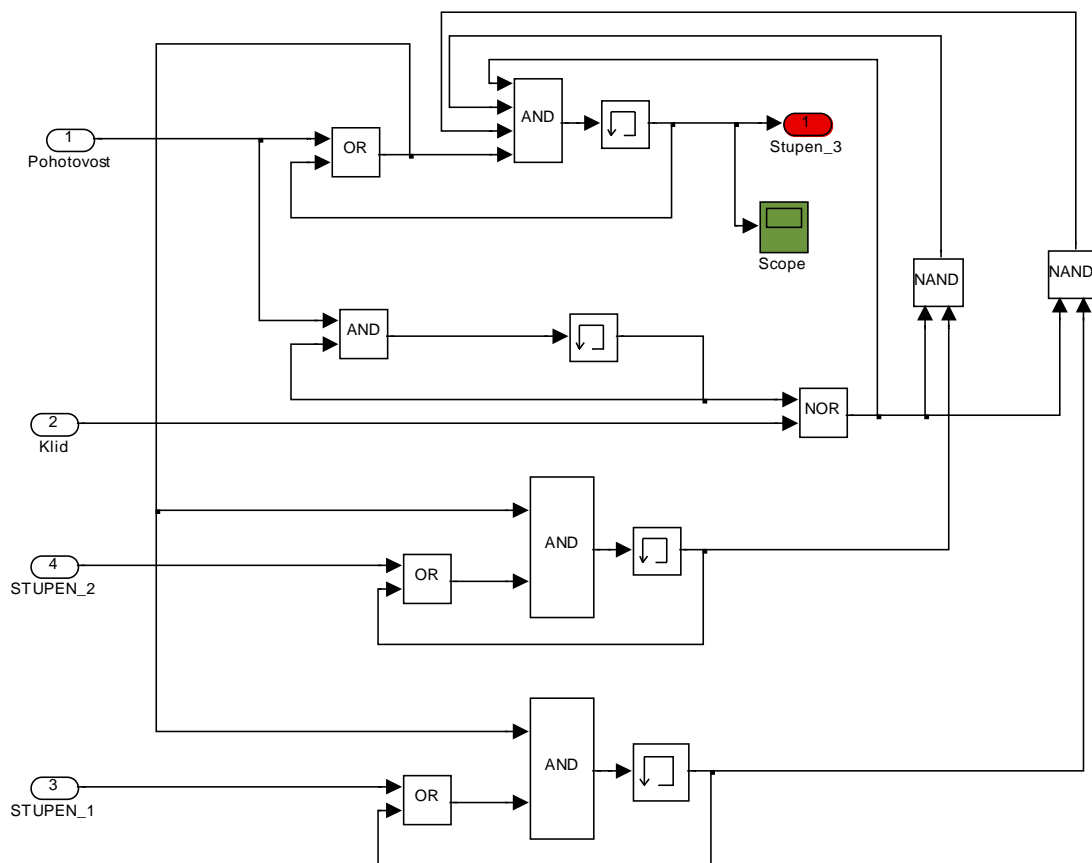
se jedná o: Reaktor, Čerpadlo, Kontejnment, Kondenzátor a Potrubí. Obsluha jednotlivých zařízení informuje o jejich stavu. V případě poruchy je aktivován bezpečnostní systém v jednotlivých částech jaderné elektrárny, který v modelu nahrazují jednotlivé spínače. Defaultní hodnota tohoto bezpečnostního spínače je „0“, což odpovídá standardnímu, bezporuchovému chodu zařízení.

### **Stavový diagram Stateflow**

Ve stavovém diagramu dochází ke kontrole a vyhodnocení stavu jaderné elektrárny. Na základě vstupních hodnot od bezpečnostního zařízení dojde k vyhodnocení závažnosti havárie a tím vyvolání dané mimořádné události. Mimořádná událost 1. stupně nastane v případě, že je zaznamenána porucha na potrubí. Pokud dojde k poruše v kondenzátoru nebo na kontejnmentu je vyhlášena mimořádná událost 2. stupně – tedy radiační nehoda. Při poruše čerpadla nebo reaktoru je vyvolána mimořádná událost 3. stupně. Klasifikaci mimořádné události na těchto pěti částech, uvedena v Tabulce 1, provádí směnový inženýr jaderné elektrárny. Výstupní signály obsahují informaci o typu události a o informovanosti příslušných úřadů.

### **Zpracování signálu**

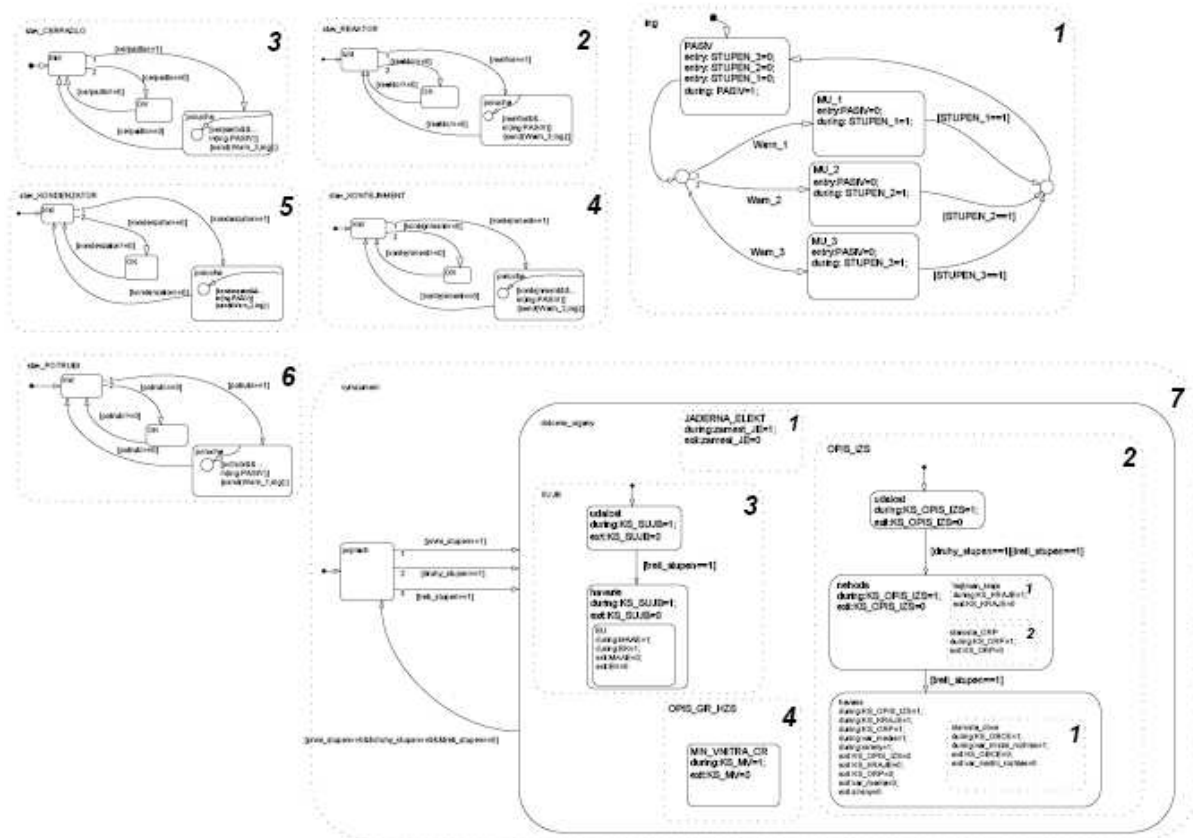
Jak již bylo zmíněno v kapitole 3 Model elektronického zabezpečení domu, výstupní signály z bloku Stateflow se chovají jako pulzní signály. Takovýto signál není výhodný pro zobrazení. Proto bylo potřeba vytvořit subsystém, který převede pulzní signál na signál nabývající konstantních hodnot 0/1. Takto upravené signály jsou zobrazeny na display (čtyři barevné display Obrázek 19) a dále konvertovány na vstupní informace pro stavový diagram. Pro vyřešení pulzních signálů byly použity bloky logických operátorů v kombinaci s prvkem MEMORY (Obrázek 20), který v paměti uchovává předešlou iterační hodnotu. Díky vnitřní logice jednotlivých subsystémů bylo docíleno konstantních výstupních signálů.



