VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV AUTOMATIZACE A MĚŘICÍ TECHNIKY

DEPARTMENT OF CONTROL AND INSTRUMENTATION

INFORMAČNÍ SYSTÉM IDENTIFIKACE BEZPEČNOSTNÍCH SYSTÉMŮ PODLE ČSN EN ISO 12100:2011

INFORMATION SYSTEM FOR ASSESSMENT OF SAFETY SYSTEMS ACCORDING TO ČSN EN ISO 12100:2011

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

AUTOR PRÁCE — Jakub Franka

AUTHOR

VEDOUCÍ PRÁCE — Ing. Radovan Holek, CSc.

SUPERVISOR

BRNO 2022

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní program **Automatizační a měřicí technika**

Ústav automatizace a měřicí techniky

Student: Jakub Franka ***ID:*** 220976

Ročník: 3 ***Akademický rok:*** 2021/22

NÁZEV TÉMATU:

Informační systém identifikace bezpečnostních systémů podle ČSN EN ISO 12100:2011

POKYNY PRO VYPRACOVÁNÍ:

1. Seznamte se a popište legislativu posouzení rizik strojních zařízení dle podle ČSN EN ISO 12100:2011.
2. Navrhněte datový a procesní model pro informační systém. Navrhněte webový informační systém pro sběr bezpečnostních parametrů pro další vyhodnocování bezpečnostních systémů.
3. Realizujte informační systém na platformě C# a databázi MSSQL se zaměřením na konfigurovatelnost procesů.
3. Ověřte chování systému při sběru a vyhodnocování bezpečnostních parametrů a vyhodnocování bezpečnostních systémů.

DOPORUČENÁ LITERATURA:

Safebook 5. Principles of Machine Safety – Legislation, Theory and Practice. Rockwell Automation. 2016. 145 s.
RÁČEK, J. Strukturovaná analýza systémů. 1.vyd. Brno Masarykova univerzita. 2006. 103 s. ISBN 80-2010-4190-

Termín zadání: 7.2.2022 ***Termín odevzdání:*** 23.5.2022

Vedoucí práce: Ing. Radovan Holek, CSc.

doc. Ing. Václav Jirsík, CSc.
předseda rady studijního programu

Abstrakt

Táto práca je zameraná na návrh a implementáciu informačného systému určeného k uľahčeniu práce pri návrhu bezpečnostných systémov strojných zariadení. Práca sa venuje návrhu dátového modelu, serverovej a klientskej časti aplikácie a užívateľského rozhrania so zameraním na konfigurovateľnosť. Návrh systému vychádza z noriem EN ISO 13849-1 a IEC/EN 62061.

Klíčová slova

Bezpečnostné systémy, bezpečnosť strojných zariadení, informačný systém, úroveň vlastnosti, úroveň integrity bezpečnosti

Abstract

This thesis is focused on the design and implementation of an information system intended for simplifying work with machine safety systems. It addresses design of the data model, server and client parts of the app and user interface with focus on customizability. The design of the system is based on the norms EN ISO 13849-1 and IEC/EN 62061.

Keywords

Safety systems, machine safety, information system, performance level, safety integrity level

Bibliografická citace

FRANKA, Jakub. Informační systém identifikace bezpečnostních systémů podle ČSN EN ISO 12100:2011. Brno, 2022. Dostupné také z: https://www.vutbr.cz/studenti/zav-prace/detail/142709. Bakalářská práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav automatizace a měřicí techniky. Vedoucí práce Radovan Holek.

Prohlášení autora o původnosti díla

Jméno a příjmení studenta:	*Jakub Franka*
VUT ID studenta:	*220976*
Typ práce:	*Bakalářská práce*
Akademický rok:	*2021/22*
Téma závěrečné práce:	*Informační systém identifikace bezpečnostních systémů podle ČSN EN ISO 12100:2011*

Prohlašuji, že svou závěrečnou práci jsem vypracoval samostatně pod vedením vedoucí/ho závěrečné práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené závěrečné práce dále prohlašuji, že v souvislosti s vytvořením této závěrečné práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

.

V Brně dne: 23.května 2022 ----------

podpis autora

Poděkování

Ďakujem vedúcemu práce Ing. Radovan Holek, CSc. za ochotu a čas mne venovaný pri konzultáciách a tvorbe tejto práce.

V Brně dne: 23.května 2022 ----------

podpis autora

Obsah

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

Úvod

Návrh bezpečnostných systémov je nevyhnutnou súčasťou návrhu a výroby akéhokoľvek potenciálne nebezpečného strojného zariadenia. Komplexnosť návrhu bezpečnostného systému stúpa s požiadavkami na úroveň bezpečnosti a schopnosti systému odolávať poruchám.

Vzhľadom na komplikované požiadavky pri návrhu bezpečnostných systémov na znalosť a dodržiavanie noriem a vykonávanie výpočtov, často z veľkým množstvom dát (pri zložitých strojných zariadeniach), je veľkou výhodou možnosť využitia software určeného na zjednodušenie tohto návrhu. Je nutné zamedziť ľudským chybám pri vykonávaní výpočtov, nakoľko akákoľvek chyba môže mať pri poruche vážne následky.

Pri návrhu bezpečnostného systému je tiež nutné správne voliť jeho súčasti tak aby bolo dostatočne znížené riziko ktorému sú ľudia pri používaní strojného zariadenia vystavení. Aj s touto problematikou môže pomáhať software, ktorý navrhne vyhovujúci prvok pre určité použitie.

Prvá časť tejto práce sa zaoberá zhrnutím obsahu dôležitých noriem týkajúcich sa návrhu bezpečnostných systémov. Popisuje postupy, výpočty a parametre definované týmito normami pri návrhu bezpečnostných systémov s ktorými musí navrhovaný informačný systém pracovať.

V druhej časti je popísaný návrh informačného systému a požiadavky na jeho funkciu. Je opísaný dátový model a jeho časti, použité frameworky, navrhnuté formuláre, navigácia medzi nimi a špecifické ovládacie prvky navrhnuté na konkrétnu aplikáciu. Tiež je popísaný postup pri zadávaní údajov do systému a algoritmus s akým systém vykonáva výpočty so zadanými dátami. Keďže systém je určený k výpočtom podľa dvoch rôznych postupov definovaných v normách, je nutné aby dátový model umožňoval ukladať dáta pre výpočty podľa obidvoch metodík. Súčasťou popisu dátového modelu je popis možností konfigurácie systému, teda užívateľských práv, prístupu k ovládacím prvkom formuláru podľa stavu záznamu a doménového číselníku ako náhrady samostatných číselníkov.

1. BEZPEČNOSŤ STROJNÝCH ZARIADENÍ

1.1 Norma EN ISO 12100

EN ISO 12100 je medzinárodná norma špecifikujúca terminológiu a metodológiu týkajúcu sa bezpečnosti strojných zariadení. Obsahuje zásady a postupy posudzovania a znižovania rizika založené na skúsenostiach z konštrukcie, používania a rizík u strojných zariadeniach. Slúži na uľahčenie práce konštruktérov pri návrhu a dokumentácii strojných zariadení.

Slúži tiež ako základ pre tvorbu ďalších noriem, podľa štruktúry [podľa EN ISO 12100]:

A. Základné bezpečnostné normy – základné pojmy, zásady pre konštrukciu, všeobecné normy uplatniteľné na všetky strojné zariadenia
B. Skupinové bezpečnostné normy – jedno bezpečnostné hľadisko (B1) / typ bezpečnostného zariadenia (B2), použiteľné na väčší počet strojných zariadení.
C. Bezpečnostné normy pre stroje – detailné bezpečnostné požiadavky pre jednotlivý stroj / skupinu strojov

Norma definuje stratégiu pri posúdení a znížení rizika ako radu logických krokov umožňujúcich analýzu a zhodnotenie rizík spojených s daným strojným zariadením, pričom ak je to nutné po posúdení rizika nasleduje jeho zníženie [podľa EN ISO 12100]:

a) určenie medzných hodnôt a hraníc stroja – určenie prístupových bodov pri bežnom predpokladanom používaní stroja aj predvídateľnom nesprávnom použití.
b) identifikácia nebezpečných situácií
c) odhad rizika a nebezpečenstva pre každú nebezpečnú situáciu
d) zhodnotenie rizika a rozhodnutie o nutnosti jeho zníženia
e) vylúčenie alebo zníženie rizika pomocou ochranných opatrení

Tento postup je iteratívny a na dostatočné zníženie rizika môže byť nutné ho použiť niekoľko krát za sebou. Pri vykonávaní tohto postupu je nutné dbať na nižšie uvedené štyri faktory, prednostne v uvedenom poradí.

1) bezpečnosť stroja počas všetkých fáz jeho životnosti
2) schopnosť stroja vykonávať funkciu
3) použiteľnosť stroja
4) náklady na výrobu, prevádzku a vyradenie stroja

Norma ďalej podrobne popisuje postup pri jednotlivých krokoch posúdenia a zhodnotenia rizika.

a) Určenie medzných hodnôt strojného zariadenia
    - Vymedzenie používania
        - Predpokladané používanie a predvídateľné nesprávne použitie
        - Prevádzkové režimy a postupy zásahov užívateľa
        - Osoby používajúce zariadenie (pohlavie, vek, pravá/ľavá ruka, obmedzené fyzické schopnosti, úroveň zácviku)
    - Vymedzenie priestoru
        - Rozsah pohybu
        - Prevádzka a údržba
    - Vymedzenie doby
        - Životnosť zariadenia
        - Intervaly údržby
    - Ostatné
        - Spracovaný materiál / materiály
        - Udržovateľnosť
        - Prostredie (napr. min. a max. teplota)

b) Identifikácia nebezpečenstva

    Pre posúdenie rizika u každého stroja je dôležitá systematická identifikácia predvídateľných nebezpečí
        - Pri doprave, montáži a inštalácií
        - Pri sprevádzkovaní
        - Počas používania
        - Pri demontáži a likvidácií
    - Vzájomné pôsobenie človeka a stroja počas životného cyklu stroja
    - Možné stavy stroja
        - Vykonáva predpokladanú funkciu – normálna prevádzka
        - Nevykonáva predpokladanú funkciu – zlyhanie
    - Nepredpokladané chovanie obsluhy / predvídateľné zlyhanie stroja

c) Odhad rizika
    - Pre každú nebezpečnú situáciu je nutné vykonať odhad rizika určením prvkov rizika
        - Riziko spojené s určitou nebezpečnou situáciou závisí na závažnosti a pravdepodobnosti úrazu

d) Zhodnotenie rizika
    - Musí byť vykonané aby bolo možné určiť či je nutné znižovanie rizika.

e) Zníženie rizika
    - Dosahuje sa vylúčením nebezpečenstva alebo znížením závažnosti aj pravdepodobnosti výskytu úrazu
        - Zabudovanými bezpečnostnými opatreniami
        - Bezpečnostnou ochranou

Normy IEC/EN 62061 a (EN) ISO 13849-1 sa zaoberajú elektrickými bezpečnostnými systémami. Použitie obidvoch noriem má porovnateľné výsledky a obidve sú harmonizované podľa európskej smernice pre strojné zariadenia. Rozdiel medzi nimi je v použitých. Použitie jednej alebo druhej normy záleží na užívateľovi, pričom norma IEC/EN 62061 je určená pre komplexnejšie bezpečnostné funkcie a je vhodnejšia na elektrické systémy, zatiaľ čo norma (EN) ISO 13849-1 poskytuje jednoduchší postup pre konvenčnejšie systémy a je použiteľná na pneumatické, hydraulické, mechanické aj elektrické systémy.

1.2 (EN) ISO 13849-1

Norma (EN) ISO 13849-1 popisuje požiadavky na bezpečnostné systémy a ich komponenty:

- Architektúra systému
- Spoľahlivostné údaje prvkov systému
- Diagnostické pokrytie (DC) systému
- Ochrana proti zlyhaniu so spoločnou príčinou
- Ochrana proti systematickému zlyhaniu
- Software

Pre použitie tejto normy je potrebné najprv vykonať analýzu rizík podľa EN ISO 12100.

Výstupom (EN) ISO 13849-1 je úroveň vlastností (PL) a, b, c, d, alebo e. PL určuje schopnosť komponentov bezpečnostného systému vykonávať ich funkciu. Aby bolo možné prehlásiť úroveň vlastností za systém je treba najprv splniť požiadavky ktoré norma (EN) ISO 13849-1 popisuje.

Úroveň PL je možné určiť z:

- Strednej doby do nebezpečného zlyhania (Mean Time to Dangerous Failure, $MTTF_D$)
- Diagnostického pokrytia (Diagnostic Coverage, DC)
- Architektúry systému

Úroveň PL bezpečnostnej funkcie musí dosiahnuť minimálne požadovanú úroveň vlastností (PL_r). PL_r je určené podľa grafu rizík (tabuľka 1) ktorého vstupmi sú závažnosť potenciálneho zranenia, frekvencia výskytu rizika a možnosť jeho vylúčenia [1].

