Univerzita Pardubice

Dopravní fakulta Jana Pernera

Analýza možných poruch zadaného systému pro bezpečné zobrazení a návrh opatření pro eliminaci jejich vlivu

Bc. Ondřej Blažek

Diplomová práce

2018

Univerzita Pardubice
Dopravní fakulta Jana Pernera
Akademický rok: **2017/2018**

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Ondřej Blažek**
Osobní číslo:	**D16503**
Studijní program:	**N3708 Dopravní inženýrství a spoje**
Studijní obor:	**Elektrotechnické a elektronické systémy v dopravě**
Název tématu:	**Analýza možných poruch zadaného systému pro bezpečné zobrazení a návrh opatření pro eliminaci jejich vlivu**
Zadávající katedra:	**Katedra elektrotechniky, elektroniky a zabezpečovací techniky v dopravě**

Zásady pro vypracování:

Popis architektury zadaného systému
Popis nebezpečných poruch zadaného systému a cílů bezpečnosti
Identifikace poruchových módů systému vedoucích k nebezpečným poruchám
Koncepce bezpečnosti a návrh opatření pro eliminaci jednotlivých nebezpečných poruch
Demonstrace vlivu vybraných navržených opatření

Rozsah grafických prací:

Rozsah pracovní zprávy:

Forma zpracování diplomové práce: **tištěná**

Seznam odborné literatury:

RÁSTOČNÝ, K. - KUNHART, M. - ZAHRADNÍK, J. Bezpečnost železničných zabezpečovacích systémov. 1. vyd. Žilina: EDIS, 2004. 276 s. ISBN 80-8070-296-9. Dostupná také z WWW: <http://kris.uniza.sk/images/stories/dok/BZS_Kniha_Za_Ra_Ku.pdf>.
CHUDÁČEK, V. a kol. Železniční zabezpečovací technika. 2. přeprac. a doplň. vyd. Praha: VÚŽ, 2005. 145 s. Dostupná také z WWW: <http://zabzar.cz/sites/default/files/ZZT_n>.
ČSN EN 50126-1. Drážní zařízení - Stanovení a prokázání bezporuchovosti, pohotovosti, udržovatelnosti a bezpečnosti (RAMS). Praha: Český normalizační institut, 2001. 72 s.
ČSN EN 50128 ed. 2. Drážní zařízení - Sdělovací a zabezpečovací systémy a systémy zpracování dat - Software pro drážní řídící a ochranné systémy. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2012. 108 s.
ČSN EN 50129. Drážní zařízení - Sdělovací a zabezpečovací systémy a systémy zpracování dat - Elektronické zabezpečovací systémy. Praha: Český normalizační institut, 2003. 104 s.

Vedoucí diplomové práce: **Ing. Jan Ouředníček, Ph.D.**
AŽD Praha

Datum zadání diplomové práce: **10. listopadu 2017**
Termín odevzdání diplomové práce: **18. května 2018**

doc. Ing. Libor Švadlenka, Ph.D.
děkan

L.S.

Ing. Dušan Čermák, Ph.D.
vedoucí katedry

V Pardubicích dne 12. března 2018

Prohlášení

Prohlašuji:

Tuto práci jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury. Byl jsem seznámen 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.

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 9/2012, bude práce zveřejněna v Univerzitní knihovně a prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 18. 5. 2018

Ondřej Blažek

Poděkování

Na tomto místě bych chtěl poděkovat především svému vedoucímu Ing. Janu Ouředníčkovi, Ph.D. Dále bych chtěl poděkovat mým kolegům z pracoviště VP06 za jejich rady a podporu, zejména Ing. Liboru Šimkovi za to, že se dobrovolně a svědomitě ujal role konzultanta, a svými podněty výrazně přispěl k této práci. V neposlední řadě děkuji své rodině, bez jejíž podpory by tato práce vůbec nemohla vzniknout.

Anotace

Diplomová práce se zabývá návrhem opatření pro podporu technické bezpečnosti zadaného systému bezpečného zobrazení. Ve své první části popisuje zadaný systém a jeho potenciálně nebezpečné poruchy. Dále analyzuje jednotlivé poruchové módy vedoucí k těmto poruchám. Na základě této analýzy práce stanovuje koncepci technické bezpečnosti zobrazovacího systému v podobě opatření eliminujících nebezpečné projevy poruch. Ve své poslední kapitole demonstruje vliv vybraných opatření.