Obrázek 20 – Subsystém bloku I/O BOX [vlastní]

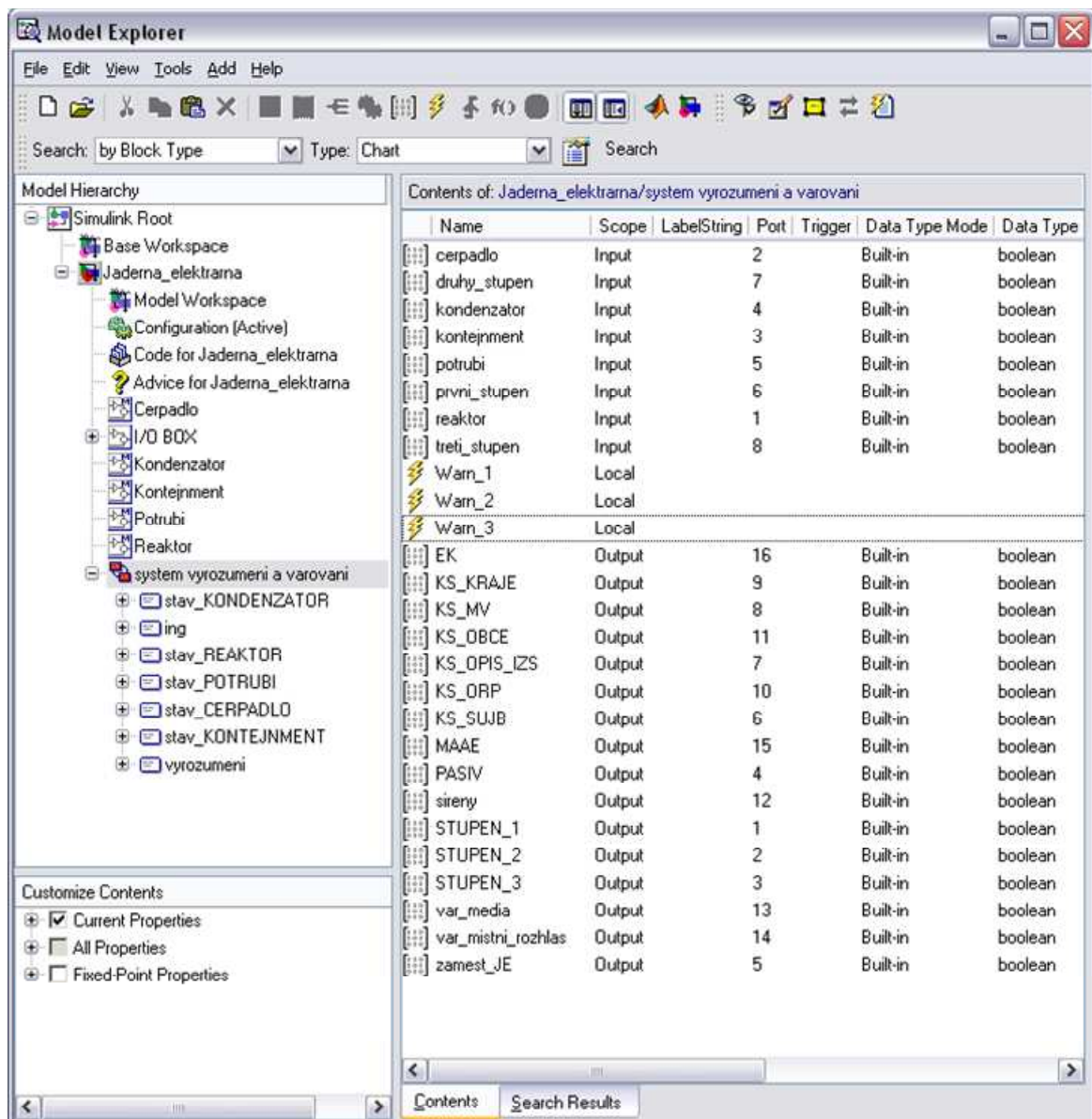
### 4.3.1 Stavový diagram Stateflow

Stavový diagram system vyrozumění a varování obsahuje sedm paralelních stavů (Obrázek 21). Jedná se o stavy, v nichž se nachází jednotlivé části jaderné elektrárny (stavy 2 až 6), stav klasifikace událostí (1 ing), a stav vyrozumění a varování (7 vyrozumění). Pořadí jednotlivých stavů je dáno jejich důležitostí a zaznamenáno v pravém horním rohu paralelních stavů. První je stav ing, který představuje operační mozek celého systému a hlídá stav jednotlivých částí. Je zde zaznamenána logika klasifikace MU a dochází zde k zaktivnění událostí nesoucí rozsah MU. Dalším v pořadí jsou bloky s jednotlivými zařízeními jaderné elektrárny, kde může dojít k poruše, které zpracovávají vstupní informace. A poslední v pořadí je nejobsáhlejší stav vyrozumění, který zajišťuje aktivaci výstupních událostí.