Tabuľka 1 Určenie úrovne PL_r [1]

<table>
<tr><td>A</td><td colspan="2">b</td><td colspan="2">c</td><td colspan="2">d</td><td>e</td></tr>
<tr><td>P1</td><td>P2</td><td>P1</td><td>P2</td><td>P1</td><td>P2</td><td>P1</td><td>P2</td></tr>
<tr><td colspan="2">F1</td><td colspan="2">F2</td><td colspan="2">F3</td><td colspan="2">F4</td></tr>
<tr><td colspan="4">S1</td><td colspan="4">S2</td></tr>
<tr><td colspan="8">↑ ŠTART ↑</td></tr>
</table>

Systém je možno rozdeliť na jeho komponenty (subsystémy), väčšinou na vstupný, logický, výstupný subsystém a subsystémy realizujúce komunikáciu medzi nimi. Každý systém nemusí obsahovať všetky typy subsystémov. Zloženie systému so subsystémov a jeho diagnostické pokrytie určuje jeho kategóriu architektúry (B/1/2/3/4).

Na výpočet úrovne PL dosiahnutej bezpečnostným systémom využíva norma (EN) ISO 13849-1 kvantitatívne údaje o spoľahlivosti (podľa tabuľky 2). Základným typom týchto údajov je pravdepodobnosť nebezpečnej poruchy za hodinu (Probability of Failure per Hour, PFH_D). Rovnaký údaj používa aj norma IEC/EN 62061 [1].

Tabuľka 2 Určenie PL podľa PFH_D [1]

PL	PFH_D
a	$\geq 10^{-5}$ .. $<10^{-4}$
b	$\geq 3\times10^{-6}$ .. $<10^{-5}$
c	$\geq 10^{-6}$ .. 3×10^{-6}
d	$\geq 10^{-7}$ .. 10^{-6}
e	$\geq 10^{-8}$ .. 10^{-7}

Ak nie je údaj PFH_D k dispozícii, je možné určiť počítať so strednou dobou do nebezpečnej poruchy ($MTTF_D$). Tento údaj sa určuje pre jeden kanál systému alebo subsystému ako priemer $MTTF_D$ komponentov kanálu podľa vzorca [1]

$$\frac{1}{MTTF_D} = \sum_{i=1}^{N} \frac{1}{MTTF_{Di}} = \sum_{j=1}^{N} \frac{nj}{MTTF_{Dj}}. \quad (1)$$

Pre väčšinu dvojkanálových systémov je $MTTF_D$ rovnaké pre obidva kanály, výsledok teda platí pre každý kanál. Norma obsahuje aj vzorec pre prípad že sú kanály rôzne [1]:

$$MTTF_D = \frac{2}{3}\left[MTTF_{dC1} + MTTF_{dC2} - \frac{1}{\frac{1}{MTTF_{dC1}}+\frac{1}{MTTF_{dC2}}}\right]. \quad (2)$$

Norma rozdeľuje hodnoty MTTFD na nízku, strednú a vysokú úroveň podľa tabuľky 3.

Tabuľka 3 Úrovne $MTTF_D$ [1]

Označenie $MTTF_D$ pre každý kanál	Rozsah MTF_D
nízka	3 roky ≤ MTTFD < 10 rokov
stredná	10 rokov ≤ MTTFD < 30 rokov
vysoká	30 rokov ≤ MTTFD < 100 rokov

Niektoré kategórie architektúry systémov vyžadujú určitú formu diagnostického testovania funkčnosti bezpečnostnej funkcie. Účinnosť tohto testovania popisuje diagnostické pokrytie (Diagnostic Coverage, DC). Ako označenie miery zlyhania sa používa znak λ. Rozlišujú sa dva typy nebezpečného zlyhania [1].

- Nebezpečné detegované zlyhanie (λdd) – porucha ktorá môže spôsobiť stratu bezpečnostnej funkcie ale je odhalená testom. Po zachytení poruchy musí systém prejsť do bezpečného stavu.
- Nebezpečné zlyhanie (λd) – akákoľvek porucha ktorá môže spôsobiť stratu bezpečnostnej funkcie.

Hodnota DC sa vyjadruje v percentách podľa vzorca: $DC = \frac{\lambda dd}{\lambda d}$ (3) a rozdeľuje sa do úrovní podľa tabuľky 4.

Tabuľka 4 Úrovne DC [1]

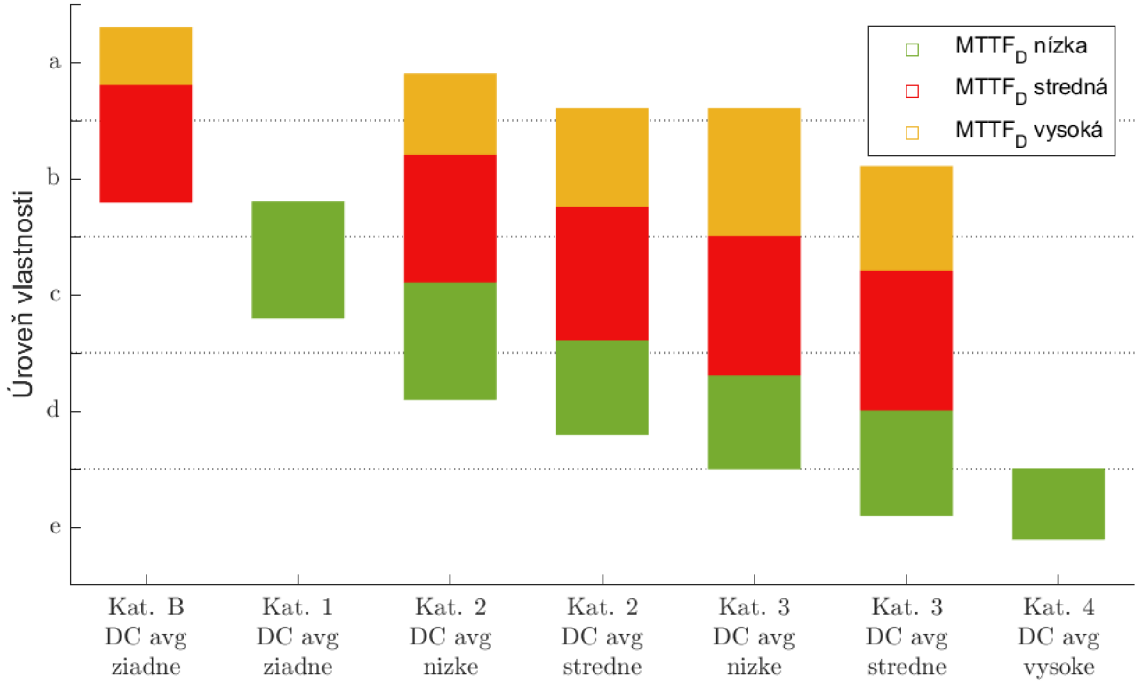
Označenie DC	Rozsah DC
žiadne	DC < 60%
nízke	60% ≥ DC < 90%
stredné	90% ≥ DC < 99%
vysoké	99% ≥ DC

Pri dvojkanálových systémoch môže dôjsť k poruche obidvoch kanálov spôsobenej jednou udalosťou, napríklad zlyhanie jedného komponentu, teda k zlyhaniu so spoločnou príčinou (Common Cause Failure, CCF). Stupeň náchylnosti k CCF sa označuje ako β faktor. Norma (EN) ISO 13849-1 definuje opatrenia proti CCF a ich hodnotenie (tabuľka 5).

Tabuľka 5 Hodnotenie opatrení proti CCF [1]

Opatrenie proti CCF	Hodnotenie
Separácia/segregácia	15
Rôznosť	20
Návrh/aplikácia/skúsenosti	20
Posúdenie/analýza	5
Kompetencia/školenie	5
Okolné prostredie	35

Dosiahnutú úroveň PL je možné určiť podľa grafu (obrázok 1) alebo priamo z údaju PFH_D. Norma v prílohe obsahuje aj číselné vyjadrenie tohto grafu. Ku splneniu požadovanej úrovne PL musia byť do úvahy vzaté aj opatrenia proti zlyhaniu so spoločnou príčinou a systematickému zlyhaniu.



Obrázok 1 Určenie hodnoty PL [1]

Subsystémy splňujúce určitú úroveň vlastností je možné skombinovať do systému s výslednou hodnotou PL podľa tabuľky 6.

Tabuľka 6 Výsledná hodnota PL kombinácie subsystémov [1]

PL_{low}	N_{low}	PL
a	> 3	nepovolené
	≤ 3	a
b	> 2	a
	≤ 2	b
c	> 2	b
	≤ 2	c
d	> 3	c
	≤ 3	d
e	> 3	d
	≤ 3	e

1.3 Norma IEC/EN 62061

Norma IEC/EN 62061 obsahuje požiadavky aplikovateľné na návrh elektrických bezpečnostných riadiacich systémov, subsystémov a zariadení. Požiadavky na bezpečnostné riadiace funkcie zahrnujú:

- Požiadavky na funkčnosť
- Požiadavky na bezpečnostnú integritu

Údaje o frekvencii prevádzky, požadovanom čase odozvy, režimoch prevádzky, pracovných cykloch, prostredí a funkciách reagujúcich na poruchu sú zahrnuté v požiadavkách na funkčnosť.

Požiadavky na bezpečnostnú integritu sú určené v úrovniach (Safety Integrity Level, SIL). Aby systém spĺňal určitú úroveň SIL, musia byť zvážené niektoré alebo všetky prvky z tabuľky 7 podľa zložitosti systému [2].

Tabuľka 7 Požiadavky na úroveň SIL [2]

Prvky potrebné k určeniu úrovne SIL	Skratka
Pravdepodobnosť nebezpečnej poruchy za hodinu	PFH_D
Tolerancia poruchy hardware	HFT
Podiel bezpečných porúch	SFF
Interval kontrolného testu	T_1
Interval diagnostického testu	T_2
Tendencia k zlyhaniu so spoločnou príčinou	β
Diagnostické pokrytie	DC

Norma IEC/EN 62061 definuje subsystém ako časť systému ktorej zlyhanie spôsobí zlyhanie celého systému. Redundantné spínače teda netvoria samostatné subsystémy ale jeden subsystém [2].

Na úrovni jednotlivých komponentov využíva rovnaké metódy ako norma (EN) ISO 13849-1. V spôsobe určenia celkovej hodnoty PFH_D sa normy líšia.

Tabuľka 8 Určenie úrovne SIL [2]

SIL	PFH_D
3	$10^{-7} > PFH_D \geq 10^{-8}$
2	$10^{-6} > PFH_D \geq 10^{-7}$
1	$10^{-5} > PFH_D \geq 10^{-6}$

Úroveň bezpečnostnej integrity hardwaru ktorú je možné od systému vyžadovať je obmedzená hodnotou PFH_D, poruchovou toleranciou, a podielom bezpečných zlyhaní systému.

Poruchová tolerancia je schopnosť systému vykonávať svoju funkciu pri určitom počte porúch. Ako podiel nebezpečných porúch sa označuje časť celkovej miery zlyhaní ktorá nespôsobí nebezpečné zlyhanie. Kombináciou týchto parametrov sa určuje SIL Claim Limit (SIL CL) podľa tabuľky 9, čo je obmedzenie najvyššej dosiahnuteľnej úrovne SIL.

Tabuľka 9 Určenie SIL CL [2]

SFF	HFT		
	0	1	2
60% > SFF		SIL 1	SIL 2
90% > SFF ≥ 60%	SIL 1	SIL 2	SIL 3
99% > SFF ≥ 90%	SIL 2	SIL 3	SIL 3
SFF ≥ 99%	SIL 3	SIL 3	SIL 3

2. NÁVRH INFORMAČNÉHO SYSTÉMU

2.1 Dátový model

Táto práca nadväzuje na bakalársku prácu Bc. Samuela Janka [3]. Navrhovaný dátový model je teda upraveným dátovým modelom navrhnutým v jeho práci. Jedným jeho rozšírením je použitie doménového číselníka, čo umožňuje úpravu číselníkov aj vytvorenie nového bez nutnosti vytvorenia novej tabuľky. Ďalej je pridaná možnosť konfigurácie zobrazovania formulárov podľa stavu záznamu a poverení užívateľa.

2.1.1 Hlavná časť dátového modelu

Základ dátového modelu je odvodený od pôvodného, pričom sa miesto odkazov do samostatných číselníkov cez cudzie kľúče používajú odkazy do doménového číselníka a okrem aktuálneho stavu sa tiež ukladá aj budúci stav, teda stav do ktorého užívateľ plánuje záznam previesť. Hlavnú časť dátového modelu tvorí 8 entít znázornených na obrázku 2.

Dáta o strojných zariadeniach na ktorých sa vykonáva bezpečnostná analýza sú uložené v tabuľke *machine*.

Na určenie rozsahu prístupu ku strojnému zariadeniu slúži tabuľka *access_point*, opisujúca prístupové body k strojnému zariadeniu ktoré musia byť ošetrené bezpečnostnými funkciami. K jednému stroju môže existovať viacero prístupových bodov no jeden prístupový bod patrí len jednému stroju, tabuľka *machine* je teda k tabuľke *access_point* vo vzťahu 1:M.