Title

Analysis of Possible Failures of an Assigned Safety Display System and Measures Proposed to Eliminate their Impact

Klíčová slova

Bezpečné zobrazení, Technická bezpečnost, LCD, S1D12L01, TCG043WQLBAANN-GN50

Annotation

The Thesis deals with the proposal of measures supporting technical safety of an assigned safety display system. Its first part describes the assigned system and its potentially dangerous failures. Further, it analyses the individual failure modes leading to these failures. Based on this analysis, the Thesis specifies a conception of technical safety of the display system which consists of measures eliminating the dangerous expressions of failures. The last chapter demonstrates the impact of the selected measures.

Keywords

safety display, technical safety, LCD, S1D12L01, TCG043WQLBAANN-GN50

Úvod

Jedním ze základních rysů, kterým se železniční zabezpečovací technika odlišuje od běžné automatizační techniky je technická bezpečnost. A právě důraz na technickou bezpečnost způsobuje pomalejší nástup některých technologií, protože je vždy nejprve nutné analyzovat rizika těchto technologií a následně navrhnout adekvátní opatření pro snižování těchto rizik. To je také důvod, proč se nezřídka kdy využívají starší a z hlediska zajištění technické bezpečnosti jednodušší technologie. Toto platí i na zobrazovací systémy používané v železniční zabezpečovací technice, kde se pro bezpečné zobrazení často používají klasické průsvitky, i přesto že například z hlediska uživatelského komfortu či prostorové náročnosti (a někdy i výrobní ceny), je výhodnější použití grafického displeje. S rostoucí technickou úrovní zařízení využívajících zobrazovací systémy jsou výhody použití grafických displejů stále výraznější a proto je třeba se zabývat jejich technickou bezpečností.

Má-li grafický displej nahradit dříve používané zobrazovací systémy, musí mít obdobnou úroveň technické bezpečnosti. V tomto případě je univerzálnost displeje, pro kterou je upřednostněn před jiným řešením, spíše nevýhodou. Displej dokáže zobrazit téměř libovolný obraz. Proto je u grafických displejů velmi důležité najít a využívat vhodná opatření, která zajistí, že vlivem poruchy nedojde k takovému zobrazení chybných informací, které způsobí nebezpečí. Aby mohla být taková opatření navržena, je třeba nejprve analyzovat poruchy, které mohou způsobit nebezpečí a zjistit jejich možné příčiny.

Tato práce si klade za cíl popsat zadaný zobrazovací systém a jeho potenciálně nebezpečné poruchy. Dále pak uvést cíle technické bezpečnosti pro tento systém. Na tomto základě analyzovat potenciálně nebezpečné poruchy, najít k nim a popsat jednotlivé poruchové módy, které je můžou způsobit. Následně navrhnout opatření, která eliminují vliv těchto poruchových módů a umožní dosáhnout vhodné úrovně technické bezpečnosti. Tato opatření popsat a zhodnotit a sestavit přehled, kterými opatřeními lze pokrýt jednotlivé poruchové módy. Vybraná opatření následně demonstrovat.

. Oba procesory mohou obousměrně komunikovat s řadičem displeje pomocí sběrnice SPI. Jeden z procesorů může pomocí stejné sběrnice SPI komunikovat také s displejem, přesněji s jeho ovladačem. Řadič displeje je paralelní sběrnicí připojen k displeji, kde toto připojení je vedeno do ovladače displeje, který následně ovládá zobrazení na vlastní LCD matici. Jeden z procesorů dále generuje PWM signál sloužící k ovládání jasu LED podsvícení.

Multiplexaci přístupu a bezpečné odpojení jednotlivých mikrokontrolerů od sběrnice

[1]Procesorový modul je modul obsahující mikrokontroler a obvody potřebné pro jeho funkci, jako například úprava napájecího napětí, zdroj časového signálu, ošetření vstupů atd.

[2]Architektura 2 ze 2 (2oo2) je v železniční zabezpečovací technice takový systém, ve kterém dvě nezávislé jednotky zpracovávají shodné vstupní informace a výstupy těchto systémů jsou aplikovány pouze pokud jsou shodné. Případná neshoda (po ošetření případných přechodových dějů) je považována za poruchu systému a celý systém se v tomto případě bezpečnou reakcí samočinně odstaví z provozu tak, aby zůstal zachován bezpečný stav.