Obrázek 21 – Stateflow model - system vyzovneni a varovani [vlastní]

Hodnoty, které do modelu vstupují stejně jako výstupní hodnoty, jsou typu Boolean, celý systém pracuje s informací porucha/MU nastala nebo nenastala – tedy logikou Booleovy algebry Ano/Ne (0/1). Tato proměnná byla vstupním hodnotám nastavena ve Stateflow Exploreru. Z Obrázku 22 níže, který zachycuje Stateflow Explorer celého systému je dobře patrné všech 8 vstupních a 16 výstupních hodnot (Input a Output hodnoty paramateru Scope) a také tři hlavní události celého systému. Jsou to události Warn\_1, Warn\_2 a Warn\_3, znak žlutého blesku, popsané dále v textu. Číselné označení u vstupů a výstupů je pouze informativní a určuje jejich vzestupné pořadí na grafickém zobrazení diagramu Stateflow v prostředí Simulink (Obrázek 19).

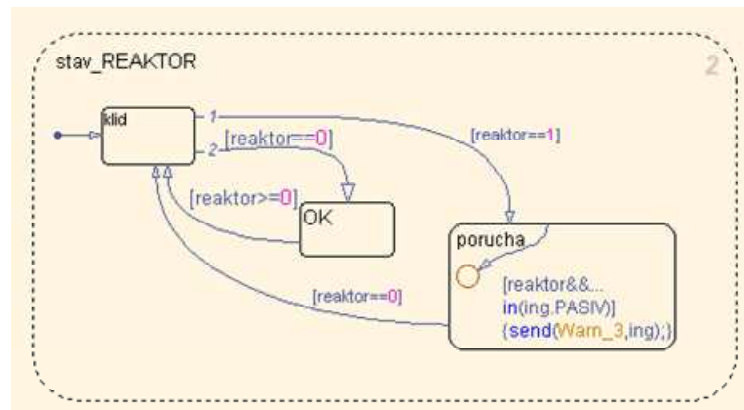


Obrázek 22 - Stateflow Explorer [vlastní]

### Stavy jednotlivých zařízení jaderné elektrárny 2 až 6:

Jedná se o stavy: stav\_REAKTOR, stav\_CERPADLO, stav\_KONTEJNMEN, stav\_KONDENZATOR a stav\_POTRUBI, které zaznamenávají shodný algoritmus. Ukázka stavu stav\_REAKTOR je na Obrázku 23. Dochází zde k nepřetržité kontrole stavu na jednotlivých zařízeních jaderné elektrárny. Implicitní přechod směřuje do stavu klid, který je aktivní jako první po vstoupení do rodiče stav\_REAKTOR. Pokud dojde k poruše v jednotlivých částech jaderné elektrárny, přejde spínač do polohy 1. Tím je aktivován přechod, díky němuž se systém dostává ze stavu klid do stavu porucha. Ve stavu porucha je vyslána událost Warn\_x do stavu ing. Událost Warn\_x je vyslána ze stavu porucha,

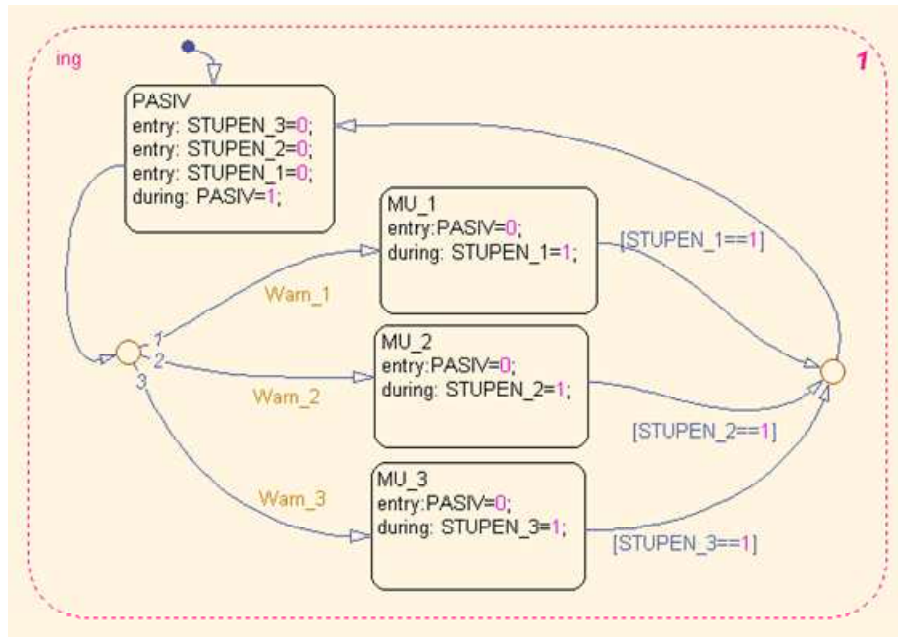
jen tehdy, pokud je splněna vnitřní podmínka stavu. Při odstranění závady na zařízení elektrárny je vyvolán přechod, který vrátí systém ze stavu porucha do stavu klid.



Obrázek 23 - Stav\_REAKTOR [vlastní]

### Stav ing

Stav ing slouží k aktivování výstupních hodnot (Obrázek 24). Implicitní přechod určuje první stav k aktivování exkluzivní stav PASIV. Spojka následně slouží jako křižovatka, kde rozhodujícím kritériem je událost zasláná z bloků 2 až 6. Při vstupu do stavů MU\_1, 2 a 3 proběhne akce PASIV=0 a průběžná aktivita STUPEN\_X=1, což zapříčiní platnost podmínky na přechodu z jednotlivého stavu a průběh všech aktivit v rodičovském stavu ing se znovu zopakuje. Zde se rozhoduje o výstupních hodnotách klasifikace mimořádné události na jaderné elektrárně neboli STUPEN\_1, STUPEN\_2, STUPEN\_3 nebo PASIV.



Obrázek 24 - Stav ing [vlastní]

Tyto výstupní hodnoty po jejich konvertování (blok I/O BOX) naplňují i poslední nejvyšší sedmý z rodičovských stavů diagramu Stateflow stav vyrozumění.