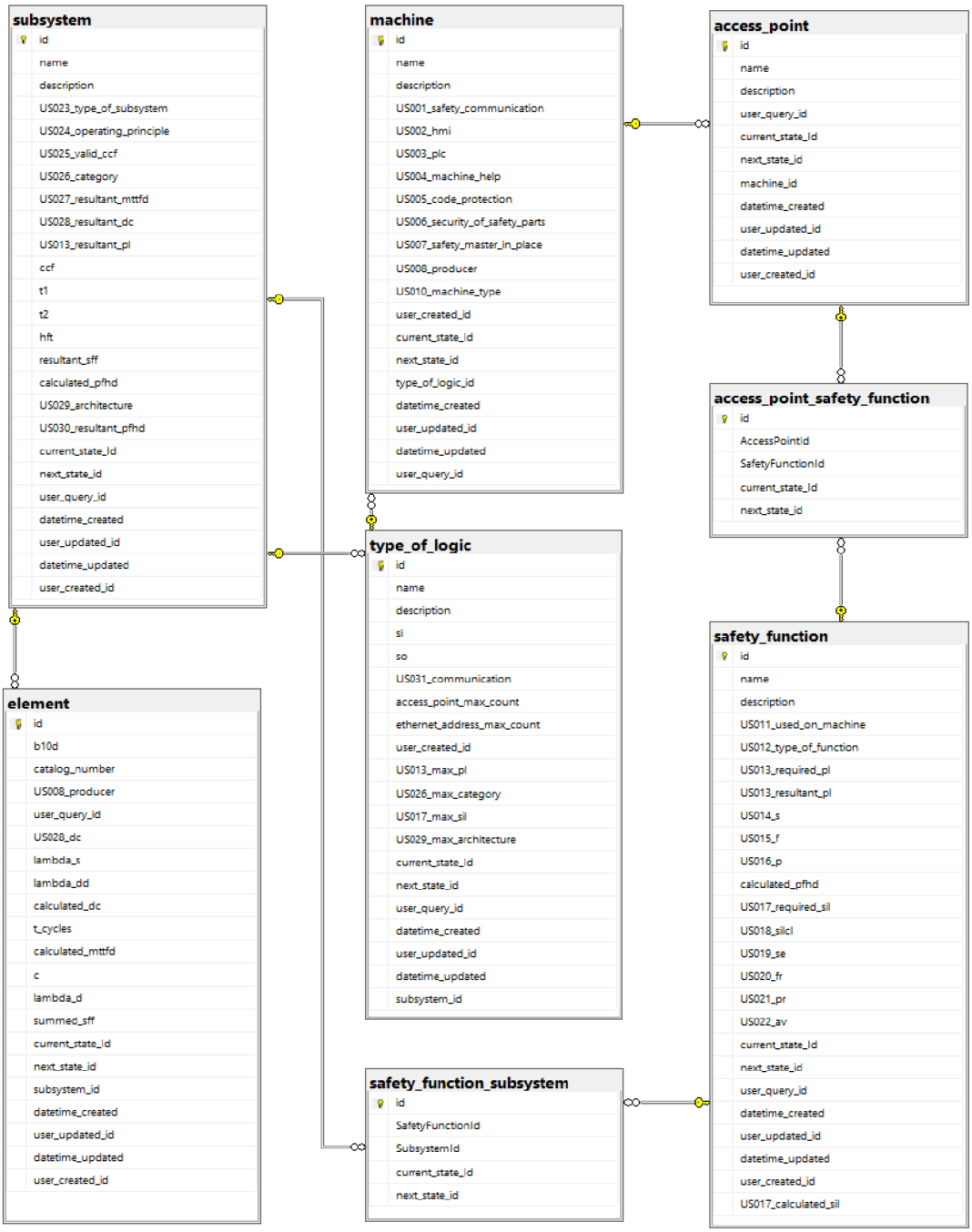
Tabuľka *safety_function* obsahuje dáta o bezpečnostných funkciách ktorými sú ošetrené prístupové body strojných zariadení. Rovnako ako ďalšie tabuľky obsahuje polia pre vyhodnocovanie bezpečnosti pomocou obidvoch metód (PL a SIL), pričom sa využívajú len tie ktoré patria ku práve používanej metóde. O tom ktorá metóda sa využíva rozhoduje stav záznamu. Keďže jedna bezpečnostná funkcia môže byť použitá pre viac prístupových bodov a jeden prístupový bod môže byť ošetrený viacerými bezpečnostnými funkciami sú tabuľky *safety_function* a *access_point* vo vzťahu N:M cez spojovaciu tabuľku *access_point_safety_function*.

Bezpečnostné funkcie sú zložené z bezpečnostných subsystémov, ktoré sú obsiahnuté v tabuľke *subsystem* a prepojené s tabuľkou *safety_function* vo vzťahu N:M so spojovacou tabuľkou *safety_function_subsystem*. O tom aké typy subsystémov (vstupný, výstupný, logický, komunikačný) sú pre bezpečnostnú funkciu potrebné rozhoduje spôsob zapojenia daného systému. Rovnako ako *safety_function* obsahuje polia pre metodiku PL aj SIL.

Každý subsystém sa skladá z jedného alebo dvoch elementov podľa počtu kanálov v jemu priradenej kategórii architektúry. Tieto elementy sú obsahom tabuľky element so vzťahom 1:N k tabuľke *subsystem*, aj keď k jednému subsystému patria najviac dva

elementy, okrem špeciálneho prípadu niektorých typov architektúry subsystému pri metodike SIL.

V tabuľke *type_of_logic* sú uložené typy logických subsystémov ktoré sú priradené jednotlivým strojným zariadeniam. Tým je z tabuľky *subsystem* priradený záznam reprezentujúci subsystém s daným typom logiky.



Obrázok 2 Diagram hlavnej časti dátového modelu

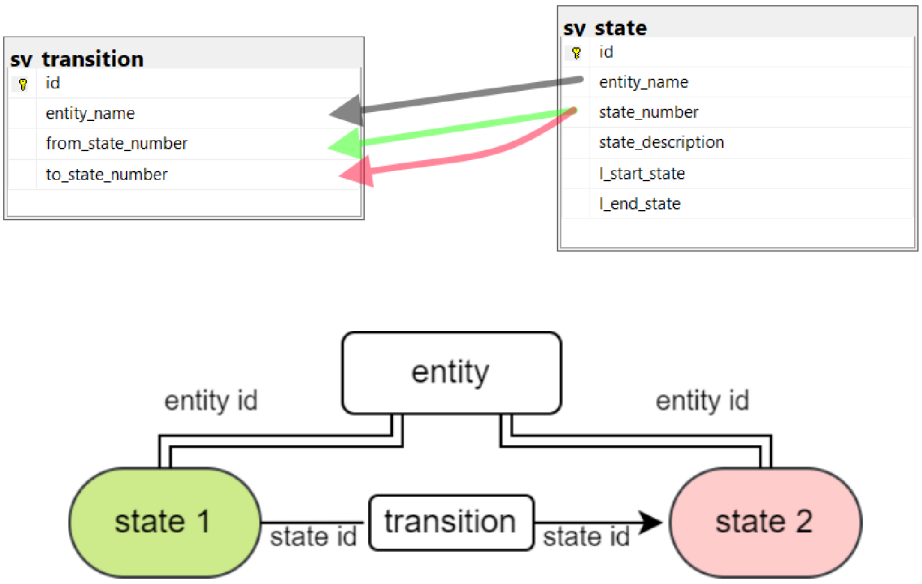
Polia v tabuľkách pre odkazy do doménového číselníku majú názvy vo formáte [názov domény]_[názov poľa] a obsahujú kód záznamu v dátovej tabuľke číselníku.

Každá entita/tabuľka hlavnej časti dátového modelu obsahuje polia pre metadáta (dáta o dátach) o každom zázname:

- **user_created_id/datetime_created** : Užívateľ, ktorý záznam vytvoril, a čas a dátum jeho vytvorenia.
- **user_updated_id/datetime_updated** : Užívateľ, ktorý záznam posledný upravil, a čas a dátum jeho poslednej úpravy.
- **current_state_id** : Aktuálny stav záznamu. Podľa tohto stavu sa záznam zobrazuje, umožňuje dynamicky vykresľovať a skrývať polia pri vytváraní a úprave záznamu.
- **next_state_id** : Plánovaný budúci stav záznamu. Je možné uložiť do akého stavu plánuje užívateľ záznam previesť a samotné prevedenie a prípadnú kontrolu spustiť neskôr.

2.1.2 Stavy a stavové prechody

Možné stavy a prechody medzi stavmi sú popísane v tabuľkách podľa obrázku 3. Každý záznam v tabuľke *sy_transition* spája dva záznamy v tabuľke *sy_state* a definuje prechod z jedného stavu do druhého. Do tabuľky stavov odkazujú ostatné tabuľky cez číslo stavu (*state_number*), pričom o tom, pre ktorú entitu konkrétny stav platí, rozhoduje pole *entity_name*. Užívateľovi systému sa potom ako stav záznamu zobrazuje obsah poľa *state_description*.



Obrázok 3 Diagram dátového modelu stavov a stavových prechodov

2.1.3 Doménový číselník

Namiesto použitia samostatných tabuliek na uloženie dát každého z číselníkov, je v novom dátovom modeli použitý doménový číselník zložený z dvoch tabuliek (obrázok 4). Výhodou doménového číselníku je jednoduchosť úpravy existujúcich číselníkov ako pridanie alebo odobranie poľa, zmena názvu poľa, či zmena obsahu číselníku a pridanie nových číselníkov bez nutnosti úpravy dátového modelu číselníkov.

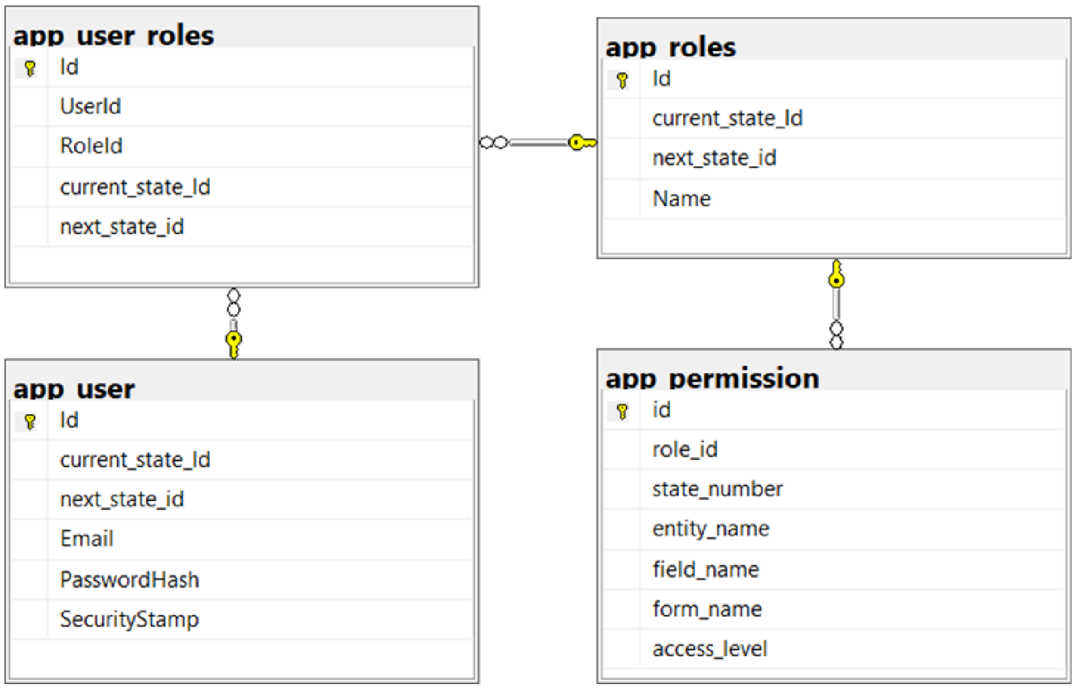
Prvá z tabuliek doménového číselníku (*sy_dictionary_data*) obsahuje položky pôvodne obsiahnuté v samostatných číselníkoch. V tejto tabuľke sú predpripravené stĺpce rôznych dátových typov, ktoré môžu byť pre číselníky potrebné. V druhej tabuľke (*sy_dictionary_definition*) sú definované hlavičky a popisy polí v *sy_dictionary_data* ktoré sa budú zobrazovať užívateľovi pri výbere položky z číselníku.

Záznamy v *sy_dictionary_data* a *sy_dictionary_definition* sú prepojené pomocou názvu domény, pričom jednotlivé záznamy *sy_dictionary_data* sú od seba rozlíšené kódom unikátnym v rámci danej domény. Záznamy v iných tabuľkách využívajúce doménový číselník potom do tabuľky *sy_dictionary_data* odkazujú pomocou tohto kódu. Integrita dát, teda istotu že kód položky z číselníku v zázname z tabuľky využívajúcej doménový číselník ktorý sa snaží užívateľ uložiť udržujú databázové triggre pri update a inserte záznamu.