]

mikrokontrolery pohlížet jako na jedno bezpečné výpočetní jádro, které tedy není pro účely zajištění technické bezpečnosti třeba blíže popisovat.

Mikrokontroler Freescale MPC5554 patří do rodiny mikrokontrolerů PowerPC 5000 vyvinuté původně společností Motorola (dnes Freescale) především pro automobilový průmysl. Obsahuje na jednom čipu nejen samotné výpočetní jádro, ale také pevnou paměť programu, operační paměť a poměrně širokou sadu inteligentních periferií.

Je to 32bitový mikrokontroler, s jmenovitou taktovou frekvencí až 132 MHz. Obsahuje výpočetní jádro e200z6, 2 MB vnitřní Flash paměti na program a konstanty a 64 kB RAM. Tato paměť je dále rozšiřitelná, což je vzhledem k velikosti jednoho snímku důležité, ale z hlediska technické bezpečnosti to není podstatné. Mikrokontroler dále obsahuje 2 časovací jednotky eTPU s 64 vstupně-výstupními kanály, 64 kanálovou jednotku eDMA, řadič přerušení s 286 škálovatelně prioritizovatelnými vstupy, debugovací rozhraní JTAG a Nexus, 40kanálový dvojitý A/D převodník s podporou DMA, 3 jednotky pro DSPI rozhraní s až 16bitovým přenosem a až šesti chip select signály, 2 CAN moduly se 64 buffery, 2 moduly pro rozšířenou sériovou komunikaci a 24kanálovou jednotku pro měření a generování pulzních signálů. Většinu nepoužitých vývodů je možno využít také jako GPIO pin.

Z hlediska zadaného systému jsou důležité především: jednotka pro SPI komunikaci, jednotka pro generování pulzních signálů a obecné vstupy a výstupy (GPIO).

Jednotka pro SPI přenos umožňuje širokou škálu režimů SPI přenosů a rychlostí, a to tak, že více omezující jsou schopnosti řadiče a ovladače displeje, se kterými mikrokontroler komunikuje. Z hlediska technické bezpečnosti jde vždy o nezabezpečený, takzvaný šedý kanál, a proto zde nebude jednotka detailněji rozepsána.

Jednotka pro generování pulzních signálů (eMIOS) je použita pro generování PWM signálu regulujícího jas LED podsvícení displeje. I zde jsou více omezující schopnosti displeje než této jednotky. Navíc tento signál nemá příliš význam pro technickou bezpečnost a proto není potřeba jednotku blíže popisovat.

Obecné vstupy a výstupy také nemá příliš cenu rozepisovat, přestože jejich relevance k technické bezpečnosti je vyšší, protože jsou využity k ovládání povolovacích vstupů oddělovačů a řídí tedy přepínání SPI sběrnice na oba mikrokontrolery. Dále jsou pomocí SPI ovládány resetovací vstupy displeje i řadiče. Nicméně se stále jedná o zcela standardní výstupy, které má valná většina mikrokontrolerů.

]

1.2.1.1 SPI

Sériové komunikační rozhraní SPI, kterým je řadič vybaven, je standardní rozhraní pracující pouze v režimu slave. Pro výběr, zda chce master komunikovat s konkrétním řadičem, slouží signál SCS#, který je aktivní v nízké napěťové úrovni. Pro přenos dat slouží signály SI (směr do řadiče) a SO (směr z řadiče). Časování zajišťuje master signálem SCK. Rychlost této sběrnice určuje master, slave má pouze v určitých případech možnost vynutit snížení této rychlosti tím, že „přidrží“ hodinový signál. To však předpokládá přímé připojení hodinového signálu mezi řadičem a mikrokontrolerem, při využití jednosměrného oddělovače by tímto došlo k rozsynchronizování master a slave obvodu. Proto je důležité dodržet maximální datovou rychlost určenou výrobcem řadiče. Tato rychlost vychází z minimální periody hodinového signálu, která je dle specifikací 30 ns, což odpovídá o něco více než 33 Mbit/s.

Z hlediska datového přenosu lze říci, že délka datového přenosu není shora nijak omezena. Každý datový přenos je vlastně přístup do paměti řadiče. Data se přenášejí v pořadí vždy od nejvyššího bitu. Přenos vždy začíná aktivací signálu SCS# a končí jeho deaktivací. Zda jde o čtení či zápis a v jakém režimu je dáno příkazem poslaným do řadiče v prvním byte. Významy jednotlivých příkazů jsou uvedeny v následující tabulce.