### Stav vyrozumění

Stav vyrozumění je rozhodující pro předání informace o vzniku mimořádné události všem dotčeným orgánům. Celý tento stav reprezentuje Obrázek 25. Dva exkluzivní stavy poplach a dotcene\_organy nepřetržitě kontrolují rozsah mimořádné události. V případě, že nastane MU 1, 2 nebo 3, provedou se přechody ze stavu poplach a aktivní se stane stav dotcene\_organy. Stav dotcene\_organy je rodičem čtyř paralelních podstavů zastupujících jednotlivé složky havarijní odezvy – stav JADERNA\_ELEKT, stav OPIS\_IZS, stav SUJB a stav OPIS\_GR\_HZS, které jsou popsány dále. Všechny tyto stavy zahrnují stejnou logiku, kdy jakmile je stav aktivní průběžná aktivita = 1 a při opuštění stavů jsou všechny průběžně aktivity ukončeny výstupní aktivitou, kdy jejich hodnota je přenastavena na 0. Toto přepínání hodnot se pak zobrazuje na display – dvanáct šedivých display bloků v prostředí Simulink (Obrázek 19).

- \* **Stav JADERNA\_ELEKT** - První v pořadí je aktivován stav JADERNA\_ELEKT, a provedena průběžná aktivita zamest\_JE=1, která je výstupní událostí celého stavového diagramu a zobrazí se na display zamestnanci JE.

- \* **Stav OPIS\_IZS** – O vzniku mimořádné události na jaderné elektrárně je neprodleně informován i OPIS IZS, který tuto informaci předává dál na úroveň krajů a obcí a v případě jaderné havárie spouští sirény v obcích ZHP a vydá pokyn k odvysílání výstražné informace Českou televizí a Českým rozhlasem.

V modelu jsou ve stavu vytvořeny tři podstavy zastupující jednotlivé mimořádné události.

Stav udalost je aktivován jako první a provedou se zde akce průběžná aktivita KS\_OPIS\_IZS=1, výstupní aktivita KS\_OPIS\_IZS=0, kdy každá tato událost je zobrazena na display krizovy stab OPIS IZS.

Stav nehoda je aktivní jakmile jsou splněny podmínky přechodu druhu\_stupen=1 nebo tretí\_stupen=1. Zde dochází opět ke stejné průběžné akci jako ve stavu udalost a navíc jsou zde definovány dva paralelní podstavy hejtman\_kraje a starosta\_ORP, kdy každý po jejich aktivaci provede průběžnou aktivitu KS\_KRAJE=1 a KS\_ORP=1. To jsou opět výstupní události zobrazené na display.

Stav havarie je aktivní v případě splnění přechodové podmínky tretí\_stupen=1. Postupně jsou prováděny akce shodné pro předchozí stav nehoda. Navíc je zde průběžná aktivita var\_media, kterou zastupuje display varovani v mediich. Tento stav je rodičem jednoho podstavu starosta\_obce, který po svém aktivování provádí průběžné akce KS\_OBCE=1 a var\_mistni\_rozhlas=1, které jsou zobrazeny na display krizovy stab obce a varovani mistni rozhlas.

- \* **Stav SUJB** – Třetí v pořadí důležitosti je paralelní stav zastupující v realitě Státní úřad pro jadernou bezpečnost. Zde jsou vytvořeny dva exkluzivní podstavy udalost a havarie, kdy je nejprve vstoupeno do stavu udalost a při platnosti podmínky tretí\_stupen=1 je z něj vystoupeno a vstoupeno do stavu havarie.

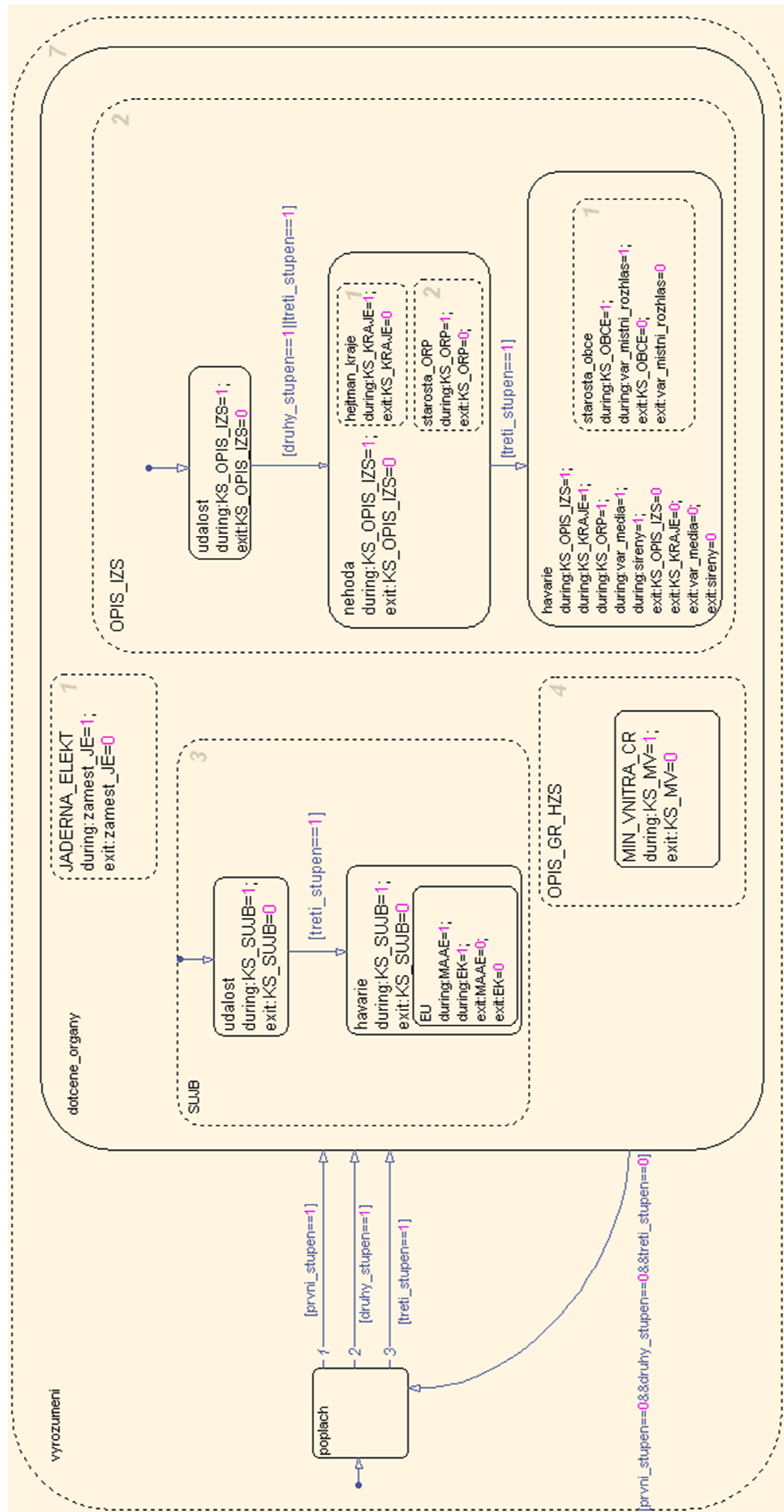
Stav udalost jakmile je aktivní je prováděna průběžná aktivita KS\_SUJB=1, v modelu Simulink zastoupena blokem display krizovy stab SUJB.