Obrázok 4 Diagram dátového modelu stavov a stavových prechodov

2.1.4 Užívatelia a ich oprávnenia

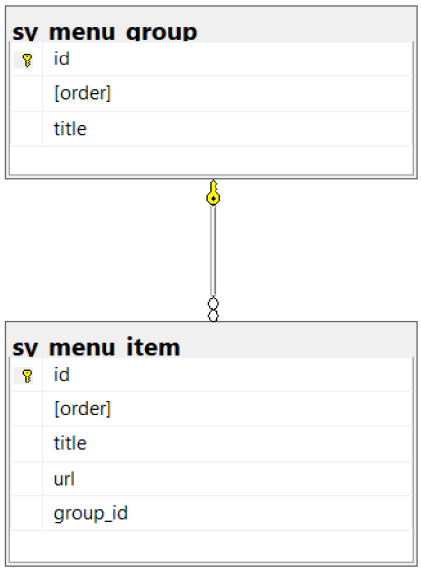
Spolu so stavmi záznamov, tabuľky užívateľov, ich rolí a oprávnení znázornené na obrázku 5 ovplyvňujú prácu jednotlivých užívateľov na záznamoch hlavných tabuliek. V tabuľke *app_user* sú uložené hlavné dáta užívateľov, teda ich emailové adresy a zašifrované heslá. K tejto tabuľke existuje tabuľka *app_roles* ktorá obsahuje definície rolí užívateľov. Jeden užívateľ môže mať viacej rolí a jedna rola môže byť priradená viacerým užívateľom, sú teda vo vzťahu N:M cez tabuľku *app_user_roles*. V tabuľke *app_permisson* je definované zobrazenie polí záznamov vo formulároch užívateľom podľa im priradených rolí a stavu vybraného záznamu. Úroveň *access_level* v tabuľke *app_permision* určuje úroveň prístupu. Úroveň 0 znamená že sa ovládací prvok nezobrazuje, úroveň 1 že sa ovládací prvok zobrazuje ale nie je možné ho používať a úroveň 3 že je ho možné aj používať. Je možné určiť úroveň prístupu aj k navigačným prvkom, čím je možné zamedziť napríklad uloženiu zmien alebo prístupu k určitým formulárom pre určitých užívateľov.



Obrázok 5 Diagram dát užívateľov, rolí a oprávnení

2.1.5 Menu

Obsah hlavného menu je definovaný v databáze v tabuľkách *sy_menu_group* a *sy_menu_item*. Je možné definovať skupiny odkazov (*sy_menu_group*) a určiť im názov a ich poradie. Do skupiny odkazov sa zaraďujú odkazy popísané v tabuľke *sy_menu_item*, kde je definovaný ich názov, poradie a http odkazy.



Obrázok 6 Diagram dát menu

2.1.6 SQL View

Pri prehliadaní zoznamu záznamov z databázy užívateľom nie je potrebné mu zobrazovať cudzie ID prepojených záznamov z inej tabuľky ale identifikovať ho ľudsky čitateľným spôsobom, napríklad jeho názvom. Aby nebolo nutné pre každý záznam v tabuľke vytvárať nový dotaz na databázu, je vhodné vytvoriť SQL view pre každú entitu, vďaka ktorému je možné z databázy priamo získať dáta tak, ako sa majú zobraziť užívateľom. View obsahuje SQL kód ktorý sa vykoná pri dotaze na neho. Pomocou príkazov join sú potom pripojené záznamy z druhých tabuliek. V prípade že je k jednému záznamu priradený len jeden cudzí záznam, je možné do jedného riadku výsledného SQL view vložiť názov priradeného záznamu. Ak je možné že priradených záznamov je viac, je najjednoduchšou možnosťou zobraziť užívateľovi počet priradených cudzích záznamov pre konkrétny záznam.

SQL view je použitý na nahrázdanie cudzieho ID zázamov iných entít v hlavnej časti dátového modelu ich menom alebo počtom, doplnenie názvu stavov a popisu vybranej hodnoty z doménového číselníka. Databáza obsahuje viewy:

- access_point_view
- element_view
- machine_view
- safety_function_view
- subsystem_view
- type_of_logic_view

Teda jeden view pre každú entitu z hlavnej časti dátového modelu.

2.1.7 Postup pri zadávaní údajov do systému a ich spracovanie

Pred vykonaním výpočtov a určení výslednej bezpečnosti systému je nutné do systému zadať údaje z ktorých sa výpočty vykonávajú. Okrem umožneniu zadávania údajov sa musí systém prispôsobovať práve používanej metodike vyhodnocovania bezpečnosti pre konkrétne strojné zariadenie. Podľa zvolenej metodiky PL/SIL systém musí požadovať rôzne údaje a vykonávať rôzne výpočty. Jedna bezpečnostná funkcia nepodporuje vyhodnotenie bezpečnosti viac ako jednou metodikou, čím by sa výrazne skomplikoval postup aj výpočty.

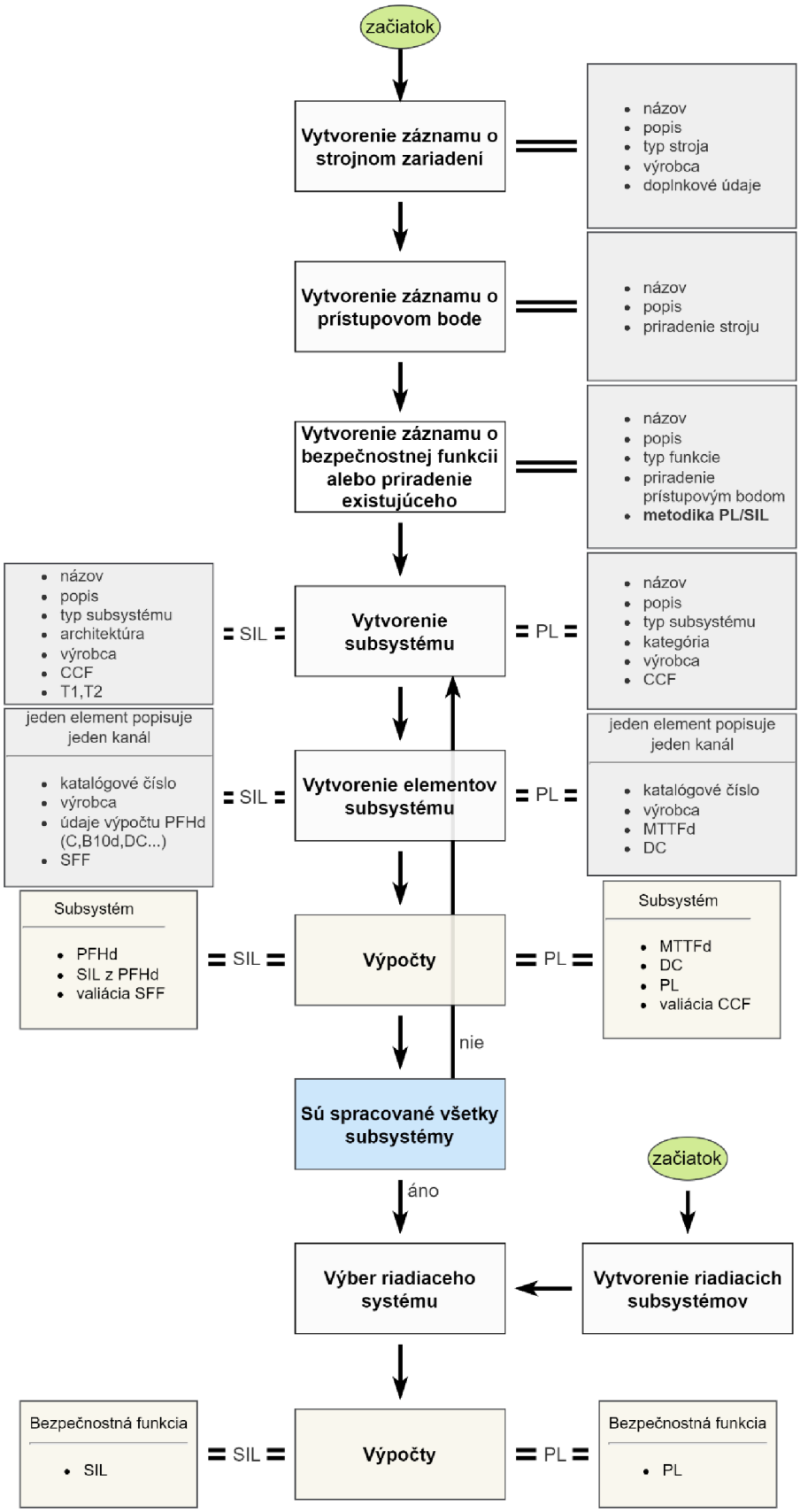
Rovnako ako v pôvodnej práci je cieľom automaticky vybrať najvhodnejší komunikačný subsystém z dostupných systémov v databáze tak aby splňoval minimálne požiadavky. Užívateľovi je dovolené zmeniť zvolený komunikačný subystém ručne po jeho automatickom zvolení. Rozšírením pôvodnej aplikácie je možnosť vytvorenia ďalších komunikačných subsystémov pre užívateľov so správnymi oprávneniami.

Užívateľ údaje zadáva podľa ním zvoleného pracovného postupu, je možné zadávať údaje o prístupových bodoch či subsystémoch v ľubovoľnom poradí, mať rozpracovaných niekoľko záznamov naraz. Systém by mal umožňovať aj prácu viacerích užívateľov na jednom strojnom zariadení, napríklad na rôznych prístupových bodoch alebo v rôznych fázach zadávania údajov podľa stavu záznamu.

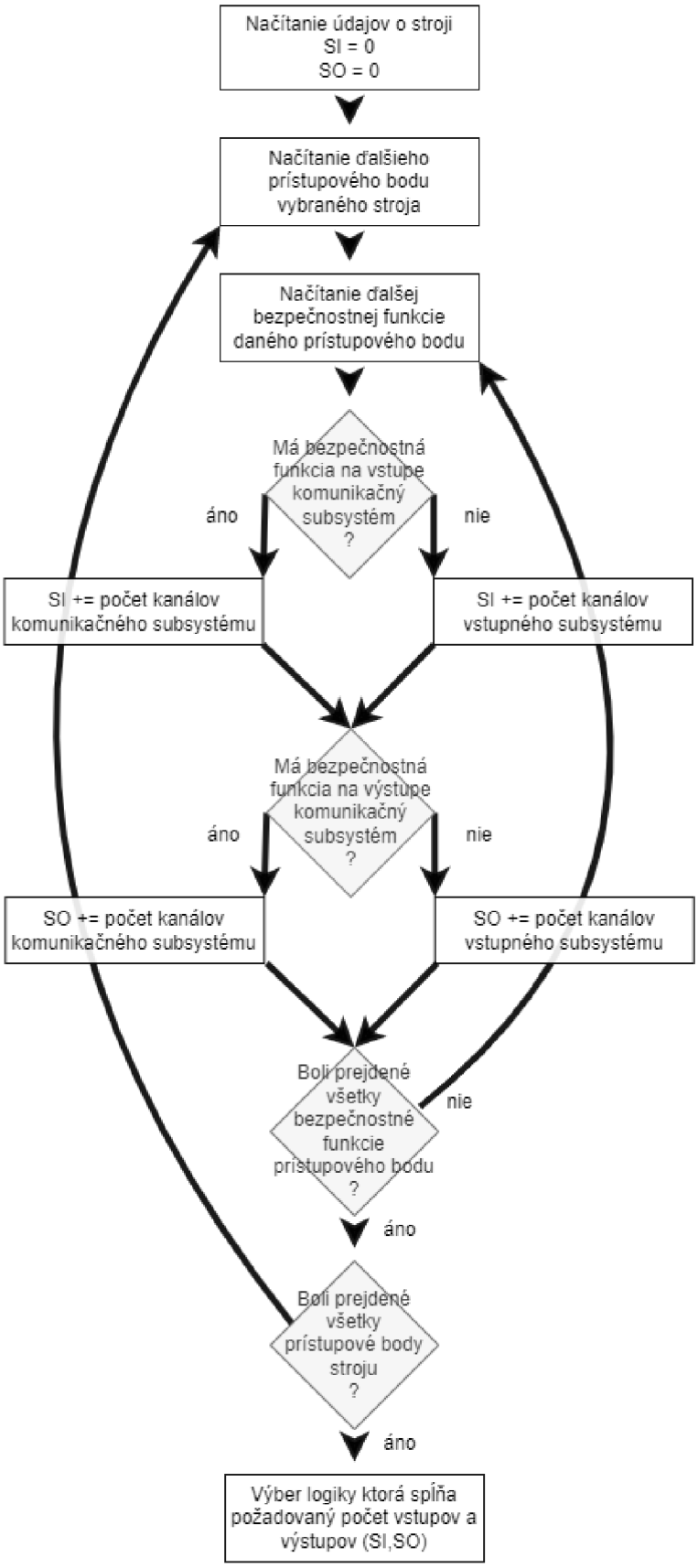
Pri automatickom výbere logického systému sa systém rozhoduje podľa počtu dostupných vstupov a výstupov (I/O) logického subystému. Požaduje sa dostatočný počet I/O aby bol logický subsystém prepojiteľný zo všetkými subsystémami obsiahnutými v bezpečnostných funkciách daného prístupového bodu. Požadovaný počet vstupov teda závisí na spôsobe zapojenia subsystémov bezpečnostnej funkcie, ktorý je určený kategóriou zapojenia. Spôsob zapojenia určuje počet komunikačných kanálov medzi vstupným, výstupným a komunikačnými subsystémami, ktorých celkový počet v bezpečnostnej funkcii určujé požadovaný počet vstupov a výstupov logického subsystému.

Po určení vhodného logického subsystému pre daný stroj, ho systém automaticky priradí do všetkých bezpečnostných funkcií. Užívateľovi je umožnené určiť zvolený logický subsystém ručne, systém potom akceptuje užívateľom zvolený subsystém a doplní automaticky zvolený subsystém do bezpečnostných funkcií kde užívateľ ponechal logický subsystém nezvolený. Po doplnení logických subsystémov môže užívateľ spustiť vykonanie výpočtov vyhodnotenia výslednej úrovne bezpečnosti stroja. Na vyhodnotenie bezpečnosti je potrebné, aby bol každej bezpečnostnej funkcii priradený správny počet a typy subsystémov a všetkým subsystémom priradený správny počet elementov podľa spôsobu zapojenia bezpečnostnej funkcie. Správnosť vyplnených údajov je možné kontrolovať pred vykonaním výpočtov.