Příkaz	Význam
10000000	Zápis v 8bitovém režimu
11000000	Čtení v 8bitovém režimu
10001000	Zápis v 16bitovém režimu
11001000	Čtení v 16bitovém režimu
Ostatní	Nejsou povoleny

Tabulka 1.2: SPI příkazy řadiče

Po příkazu následují tři byte adresy, od které se má začít zapisovat nebo číst. V prvním adresním byte jsou pouze tři nejvyšší bity adresy zleva doplněné nulami, následuje byte s osmi prostředními bity a nakonec byte s osmi nejnižšími bity. Následně se již režimy liší. 8bitové režimy přitom mají délku slova 8 bitů a 16bitové 16.

Při zápisu odesílá master bezprostředně po adrese slova, která se zapisují postupně do paměti řadiče od zadané adresy výše, neboli adresa na kterou se ukládá následující slovo je vždy vyšší o 1, v případě 8bitového, nebo o 2, v případě 16 bitového režimu, než adresa slova předešlého.

V případě zápisu se po odeslání adresy mění tok dat a data začíná posílat řadič

masteru. Pokud master i dále posílá data, jsou řadičem ignorovaná. Řadič ale není schopen okamžitě posílat data (potřebuje trochu času, aby přenesl data z požadované adresy do odesílacího bufferu) a proto jako první slovo pošle prázdné (nesmyslné) slovo. Odeslání jednoho slova mu poskytne dostatečný čas na přípravu odeslání následujícího slova, a tak po jednom prázdném slovu následuje již nepřerušovaný tok slov z paměti řadiče od adresy zadané masterem, přičemž následující slovo je vždy z adresy o délku slova vyšší než bylo předchozí.

V obou případech přenos ukončuje master deaktivací signálu SCS#. Na předchozí přenosy nelze přímo navázat, všechny přenosy musejí vždy začít příkazem a adresou (navázat lze pouze tak, že se zadá navazující adresa).

Na závěr popisu SPI rozhraní je nutné podotknout, že se jedná o nezabezpečený datový přenos a pokud vlivem poruchy dojde k chybě v přenášených datech, řadič ani master to nepozná a pracuje s chybnými daty. To je třeba při návrhu koncepce technické bezpečnosti zohlednit.

1.2.1.2 Obrazový výstup

Obrazový výstup je tvořen až 24bitovou paralelní sběrnicí, třemi signály zajišťujícími synchronizaci snímků, řádků, označujícími platnost a hodinového signálu. Datový tok je na této sběrnici pouze jednosměrný, a to ve směru od řadiče k displeji. V nastavení řadiče je možné konfigurovat šířku datové sběrnice na 16, 18 nebo 24 bitů. Pokud je šířka sběrnice menší než 24 bitů, lze zbývající výstupy konfigurovat jako obecné bitové vstupy/výstupy.

Přenosy na tomto rozhraní také nejsou zabezpečeny proti chybám vlivem poruch či rušení a řadič nemá možnost kontroly správnosti tohoto přenosu.

1.2.1.3 Resetovací vstup

Tento vstup je aktivní při nízké napěťové úrovni a jeho aktivace způsobí reset řadiče. Při resetu řadiče dojde k přerušení generování obrazového výstupu a řadič převezme výchozí konfiguraci. Vlivem resetu nemusí dojít ke smazání paměti řadiče, obrazová data v ní mohou zůstat zachována.

1.2.1.4 Výstup TE

Jedná se o konfigurovatelný výstup řadiče, který slouží k synchronizaci nadřazeného systému se snímkovou frekvencí výstupu řadiče. Tento signál má standardně nízkou napěťovou úroveň (logická 0) a podle nastavení může přecházet do vysoké úrovně (logická 1) v době mezi snímky, nebo po odeslání zadaného počtu řádků snímku. Se začátkem nového snímku se vždy vrací do nízké úrovně (logická 0). Pokud je tento výstup zakázán, setrvává stále v nízké úrovni (logická 0).