Stav havarie je aktivní po splnění podmínky přechodu a jsou zde provedeny shodné aktivity jako ve stavu udalost. Potomek stavu havarie stav



EU po své aktivaci provádí aktivity MAAE=1 a EK=1, zobrazované na display zprava MAAE a zprava EK.

- \* **Stav OPIS\_GR\_HZS** – Poslední, čtvrtý z podstavů rodiče dotcene\_organy je stav OPIS\_GR\_HZS. Zde je vnořen další stav MIN\_VNITRA\_CR, který pokud je aktivní provádí aktivitu KS\_MV=1 zobrazovanou na display krizovy stab min. vnitra.

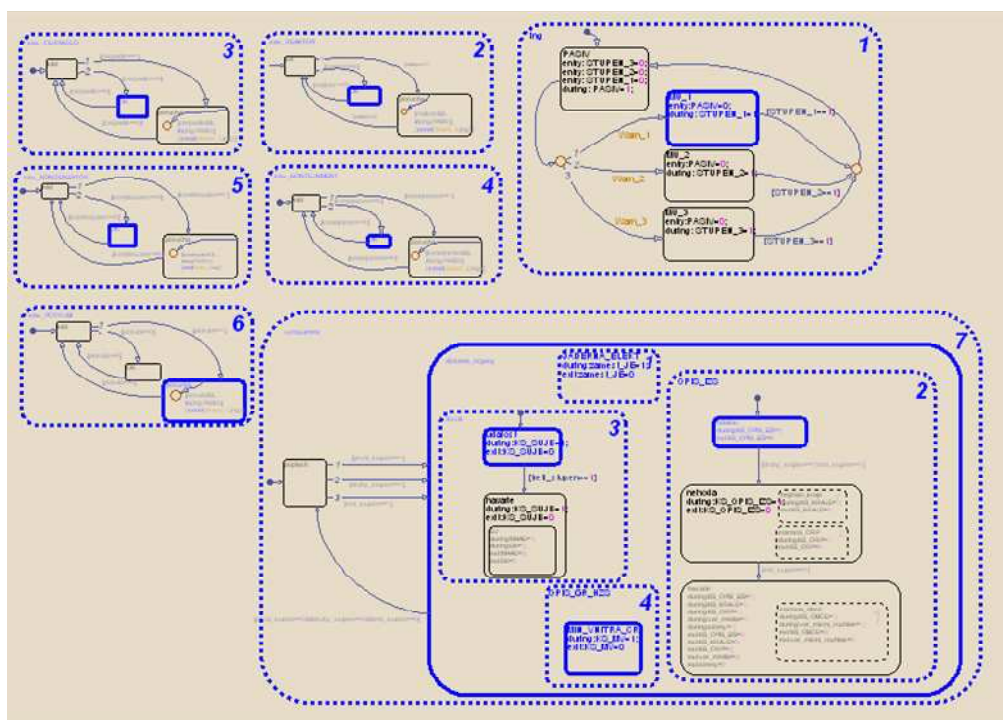


Obrázek 25 - Stav vyrozumeni [vlastní]

### 4.3.2 Realizace modelu

Pro zobrazení funkčnosti celého modelu byl vytvořen obrazový záznam v podobě téměř tří minutového videa, kde je znázorněna simulace jednotlivých situací modelu. Toto video je uloženo na příloženém CD.

Záznam zobrazuje algoritmus vytvořeného modelu. V levé polovině videa je celý model v prostředí Simulinku a v pravé polovině jsou zaznamenány všechny grafické objekty stavového automatu Stateflow. Postupně pak dochází k simulacím poruch na jednotlivých zařízeních jaderné elektrárny. Z činnosti modelu je patrné, že ve stavovém automatu nejprve dojde k zaktivnění všech sedmi hlavních stavů a jejich exkluzivních podstavů, do nichž vstupuje implicitní přechod. Automat je poté ve výchozí pozici připraven na přijetí událostí.