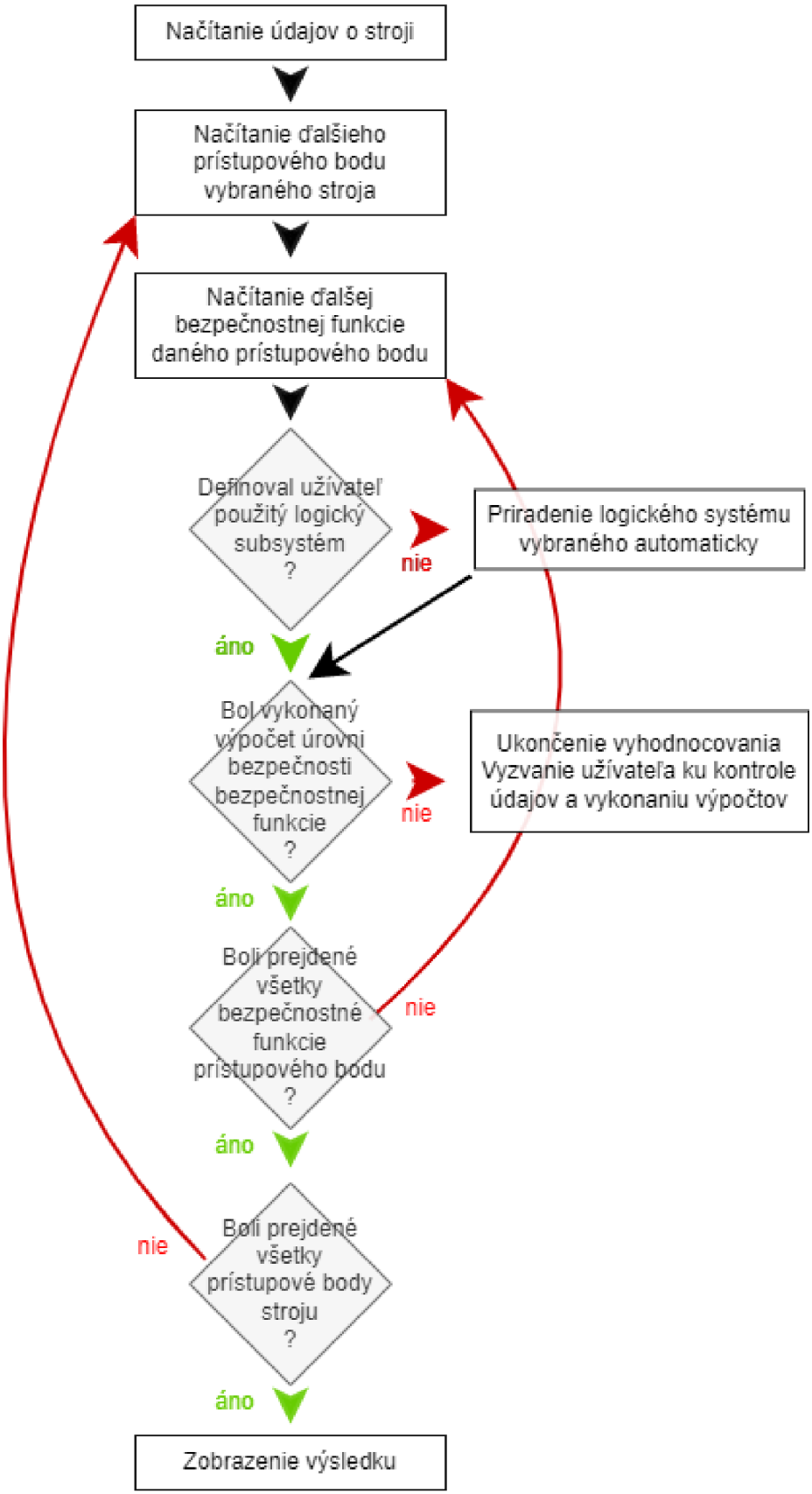
V prípade že vyplnené údaje sú validné, je možné vykonať výpočty podľa zvolenej metodiky a výsledky zobraziť užívateľovi. V opačnom prípade sa výpočet nevykoná a užívateľ bude mať možnosť údaje upraviť.



Obrázok 7 Postup pri zadávaní údajov



Obrázok 8 Algoritmus určenia požadovaného počtu I/O logického subsystému



Obrázok 9 Algorytmus vyhodnotenia úrovne bezpečnosti stroja

2.2 Testovacia aplikácia

2.2.1 Frameworky

Pre testovaciu aplikáciu bol zvolený framework Blazor WASM (front end) spolu s ASP.NET core (back end).

ASP.NET je open source cross platform (Windows, Linux, macOS, ...) webový framework vytvorený spoločnosťou Microsoft. Pomocou tohto frameworku bolo realizované Webové API (application programmer interface) umožňujúce komunikovať serverovej časti systému s klientami cez http protokol. Dáta sa prenášajú pomocou parametrov v URL a zakódované do JSON alebo XML v tele http dotazu od klienta alebo odpovede od servera. ASP.NET zachytáva http dotazy a mapuje ich na volanie funkcií napísaných v C#. Pri volaní funkcie sú automaticky dekódované parametre z adresy a z tela dotazu a sú predané funkcii. Tieto funkcie sú triedené podľa oblasti použitia do objektov (tzv. kontrolérov) a URL adresa na ktorú sú mapované sa im priraďuje podľa C# atribútov kontroléra a funkcie a parametrov ktoré sú označené ako parametre z URL.

```
[ApiController]
[Route("[controller]")] // Prvá časť URL
public class StateController : ControllerBase
{
    ...
    [HttpGet] // Odpoveď na dotaz typu http get
    [Route("Get")] // Druhá časť URL
    public async Task<ActionResult<State>> Get(
        [FromQuery] string entityName,
        [FromQuery] int id) // Parametre z URL
    {
        var states = await dbContext.States.FirstOrDefaultAsync(
            state =>
                state.EntityName == entityName &&
                state.StateNumber == id
            );
        return states;
    }
}
```

Vyššie je uvedený príklad kódu metódy ktorá vracia objekt popisujúci stav záznamu podľa dodaného mena entity a čísla stavu. Vracaná hodnota je automatiky zakódovaná do json/xml súboru. Adresa dotazu na túto metódu ktorá vznikne po zložení názvu kontroléra a cesty k funkcii je „/State/Get?entityName={meno entity}&id={číslo stavu}“.

Na prepojenie s databázou a jednoduchšiu úpravu dátového modelu bol využitý Entity Framework Core. Tento framework mapuje C# objekty na entity v databáze. Mapovanie na databázu sa riadi C# atribútmi. Podporuje LINQ dotazy (Language Integrated Query) ktoré prekladá na dotazy na databázový server. Výhodou použitia LINQ je že dotazy sú preložené a odoslané databázovému serveru až v momente keď dôjde k čítaniu dát. Entity framework tiež umožňuje vytvárať databázovú schému

(tabuľky a vzťahy medzi nimi) z tried ktoré sa majú na databázu mapovať pomocou tzv. migrácii. Migrácie sa generujú vo Microsoft Visual Studiu. Po vykonaní zmien v dátovom modeli na strane aplikácie sa zmeny prenesú do databáze vytvorením novej migrácie a jej spustením. V prípade nutnosti založiť novú databázu je potom možné jednoducho spustiť všetky migrácie za sebou, čím sa vykonajú všetky zmeny zaradom v poradí v akom boli migrácie generované.

```
[Table("access_point")]
public class AccessPoint : IStateChangable
{
    [Key]
    [Column("id")]
    public int Id { get; set; }

    [StringLength(100)]
    [Column("name")]
    public string Name { get; set; }

    [ForeignKey("machine_id")]
    public Machine Machine { get; set; }

    [NotMapped]
    public string MachineIdHash { get; set; }
    ...
}
```

V tomto príklade je uvedená časť definície tabuľky *access_point*. Pomocou atribútov je nastavený názov tabuľky a jej stĺpcov, ktoré zo stĺpcov slúžia ako hlavný kľúč a cudzie kľúče a ktoré dáta v objekte sa neukladajú do databáze. Rovnakým spôsobom sú mapované SQL viewy, tie však slúžia len na čítanie dát, nie na zápis do databáze. Obsah dotazu uloženého vo viewovch sa negeneruje, je ich teda potrebné vytvoriť ručne.

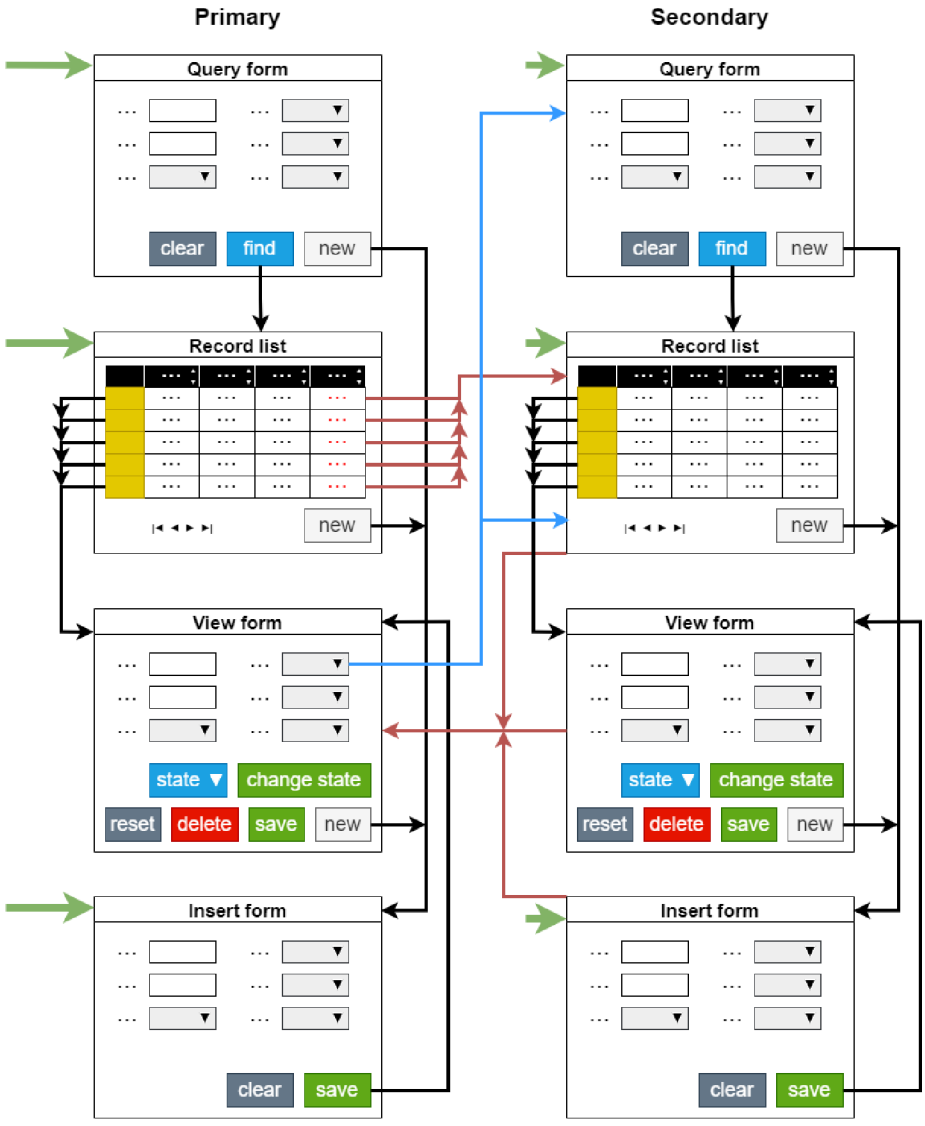
Front end je realizovaný pomocou Blazor WASM frameworku ktorý je rozšírením .NET frameworku. Umožňuje programovanie klientskej časti aplikácie v jazyku C# namiesto bežne používaného javascriptu. Kód užívateľského rozhrania je kombináciou HTML, CSS a C#. Dáta zo servera sa získavajú pomocou http dotazov na Web API, ktoré sa zo strany klienta odosielajú pomocou knižnice C#. WASM (Web Assembly) umožňuje inštalovať klientsku časť aplikácie na zariadenie klienta, pokiaľ to podporuje ich zvolený prehliadač. Aplikáciu sa potom nemusí s každým spustením sťahovať zo serveru čím sa urýchľuje jej načítavanie. Tiež je potom možné aplikáciu používať bez pripojenia ku serveru, avšak vzhľadom na požadované pripojenie k databáze pre prácu so systémom nie je táto výhoda podstatná.

2.2.2 Užívateľské rozhranie

Užívateľské rozhranie pre prácu s dátami v testovacej aplikácii je vytvorené zo štyroch typov formulárov:

- Query form – filtrovanie a vyhľadávanie záznamov, slúži ako vstup do record listu
- Record list – zobrazenie zoznamu položiek filtrovaného podľa query formu
- View form – zobrazenie jedného záznamu s možnosťou úpravy dát v prípade že to dovoľuje stav záznamu
- Insert form – vytváranie nových záznamov

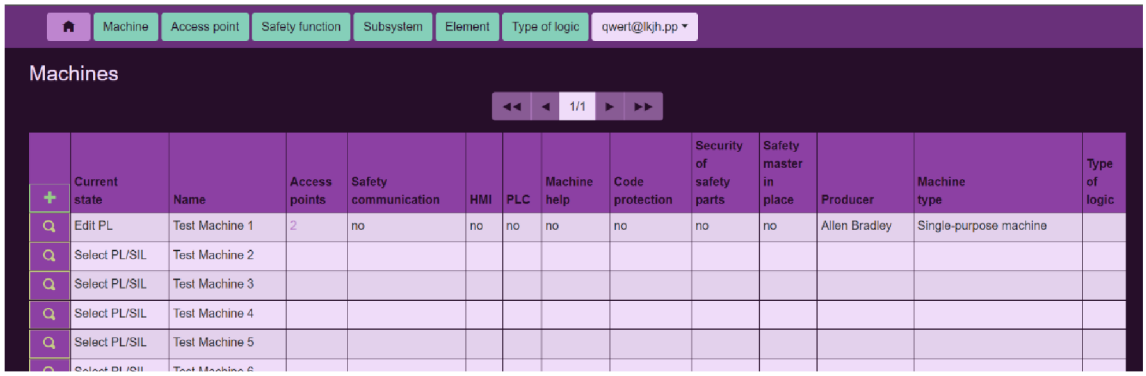
Navigácia medzi formulármi je znázornená na obrázku 10. Zelenými šípkami sú vyznačené možné body vstupu z menu systému. Čiernymi šípkami sú zobrazené prechody medzi formulármi rovnakej entity, červenými medzi formulármi rôznych entít. Modrá šípka naznačuje možnosti navigácie pri výbere záznamu na ktorý editovaný záznam odkazuje.



Obrázok 10 Navigácia a typy formulárov

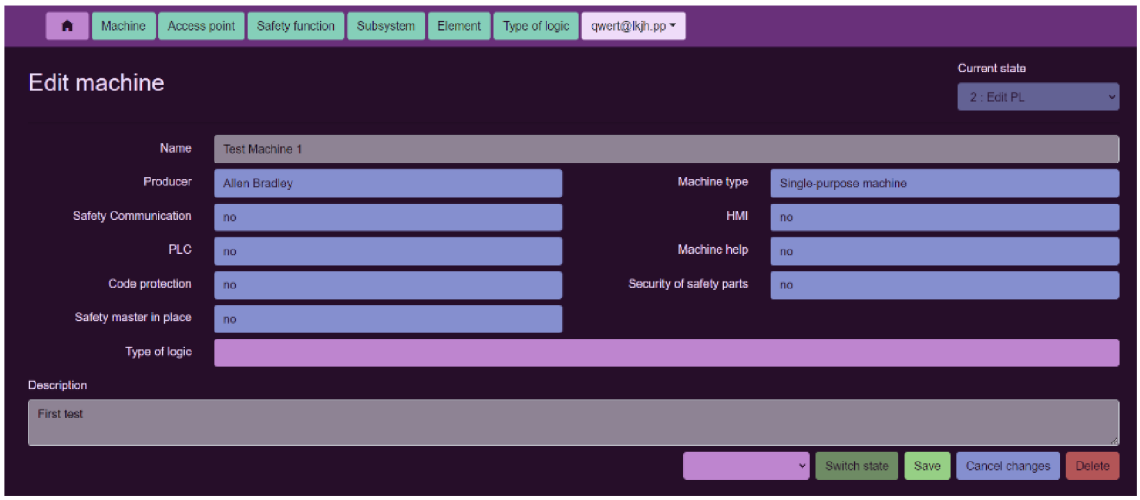
V prípade že sú dve entity vo vzťahu 1:M, je možné z record listu podradenej entity prejsť priamo do edit formu priradeného záznamu nadradenej. Použitím menu je možné kedykoľvek prejsť k query formu alebo record listu ktorejkoľvek entity. Pri vstupe do record listu sa použijú konkrétnym užívateľom naposledy zadané dáta do query formu na vyfiltrovanie zobrazovaných záznamov.

Navigácia z record listu (obrázok 11) k insert formu a view formu jednotlivých záznamov je možná tlačidlami na ľavej strane tabuľky.

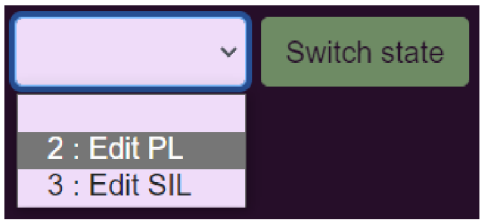


Obrázok 11 Record list

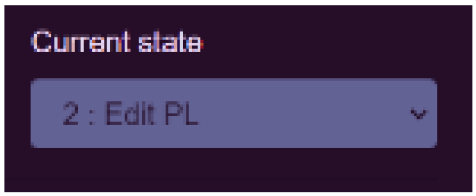
View form (obrázok 12), insert form (obrázok 15) aj query form. sú postavené na rovnakom základnom formulári s rozdielnymi ovládacími a navigačnými prvkami. Zobrazené ovládacie prvky a ich vzhľad je upravovaný podľa užívateľských oprávnení. Konfigurácia formulárov je popísaná v kapitole 2.2.5. Vo view forme je možné upravovať existujúci záznam. Obsahuje teda navyše ovládacie prvky pre uloženie zmien, zrušenie zmien, čím sa vrátia dáta späť do podoby v akej boli pred vykonaním neuložených zmien, odstránenie záznamu a zmenu jeho stavu. Ovládanie stavu záznamu je možné buď priamou zmenou jeho stavu zobrazovaného v pravom hornom rohu, čo však bežným užívateľom nie je umožnené, alebo prechodom medzi stavmi podľa stavového prechodového diagramu definovaného v databáze.



Obrázok 12 View form

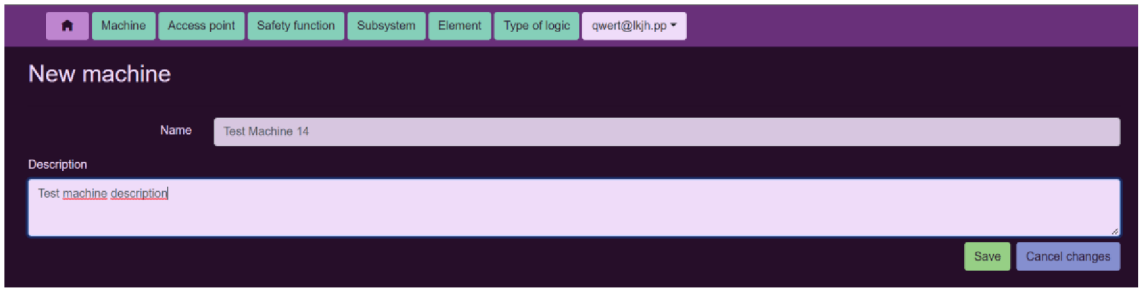


Obrázok 13 Rozbaľovacia ponuka výberu nasledujúceho stavu záznamu



Obrázok 14 Zobrazenie aktuálneho stavu záznamu

Insert form je založený na rovnakom formulári ako view form, má možnosť zobraziť rovnaké základné ovládacie prvky na zadávanie údajov. Pridané sú prvky na uloženie záznamu ako nový záznam a zrušenie zmien čím sa vymažú všetky zadané údaje. Na obrázku je zobrazený insert form nastavený tak, aby sa pri vytváraní nového záznamu vypĺňali len základné údaje, podrobnejšie údaje je možné zadať neskôr cez view form, poprípade v stave záznamu keď sú relevantné. Na obrázku 12 je zobrazený záznam v stave, kedy tieto základné údaje už nemožno upravovať.



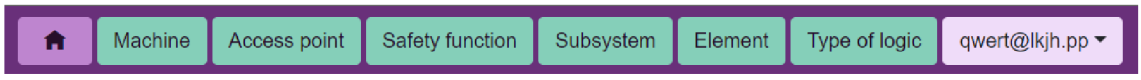
Obrázok 15 Insert form

Query form, takisto založený na rovnakom formulári, slúži na zadanie údajov, podľa ktorých sa vyhľadávajú záznamy pri zobrazovaní record listu. Obsahuje tlačidlo na uloženie vyhľadávacích údajov a prechod do record listu, a na odstránenie zadaných údajov. Ak nie sú zadané žiadne údaje, zobrazia sa v record liste všetky záznamy.

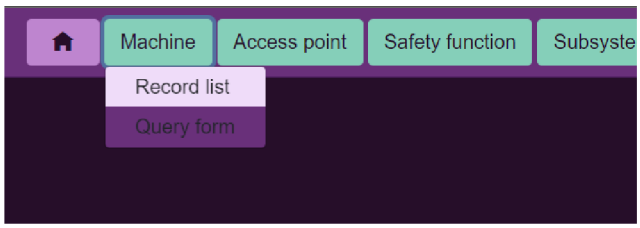
Obrázok 16 Query form

2.2.3 Dynamicky vykresľované menu

Hlavné menu je prístupné v akomkoľvek formulári a zobrazuje sa na vrchu stránky, nad obsahom formuláru. Skupiny menu sa zobrazujú ako tlačidlá zoradené do jedného riadku. Tým sa ušetrí viac priestoru ako keby sa menu zobrazovalo z boku stránky. Ako prvé je v rade menu tlačidlo domov, ktoré odkazuje na domovskú stránku aplikácie. Na konci riadku je tlačidlo na odhlásenie užívateľa, na ktorom sa zobrazuje aktuálne prihlásený užívateľ. Odkazy sa v menu zobrazia po kliknutí na tlačidlo skupiny odkazov ako vysúvací zoznam.



Obrázok 17 Hlavné menu



Obrázok 18 Vysúvací zoznam odkazov menu

V tabuľke *app_permission* je definovaný prístup k položkám menu. Je možné samostatne určiť prístup k jednotlivým skupinám aj odkazom podľa užívateľskej role. Každému užívateľovi sa tak môže zobraziť menu prispôsobené tomu aké činnosti môže s jemu pridelenými rolami vykonávať.

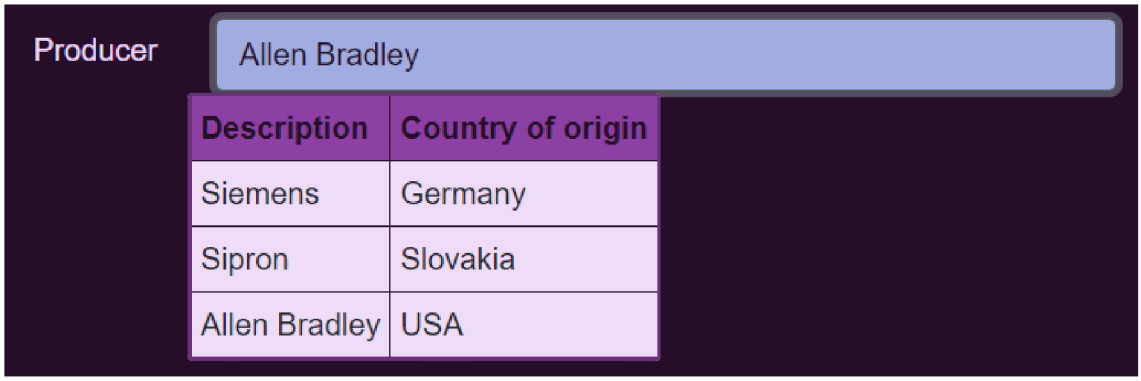
2.2.4 Vlastné ovládacie prvky formulárov

Pre niektoré funkcie informačného systému je nutné vytvoriť vlastné ovládacie prvky. Použitý framework Blazor umožňuje jednoducho vytvárať ovládacie prvky kombináciou HTML a C# kódu, ktoré sa potom dajú jednoducho opakovane použiť a parametrizovať. Každý ovládací prvok môže obsahovať kód, ktorý napríklad pri jeho načítaní automaticky posiela požiadavky o údaje na server. Server potom z databáze načíta požadované dáta podľa daného dotazu a odošle ich klientovi.

Jedným z vlastných prvkov je všeobecný record list, ktorému sa v konkrétnom formulári určenom konkrétnej entite priradí dátový typ reprezentujúci túto entitu. Tým je record list prispôsobený tak aby zobrazoval tabuľku s poliami dát danej entity. Základný editačný formulár pre insert, view a query form je tiež jeden komponent pre jednu entitu, Každá entita má vlastný editačný formulár.