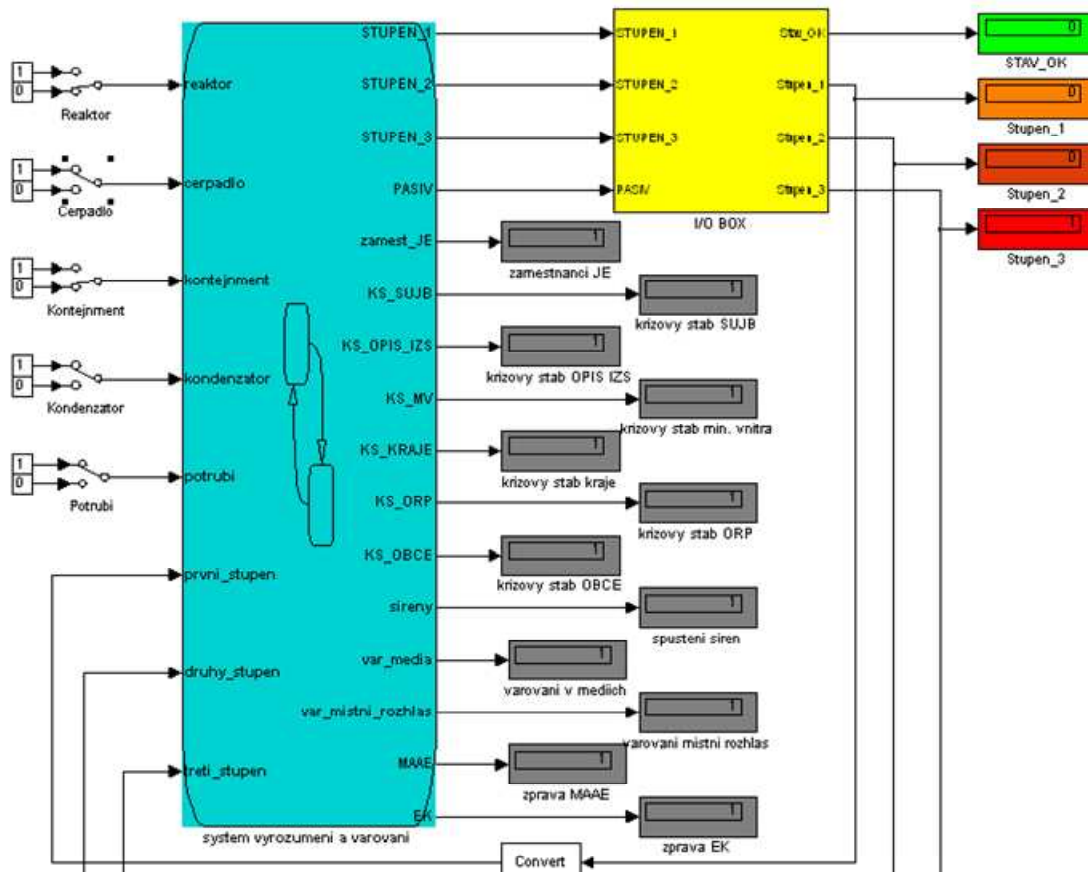


Obrázek 26 - Porucha potrubí [vlastní]

V první fázi simulace je vytvořena porucha na vstupu Potrubí viz. Obrázek 26. Ve stavovém diagramu se tato porucha projeví, neustálým vysíláním události Warn\_1 stavu ing (číslo 1). Stav ing, na základě této události, provádí v podstavu aktivitu STUPEN\_1=1, což se projeví na display jako informace o mimořádné události prvního stupně. Tato podmínka poté zpřístupní i první přechod ve stavu vyrozumění a dojde

k aktivaci příslušných podstavů a následnému provedení průběžných aktivit. Kdy se přenastavují výstupní hodnoty automatu zamest\_JE, KS\_SUJB, KS\_OPIS\_IZS a KS\_MV z 0 na 1. Na Obrázku 26 jsou všechny aktivní stavy při poruše potrubí zvýrazněny modře.

V případě, že dojde k rozšíření poruchy na kondenzátor, proběhne rekvalifikace MU a bloking provede v podstavu průběžnou aktivitu STUPEN\_2=1. Následně budou po převedení výstupního pulzního signálu na prostou 1, postupně zaktivněny přechody ve stavu vyrozumění nesoucí podmínku [druhy\_stupen==1]. Tudiž ve stavu OPIS\_IZS bude aktivní stav nehoda i se všemi svými paralelními potomky. Všechny aktivní stavy budou provádět průběžnou aktivitu, což má za následek nastavení daných výstupních hodnot na 1.



Obrázek 27 - Mimořádná událost 3. stupně [vlastní]

Další změnou na modelu byla simulace poruchy i na čerpadle. V tento moment je ze stavu stav\_CERPADLO vyslána varovná událost do stavu ing.PASIV. Zde je zaktivněn přechod do stavu MU\_3 a provedena aktivita stavu STUPEN\_3=1. Tento výstupní signál se po úpravě objeví na vstupu automatu a zpřístupní tak třetí přechod ve stavu vyrozumění. Platná podmínka [treti\_stupen==1] přesune aktivitu ve stavu OPIS\_IZS ze stavu nehoda

do stavu havarie a stejně tak i ve stavu SUJB. Všechny tyto aktivní podstavy stavu `dotcene_organy` provádí průběžnou aktivitu, která je zaznamenána na display. Porucha na čerpadle je klasifikována jako mimořádná událost 3. stupně, tudíž je na všech display týkajících se dotčených orgánů zobrazena jednička, šedé display na Obrázku 27.

Poté byly simulovány postupné opravy na zařízeních, kdy první ukončení poruchového stavu proběhlo na vstupu potrubí, a následně na kondenzátoru nakonec bylo opraveno i čerpadlo. Tato simulace dobře zachycuje prioritu jednotlivých událostí. Ačkoli došlo k postupné deaktivaci vstupů potrubí a kondenzátor, na výstupních hodnotách se nic neměnilo, protože porucha na čerpadle vyvolá MU 3. stupně, která je dvěma nižším mimořádným událostem nadřazena. Až ve chvíli, kdy byl deaktivován i vstup čerpadlo, došlo ke změně na výstupních hodnotách a signalizace bezporuchového chodu elektrárny.

Takto je díky uživatelsky velmi přívětivému prostředí Stateflow možné simulovat veškeré možné kombinace systému varování a vyrozumění při modelování různých poruch na jaderné elektrárně.

## Závěr

Cílem této práce byla tvorba diskrétně událostního modelu z oblasti veřejné správy. Bezpečnost jaderných elektráren je aktuálním tématem z prostředí veřejné správy. Tato práce analyzuje mimořádné události na české jaderné elektrárně z pohledu toku informací v případě vzniku nehody.

Po jaderné havárii v japonské elektrárně Fukušima z letošního jara propukla po celém světě debata o bezpečnosti jaderné energetiky. Některé evropské země dokonce ukončili provoz všech svých jaderných elektráren. V celé Evropské unii a některých okolních státech probíhají jejich rozsáhlé kontroly. V České republice je oproti ostatním státům EU jen velmi málo odpůrců jaderné energetiky. Dokonce se oproti trendům okolních zemí připravuje rozšíření elektrárny Temelín o dva jaderné bloky. Kontroverze jaderných elektráren plyne z možného nebezpečí šíření radioaktivního záření v případě vzniku nehody. Proto je nezbytné velice obezřetně zajišťovat havarijní připravenost a mít důkladně popsány všechny varianty vzniku a řešení mimořádných událostí na jaderné elektrárně.

Cílem této práce byl návrh a analýza modelu diskrétních událostí, který zachycuje mimořádné události na české jaderné elektrárně z pohledu toku informací v případě vzniku nehody. Klasifikace mimořádných událostí spolu se systémem vyrozumění a varování je v této práci podrobně popsána a následně zpracována v diskrétně událostním modelu.

Pro tvorbu diskrétně událostních modelů bylo vybráno prostředí Stateflow, které je plně integrováno do výpočetního prostředí MATLAB&Simulink. Interakcí nástroje Stateflow a Simulink, byly vytvořeny oba plně funkční modely. Toto uživatelsky velmi přívětivé grafické prostředí bylo před samotnou tvorbou modelů podrobně popsáno.