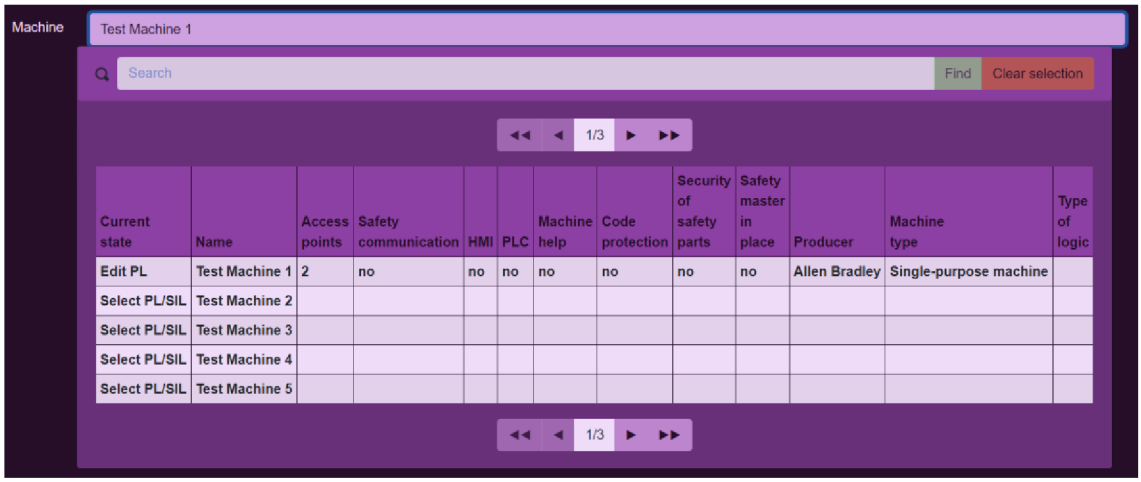
Prvým navrhnutým ovládacím prvkom bola rozbaľovacia ponuka umožňujúca užívateľovi výber záznamu z doménového číselníka. Je tvorený jedným tlačidlom, na ktorom je zobrazená práve vybratá hodnota z číselníku. Po kliknutí na toto tlačidlo je užívateľovi zobrazený zoznam hodnôt z číselníku patriacich určenej doméne. Zoznam, ktorý sa takto rozbalí, sa vykresľuje dynamicky podľa záznamu v tabuľke *sy_dictionary_definition,* pričom sa zobrazia len stĺpce s vyplneným menom. Pri použití tohto prvku vo formulári je potrebné určiť želanú doménu ktorej dáta sa majú načítať z databáze (tabuľka *sy_dictionary_data*). Pri zmene vybranej hodnoty z číselníku sa automaticky nová hodnota prenesie do formuláru. Vzhľadom na to že počet záznamov v jednej doméne číselníku nebude veľký, nie je nutné umožniť užívateľovi vyhľadávať v ponuke. Po dokončení výberu, kliknutí na iný ovládací prvok, alebo do prázdneho priestoru neobsahujúceho žiadne prvky sa ponuka automaticky zatvorí.

Obrázok 19 Tlačidlo ponuky hodnôt z doménového číselníku



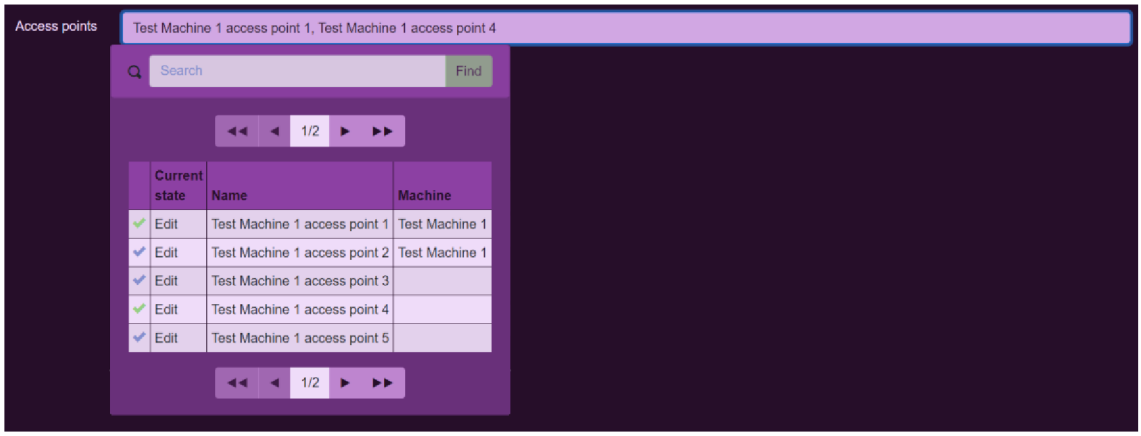
Obrázok 20 Rozbaľovacia ponuka hodnôt z doménového číselníka

Ako ďalší prvok bola navrhnutá ponuka pre výber záznamov inej entity. Tá zobrazuje tabuľku navrhnutú pre entity z ktorej záznamov sa má vyberať. Slúži pre výber prepojeného záznamu pri vzťahu 1:N zo strany entity ktorej záznam je prepojený len s jedným záznamom druhej entity. Keďže počet záznamov v hlavných tabuľkách systému je prakticky neobmedzený, obsahuje ponuka aj riadok na vyhľadávanie záznamu podľa názvu. Pri tomto riadku je aj tlačidlo pre zrušenie výberu. Rovnako ako ponuka záznamu z číselníku, sa aj ponuka záznamov z inej entity automaticky zatvorí v prípade výberu, alebo kliknutiu mimo otvorenej ponuky.



Obrázok 21 Rozbaľovacia ponuka výberu záznamov inej entity pre vzťah 1:N

Podobným, ale zložitejším prvkom je ponuka viacerých záznamov z inej entity. Tá umožňuje užívateľovi vybrať viac ako jeden záznam, pričom kliknutím na riadok je záznam buď označený alebo odznačený ako vybratý. Je určený pre vzťah N:M a je možné vyberať záznamy z obidvoch strán vzťahu. Na tlačidle ovládacieho prvku je potom zobrazený čiarkou oddelený zoznam mien vybraných záznamov. Na rozdiel od ostatných ovládacích prvkov sa tento automaticky nezavrie po zmene výberu aby bolo jednoduchšie označiť alebo odznačiť viacero záznamov.



Obrázok 22 Rozbaľovacia ponuka výberu záznamov inej entity pre vzťah N:M

Tlačidlá na otvorenie ponuky výberu záznamu z číselníka a z entity hlavnej časti dátového modelu sú od seba farebne odlíšené. Tiež sú od seba farebne rozlíšené ovládacie prvky, ktorých obsah je možno meniť (napríklad textové polia), alebo ich použiť (napríklad tlačidlá), a tie, ktoré sú zobrazené len pre čítanie.

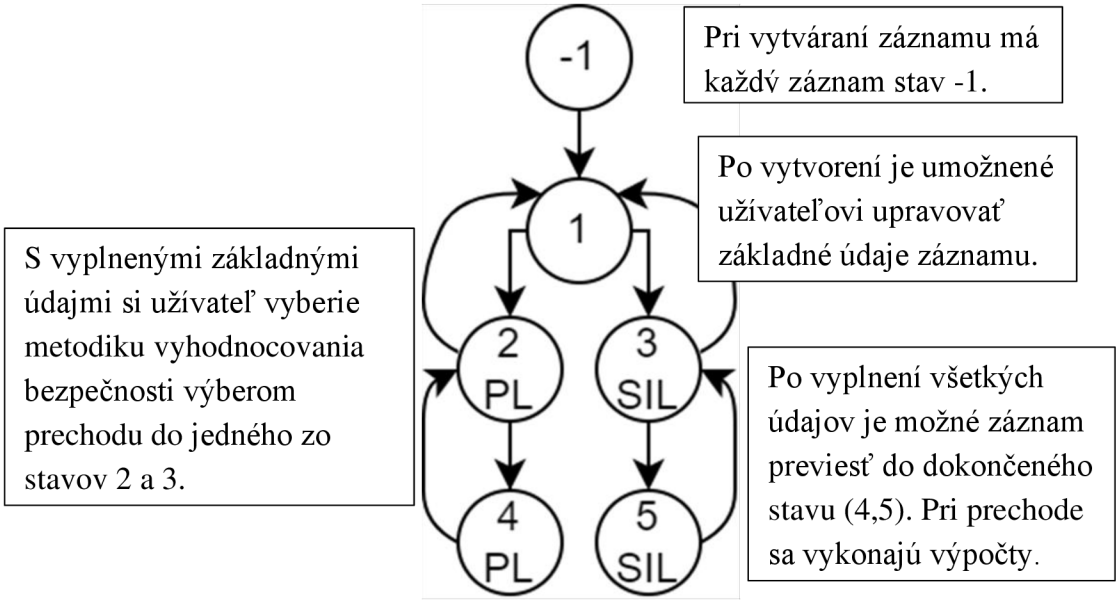
2.2.5 Konfigurovateľnosť formulárov a stavy záznamov

Pomocou tabuliek užívateľských oprávnení je možné meniť vzhľad a prístup k ovládacím prvkom formulárov v zvolených stavoch záznamu. Každý formulár má svoj zoznam oprávnení ktoré sa načítajú z tabuľky *app_permission* pri konkrétnom stave a konkrétnej užívateľskej roli. Načítanie prebieha pri otváraní formuláru a hľadajú sa oprávnenia patriace roliam priradením prihlásenému užívateľovi. Každému oprávneniu je možné určiť úroveň prístupu. V testovacej aplikácii úroveň oprávnenia 1 umožňuje užívateľovi vidieť obsah editovateľných polí, úroveň 0 mu umožňuje tento obsah aj meniť, pričom ak má užívateľ oprávnenie 0, nie je potrebné aj oprávnenie 1.

Obrázok 23 Zobrazenie prvku s oprávnením 1 (hore) a 0 (dole)

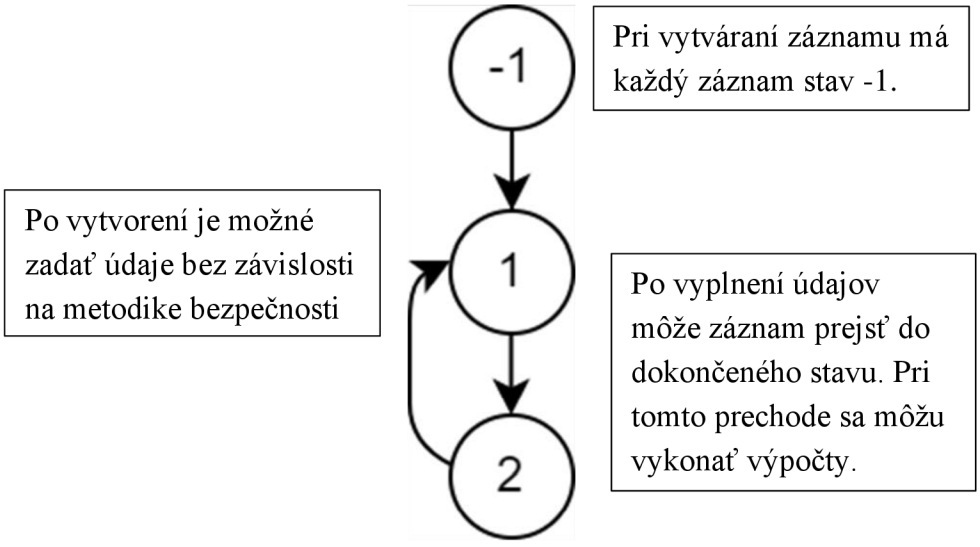
Pri prechode medzi stavmi sa potom vykonávajú kontroly a výpočty spojené s danými prechodmi. Podľa stavu záznamov je tiež určené akou metódou sa vyhodnocuje výsledná bezpečnosť. V tabuľke stavových prechodov (*app_transition*) je pre každú entitu definovaný prechodový diagram. Ak sa s touto entitou vykonávajú rôzne výpočty, alebo sa požadujú iné údaje podľa určitej metodiky, je prechodový diagram rozdelený na dve vetvy, každá pre jednu metodiku. Prepínanie medzi vetvami je možné len ak sa užívateľ vráti do základného stavu, keďže prepočet dát z jednej metodiky do druhej by bol príliš komplikovaný. Ak chce užívateľ upraviť zadané dáta a záznam sa nachádza v stave kde ich nie je možné meniť, musí užívateľ spustiť prechod späť do stavu kedy je editácia možná, čím sa zmení aj stav nadradených entít, aby bolo po zmenách nutné znovu vykonať všetky výpočty ktorých parametre sa zmenili. Výpočty sú definované v programe testovacej aplikácie na strane serveru, kde je možné rozlíšiť, o ktorý prechod ide a podľa toho vykonať správny výpočet. Prístupné polia pre potrebné údaje sú definované v tabuľke *app_permission* ako opísané vyššie.

Výsledkom kombinácie konfigurovateľných stavových prechodových diagramov, jednoducho upravovateľného doménového číselníku a užívateľských oprávnení, je výrazné zjednodušenie vykonania akýchkoľvek zmien v správaní formulárov, ktoré sa netýkajú výpočtov, a pri ktorých nie je nutné upravovať dátový model aplikácie. Pri vykonaní takýchto zmien nie je nutné zasahovať do kódu aplikácie, a tak je možné ich vykonať bez prerušenia jej chodu.



Obrázok 24 Stavový prechodový diagram rozdelený podľa metodiky PL/SIL

Tento stavový diagram používajú entity *safety_function*, *subsystem* a *element* nakoľko je potrebné užívateľovi zobrazovať iné ovládacie prvky v závislosti na používanej metodike vyhodnocovania bezpečnosti.



Obrázok 25 Stavový prechodový diagram bez metodiky PL/SIL

Takýto stavový diagram je vhodný pre entity *machine*, *access_point* a *type_of_logic*, kedže vypĺňané údaje o prístupových bodoch a o logických subsystémoch nie sú rôzne podľa používanej metodiky vyhodnocovania bezpečnosti.