V práci byl vytvořen standardní příklad diskrétně událostního modelu, kterým je elektronický zabezpečovací systém. Stavový automat demonstruje návrh chování bezpečnostního systému domu. Na tom to modelu byly ujasněny základní principy a pojmy teorie stavových automatů.

Výsledný model klasifikace událostí a systému vyrozumění a varování, může sloužit jako předloha pro řešení krizových situací na jaderné elektrárně. Díky modelu může být dále

celý reálný systém klasifikace událostí a systém vyrozumění a varování upraven, zefektivněn a odladěn tak, aby při reálné nehodě nedošlo k selhání jednotlivých orgánů. Model podrobně zobrazuje toky událostí směrem od zřizovatele jaderné elektrárny, až po konečný článek systému, kterým jsou lidé nacházející se v zóně havarijního plánování. Simulací tohoto diskrétně událostního modelu lze jednoznačně určit, který orgán veřejné správy má být informován v případě vzniku některé z mimořádných událostí na jaderné elektrárně.

Vytvořený model demonstruje přehledné použití hierarchických stavových automatů pro návrh chování diskrétně událostních modelů.

Součástí práce je i přiložené CD s vytvořenými modely a záznamem simulace.

## Použitá literatura

- [1] RÁBOVÁ, Zdeňka; ČEŠKA, Milan; ZENDULKA, Jaroslav. *Modelování a simulace*. první. Praha : Státní nakladatelství technické literatury, 1982. 337 s.
- [2] KŮS, Zdeněk; GLOMBÍKOVÁ, Viera; HALASOVÁ, Andrea. *Simulace výrobních systémů : díl 1.* první. Liberec : Technická univerzita v Liberci, 2002. 125 s. ISBN 80-7083-642-3.
- [3] PERINGER, Petr. *Modelování a simulace* [online]. 3.11.2010 [cit. 2010-10-22]. IMS. Dostupné z WWW: <<http://www.fit.vutbr.cz/study/courses/IMS/public/prednasky/IMS.pdf>>.
- [4] SLAVÍČEK, Pavel. *DISCRETE EVENT SYSTEM SPECIFICATION – DEVS*. [s.l.], 2003. 3 s. Dostupné z WWW: <[http://www.feec.vutbr.cz/EEICT/2003/fsbornik/02-Mgr/09-Computer\\_Intelligent\\_and\\_Graphic\\_Systems/08-slavicek\\_pavel.pdf](http://www.feec.vutbr.cz/EEICT/2003/fsbornik/02-Mgr/09-Computer_Intelligent_and_Graphic_Systems/08-slavicek_pavel.pdf)>.
- [5] CASSANDRAS, Christos G.; LAFORTUNE, Stéphane. *Introduction to Discrete Event System*. Second Edition. United States of America : Springer , 2008. 769 s. ISBN 978-0-387-33332-8.
- [6] KŘIVÝ, Ivan; KINDLER, Evžen. *Simulace a modelování*. [Skritum] Ostrava : Ostravská univerzita, 2001. 146 s. Dostupné z WWW: <<http://prf.osu.cz/kip/dokumenty/Msm.pdf>>.
- [7] *Úvod do objektově orientovaného programování v jazyce SIMULA* [online]. [cit. 2010-10-24]. Dostupné z WWW: <<http://oopsimula.sweb.cz/>>.
- [8] *Technical Computing, Control Engineering, Simulations / Humusoft* [online]. 1991 - 2011 [cit. 2010-10-24]. Dostupné z WWW: <<http://www.humusoft.cz/>>.
- [9] *Stateflow and Stateflow Coder : User's Guide*. Version 5. [s.l.] : The MathWorks, Inc., July 2002. Dostupné z WWW: <[http://www.mathworks.com/help/releases/R13sp2/pdf\\_doc/stateflow/sf\\_ug.pdf](http://www.mathworks.com/help/releases/R13sp2/pdf_doc/stateflow/sf_ug.pdf)>.
- [10] STODŮLKA, Petr. *Vývojový nástroj pro návrh a testování komunikujících stavových automatů*. Praha, 2004. 79 s. Diplomová práce. Karlova Univerzita, Matematicko-Fyzikální fakulta, Katedra softwarového inženýrství. Dostupné z WWW: <<http://patf-biokyb.lf1.cuni.cz/projects/statecharts/diplomka.pdf>>.



- [11] KOFRÁNEK, Jiří. *Hierarchické komunikující stavové automaty*. Praha, 18 s. Oborová práce. 1. LF UK. Dostupné z WWW: <patf-biokyb.lf1.cuni.cz/wiki/\_media/.../kofranek\_stodulka\_2004.doc>.
- [12] *Přednášky: 6 Stavové automaty* [online]. [cit. 2011-04-09]. Dostupné z WWW: <[http://www.urel.feec.vutbr.cz/~kolouch/pld/1\\_prednasky/kapitola06.html](http://www.urel.feec.vutbr.cz/~kolouch/pld/1_prednasky/kapitola06.html)>.
- [13] *Jaderná energetika / Výroba elektřiny / Skupina ČEZ* [online]. 2011 [cit. 2011-04-16]. Dostupné z WWW: <<http://www.cez.cz/cs/vyroba-elektriny/jaderna-energetika.html>>.
- [14] *Příručka pro ochranu obyvatelstva v případě radiační havárie JE Temelín s kalendářem*. 39 s. Dostupné z WWW: <<http://www.cez.cz/edee/content/file/energie-a-zivotni-prostredi/temelin/ekalete.pdf>>.
- [15] Česká republika. Vyhláška č. 318/2002 Sb., o podrobnostech k zajištění havarijní připravenosti jaderných zařízení a pracovišť se zdroji ionizujícího záření a o požadavcích na obsah vnitřního havarijního plánu a havarijního řádu, ve znění vyhlášky č. 2/2004 Sb.. In *SBÍRKA ZÁKONŮ ročník 2002*. 2002, částka 116, s. 6780 - 6788. Dostupný také z WWW: <[http://www.sujb.cz/docs/v318\\_02\\_zmeny.pdf](http://www.sujb.cz/docs/v318_02_zmeny.pdf)>.
- [16] *SÚJB - úvodní stránka* [online]. 1997 [cit. 2011-04-16]. Dostupné z WWW: <<http://www.sujb.cz/>>.
- [17] *Vícestupňové cvičení orgánů krizového řízení ZÓNA 2002 : příručka pro účastníky*. Praha : Ministerstvo vnitra České republiky, 2002. 24 s. Dostupné z WWW: <http://aplikace.mvcr.cz/archiv2008/hasici/aktualit/2002/zona02/prirucka.html>.

# Seznam příloh

PŘÍLOHA Č. 1	POPIS GRAFICKÉHO PROSTŘEDÍ STATEFLOW.....	II
PŘÍLOHA Č. 2	STATEFLOW MODEL – SYSTEM VYROZUMENI A VAROVANI.....	IV

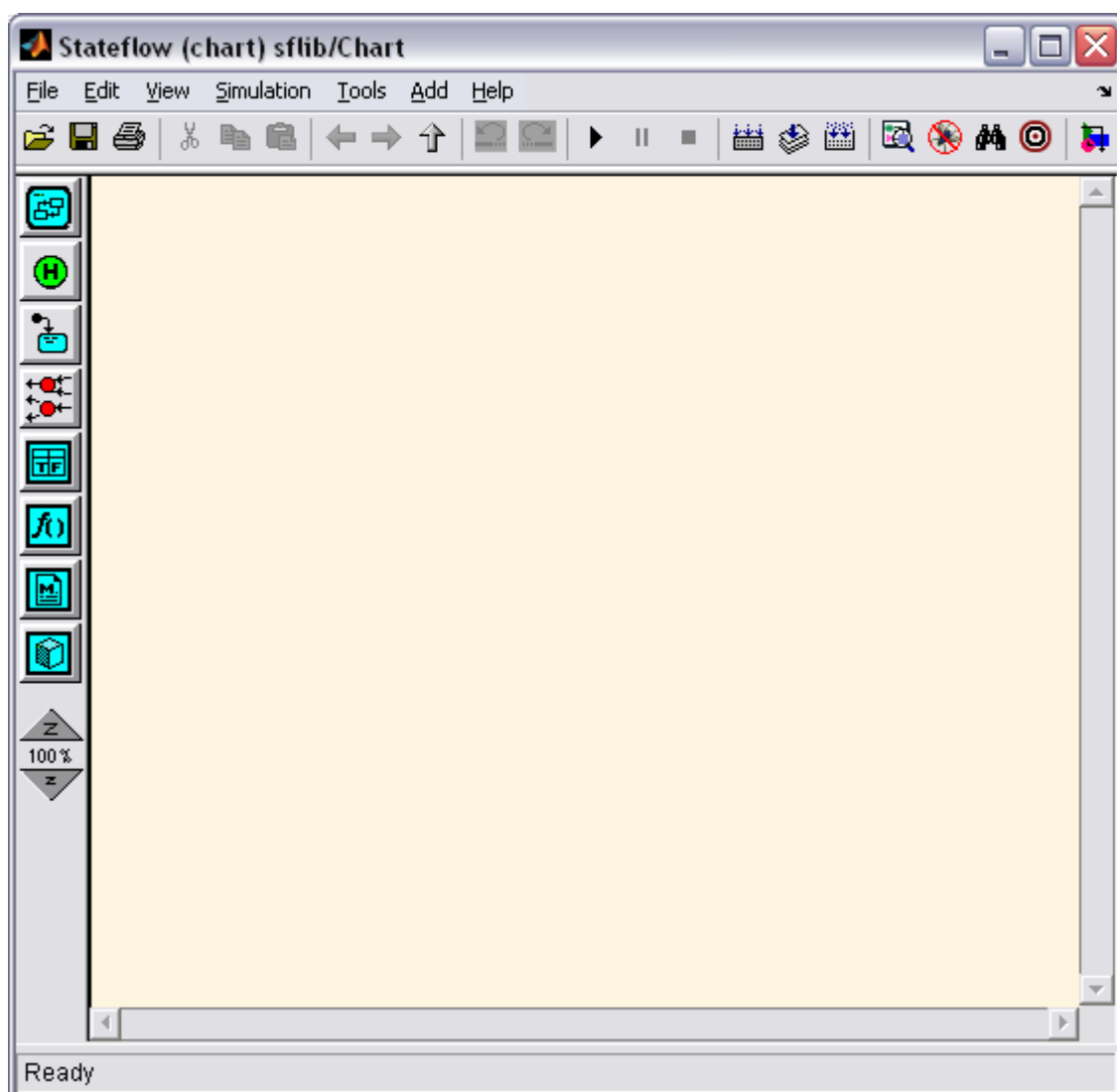
## Příloha č. 1 Popis grafického prostředí Stateflow


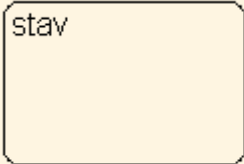







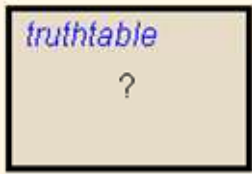

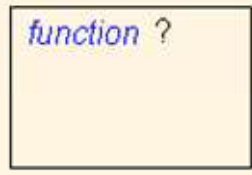

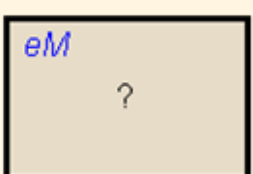


Při tvorbě modelů byl využit programu MATLAB verze 7.2 (R2006a) Simulink 6.4 a Stateflow 6.4.

Pro uložení a následné otevření modelu Stateflow je třeba nastavit kódování znaků programu MATLAB, aby bylo kompatibilní s vytvořeným modelem v prostředí Stateflow. To zajišťuje příkaz

```
bdclose all; set_param(0,'CharacterEncoding', 'windows-1252'),
```

vepsaný do příkazového řádku (Command Window) na základní obrazovce MATLABU. Před samotným nastavením kompatibility znaků je nezbytné uzavřít všechny otevřené modely a knihovny. Což zajišťuje první část příkazového řádku `bdclose all`.



		<b>Stav</b>
		<b>Historie</b>
		<b>Implicitní přechod</b>
		<b>Spojka</b>
		<b>Pravdivostní tabulka</b> Umožňuje zapsat rozhodovací logiku pravdivostní tabulky přímo do prostředí Stateflow. Pro logické chování jsou pravdivostní tabulky jednoduché k zápisu programu, přehledné a snadno čitelné.
		<b>Funkce</b> Grafická funkce poskytuje jednoduchý zápis a možnost umístění funkce přímo v modelu Stateflow
		<b>Vložená funkce z MATLABU</b> Využívá možnosti vložit a propojit funkci zapsanou přímo v MATLABU. MATLAB poskytuje bohatší možnosti zápisu funkce.
		<b>Box</b> Boxy se využívají k přehlednější organizaci Stateflow diagramu.

Příloha č. 2 Stateflow model – system vyzozumeni a varovani