Pri prechode medzi niektorými stavmi niektorých entít sa vykonávajú výpočty relevantné k danej entite a metodike PL/SIL. K úprave postupu pri týchto výpočtoch je potrebné zmeniť zdrojový kód aplikácie. Pre čo najjednoduchšiu úpravu kódu výpočtov

sú funkcie výpočtov v kontroléri zaoberajúcim sa zmenami stavu záznamov uložené v zozname. Do tohto zoznamu je možné vložiť referenciu na funkciu s vyhovujúcim predpisom (správne vstupy a výstupy). Funkcie z tohto zoznamu sú automaticky volané pri spracovávaní dotazu na zmenu stavu. Podľa dátového typu súvisejúceho s vybranou entitou je zo zoznamu vybraná referencia na funkciu vykonávajúcu výpočty s touto entitou. Výsledky vykonaných výpočtov sa uložia späť do objektu predaného funkcii referenciou, následne sú spolu so zadanými dátami uložené do databázy. Užívateľské rozhranie obsahuje polia na zobrazenie výsledkov výpočtu, ktorým je v stave po výpočte nastavená úroveň prístupu len na čítanie.

2.2.6 Overenie funkčnosti

Funkčnosť systému bola overená vytvorením záznamu o jednej bezpečnostnej funkcii pre každú metodiku. tieto bezpečnostné funkcie boli priradené prístupovým bodom, a tie boli priradené strojnému zariadeniu. Nakoniec bol vykonaný automatický výber logického subsystému.

Elements

◂◂ ◂ 1/1 ▸ ▸▸

	Current state	Producer	Catalog number	Subsystem	B10D	t cycles	Calculated MTTFd	C	λd	λdd	λs	DC	DC	Summed SFF
Q	Completed SIL	Siemens	Element A	Subsystem A	1000000			5	1E-06	9,7E-07	9E-06	0,96999997	Medium	0,9969999
Q	Completed SIL	Siemens	Element E	Subsystem A	700009			4	1,1428425E-06	9,6E-07	5,5E-06	0,8400107	Low	0,97247523
Q	Completed SIL	Allen Bradley	Element F	Subsystem B	300000			5	3,3333333E-06	3E-06	7E-06	0,90000004	Medium	0,9677419
Q	Completed SIL	Siemens	Element G	Subsystem B	2000000			30	3E-06	2,5E-06	1E-05	0,83333325	Low	0,96153843
Q	Completed PL	Allen Bradley	Element H	Subsystem C	100000	0,3	17,123287						Medium	
Q	Completed PL	Siemens	Element I	Subsystem D	250000	0,1	14,269407						High	

◂◂ ◂ 1/1 ▸ ▸▸

Obrázok 26 Záznamy o elementoch pri testovaní aplikácie

Boli vytvorené štyri elementy pre prvú bezpečnostnú funkciu, ktorá bude vyhodnocovaná pomocou metodiky SIL a dva pre druhú vyhodnocovanú pomocou metodiky PL. Výsledky výpočtov sa po ich vykonaní zobrazujú vo view forme aj v record liste.

Subsystems

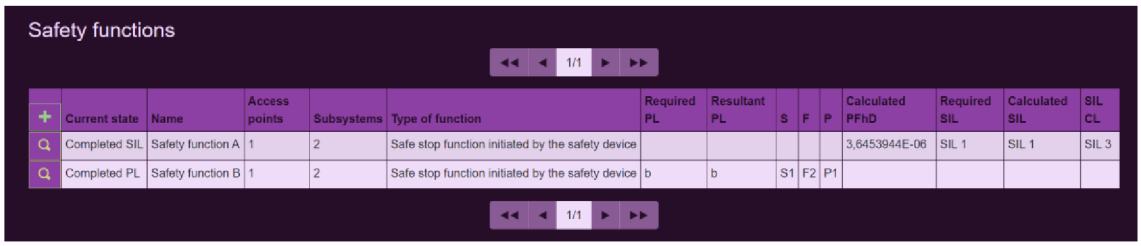
◂◂ ◂ 1/1 ▸ ▸▸

	State	Name	Type of subsystem	Operating principle	Category	Resultant MTTFd	Resultant DC	Resultant PL	CFF	T1	T2	HFT	Resultant SFF	Calculated PFHd	Architecture	Resultant PFHd
Q	Select PL/SIL	Relay logic	Logical	Electromechanical												
Q	Select PL/SIL	CR30	Logical	Electromechanical												
Q	Select PL/SIL	GMX	Logical	Electrical												
Q	Select PL/SIL	GLX	Logical	Electrical												
Q	Completed SIL	Subsystem A	Input	Electrical					40	10	2	0	2,1016693	2,1428425E-06	A	≥10^{-6} and< 10^{-5} SIL 1
Q	Completed SIL	Subsystem B	Output	Electrical					55	15	3	1	1,4428039	1,5025518E-06	B	≥10^{-6} and< 10^{-5} SIL 1
Q	Completed PL	Subsystem C	Input	Electrical	2	Medium	Medium	b	40					4,21E-06		
Q	Completed PL	Subsystem D	Output	Mechanical	2	Medium	High	b	50					5,33E-06		

◂◂ ◂ 1/1 ▸ ▸▸

Obrázok 27 Záznamy o subsystémoch pri testovaní aplikácie

Elementy boli priradené subsystémom obidvoch bezpečnostných funkcií. Počet elementov priradených každému subsystému závisí na zvolenom spôsobe jeho zapojenia, teda architektúre pre metodike SIL a kategórii pri metodike PL.

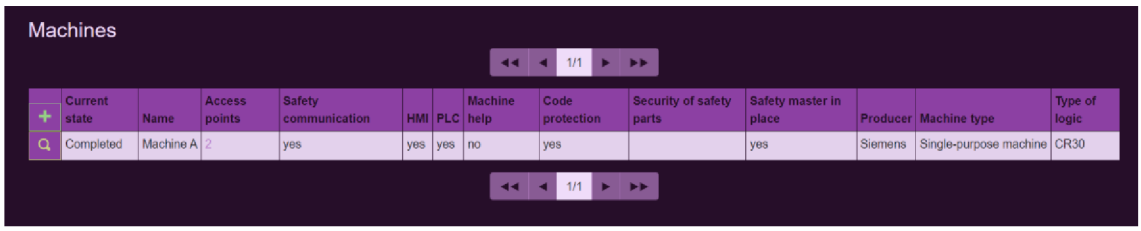


Obrázok 28 Záznamy o bezpečnostných funkciách pri testovaní aplikácie

Ďalej boli subsystémy priradené bezpečnostným funkciám. Výsledné hodnotenie bezpečnosti sa zobrazuje pre každú bezpečnostnú funkciu samostatne.

Obrázok 29 Záznamy o prístupových bodoch pri testovaní aplikácie

Prístupovými bodmi boli prepojené bezpečnostné funkcie a strojné zariadenie. Pri tejto entite sa výpočty nevykonávajú.



Obrázok 30 Záznamy o prístupových bodoch pri testovaní aplikácie

Nakoniec prevedením záznamu o stroji do dokončeného stavu bol vykonaný výber logického subsystému.

2.2.7 Publikácia aplikácie

Keďže bol pre aplikáciu zvolený framework ASP.NET, musí byť aplikácia publikovaná pre Microsoft IIS(Internet Information Services), čo je softwarový webový server, ktorý ako jediný ASP.NET podporuje. Visual Studio 2019 umožňuje aplikáciu publikovať ako balík vo formáte zip ktorý sa do IIS nainštaluje.

2.2.8 Zabezpečenie systému

Užívateľské účty sú v systéme identifikované emailovou adresou ako užívateľským menom. Nový účet je možné vytvoriť priamo z aplikácie, užívateľské oprávnenia je nutné užívateľovi priradiť v databáze administrátorom. Heslá k účtom sú do databázy ukladané po zašifrovaní pomocou PBKDF2 (Password-Based Key Derivation Function 2). PBKDF2 je kryptografická funkcia na odvodenie šifrovaného kľúča pomocou generátora pseudonáhodných čísel a hashovacej funkcie. Vďaka použitiu tejto funkcie sa znižuje citlivosť na útoky hrubou silou (skúšaním všetkých kombinácii). Aby bolo prihlasovanie naozaj bezpečné, je potrebné použiť šifrovaný komunikačný protokol medzi serverom a klientom, teda HTTPS protokol.

Prístup k záznamom je zabezpečený šifrovaním ID záznamu v linke. V record liste sú užívateľovi spolu so záznamami zobrazenými v tabuľke predané aj jednotlivé hashe ID všetkých zobrazených záznamov. Užívateľ si tak nemôže zobraziť hociktorý záznam len zmenou ID v linke a nedostane sa tak k záznamom, ku ktorým by nemal prístup.

ZÁVER

Cieľom tejto práce bol návrh informačného systému ktorého úlohou je pomoc pri návrhu bezpečnostných systémov a určovaní bezpečnosti strojných zariadení.

V prvej kapitole boli zhrnuté normy týkajúce sa bezpečnosti strojných zariadení. Boli popísané postupy pri analýze rizík a návrhu bezpečnostných systémov podľa normy (EN) ISO 13849-1 a IEC/EN 6206. Tiež boli vymenované parametre dôležité pri práci s normami.

V ďalšej kapitole bol opísaný návrh dátového modelu. Keďže táto práca nadväzuje na prácu [3], je dátový model postavený na pôvodnom dátovom modeli navrhnutom v tejto práci. Boli popísané úpravy pôvodného dátového modelu, nahradenie číselníkov jedným doménovým číselníkom a pridané konfiguračné možnosti pomocou stavov, stavových prechodov, a užívateľských rolí a oprávnení. Dátový model bol implementovaný v databáze MSSQL.

Bol opísaný postup zadávania údajov do systému a algoritmus ich spracovania, výpočtov a automatického výberu logického subsystému pre bezpečnostnú funkciu.

Ďalej boli vymenované použité nástroje a frameworky pre klientsku aj serverovú časť aplikácie navrhovaného informačného systému a ich výhody a dôvody prečo boli zvolené.

Aplikácia bola vyvinutá v jazyku C#, vo vývojovom prostredí Microsoft Visual Studio 2019. Skladá sa z dvoch častí, serverovej a klientskej. Serverová časť aplikácie sa zaoberá ukladaním, načítavaním a spracovaním dát v databáze. Klientska časť slúži na zobrazovanie dát užívateľom, ich úpravu použitím formulárov, upravuje užívateľské rozhranie podľa nastavení v databáze a komunikuje so serverovou časťou aplikácie pomocou webového API.

Ďalšia kapitola bola venovaná návrhu front endu a užívateľského rozhrania, použitým typom formulárom a navigácii medzi nimi. Bol zobrazený konkrétny návrh formulárov s demonštráciou možností konfigurácie ovládacích a navigačných prvkov a prechodov medzi stavmi. Táto konfigurovateľnosť umožňuje jednoducho zasahovať do systému a vykonávať niektoré zmeny bez nutnosti zmeny kódu, alebo prerušenia chodu aplikácie.

Dokončená aplikácia bola otestovaná a demonštrovaná návrhom bezpečnostných funkcii obidvomi dostupnými metodikami. Aplikácia bola publikovaná ako balík pre Microsoft IIS webový server.

V poslednej kapitole bolo opísané zabezpečenie systému, šifrovanie hesiel a zabezpečenie prístupu k záznamom len prepojením z iného formuláru.

LITERATURA

[1] *Bezpečnostní řídící systémy pro strojní zařízení: zásady, normy a implementace (revize 5 řady publikací Safebook)* 5. Praha: Rockwell Automation, 2016. Strojní vybavení (Rockwell). SAFEBK-RM002-CS-P.
[Návrh systému podle (EN) ISO 13849]

[2] *Bezpečnostní řídící systémy pro strojní zařízení: zásady, normy a implementace (revize 5 řady publikací Safebook)* 5. Praha: Rockwell Automation, 2016. Strojní vybavení (Rockwell). SAFEBK-RM002-CS-P.
[Návrh systému podle IEC/EN 62061]

[3] JANEK, Samuel. *Informační systém identifikace bezpečnostních systémů podle ČSN EN ISO 12100:2011. Brno, 2022*. Dostupné také z: https://www.vut.cz/studenti/zav-prace/detail/134855. Semestrální práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav automatizace a měřicí techniky. Vedoucí práce Radovan Holek.

SEZNAM SYMBOLŮ A ZKRATEK

Zkratky:

PL	úroveň vlastností
PL_r	minimálna požadovaná úroveň vlastností
$MTTF_D$	stredná doba do nebezpečného zlyhania
DC	diagnostické pokrytie
PFH_D	pravdepodobnosť nebezpečnej poruchy za hodinu
CCF	zlyhanie so spoločnou príčinou
SIL	úroveň bezpečnostnej integrity
HFT	tolerancia poruchy hardware
SFF	podiel bezpečných porúch
SIL CL	obmedzenie dosiahnuteľnej úrovne SIL

Symboly:

β	stupeň náchylnosti k CCF
λdd	počet nebezpečných detegovaných zlyhaní
λd	počet nebezpečných zlyhaní
T_1	interval kontrolného testu
T_2	interval diagnostického testu

ZOZNAM PRÍLOH

príloha A – záloha databáze je uložená na priloženom DVD

príloha B – zdrojový kód aplikácie je uložený na priloženom DVD