1.2.1.5 Napájecí vstup

Napájecí vstup není rozhraním v klasickém smyslu, ale lze jej použít k definované bezpečné reakci. Pokud není napájen, nemůže řadič generovat signál, což plyne z fyzikální podstaty obvodu a lze to považovat za prvek s vnitřní bezpečností. Je ale nutné si uvědomit, že po znovupřivedení napájení řadič převezme výchozí konfiguraci, v jeho paměti budou zcela nedefinovaná data a řadič je bude podle konfigurace převádět na obrazový signál, který většinou bude nesmyslný (šum). Odpojením napájení tedy dojde ke ztrátě konfigurace a obrazových dat.

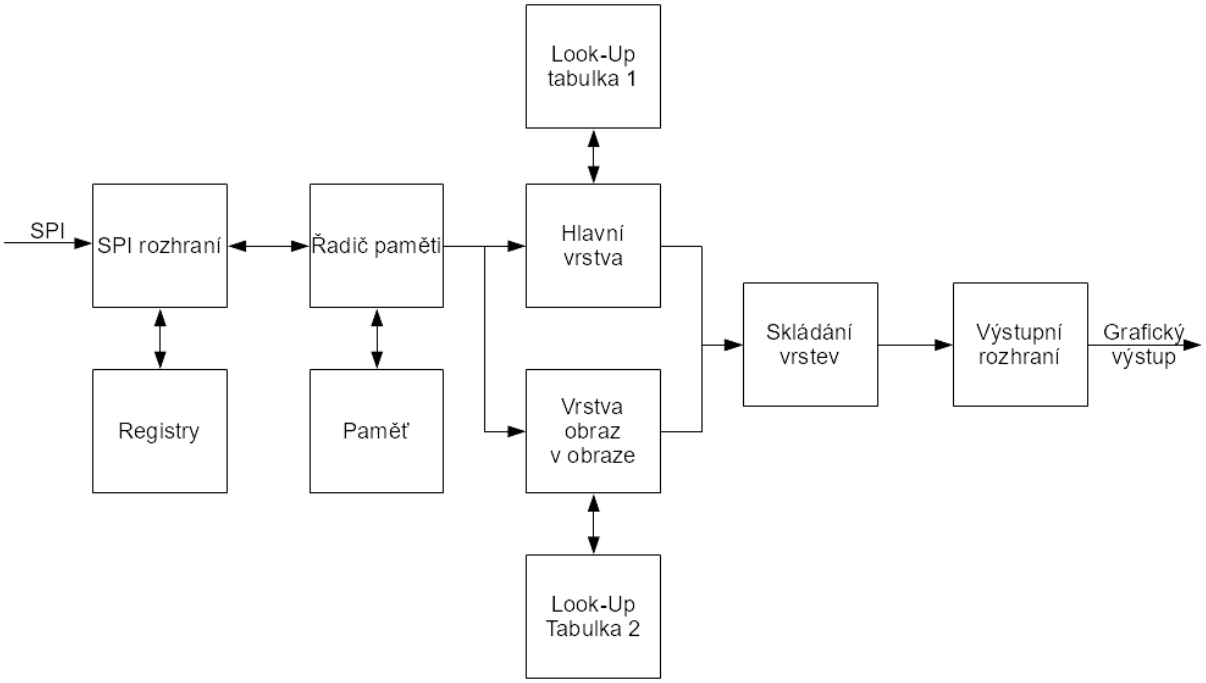
1.2.2 Vnitřní uspořádání řadiče

Na vnitřní uspořádání řadiče lze pohlížet ze dvou úhlů pohledu. Jedním je vlastní datový tok řadičem a druhým je uspořádání těchto dat v řadiči. Oba pohledy jsou důležité pro analýzu možných poruch a jsou tedy rozepsány v následujících částech práce.

1.2.2.1 Datové toky

Z pohledu datových toků se řadič dělí na jednotku vstupního rozhraní, registry, řadič paměti s pamětí, jednotku hlavní obrazové vrstvy a jednotku vrstvy obraz v obraze, obě s vlastní Look-Up tabulkou, jednotku skládající obraz z obou vrstev a jednotku rozhraní k LCD displeji. Uspořádání těchto jednotek z pohledu hlavního datového toku je zobrazeno na následujícím obrázku.

Hlavní datový tok je tok od nadřazeného systému do LCD displeje. Tento tok je pamětí rozdělen na dvě části. První část je vstupní, v ní přicházejí data přes vstupní rozhraní a řadičem paměti jsou zapsána do paměti. Tato část hlavního datového toku může být obousměrná, podle přijatých příkazů z nadřazeného systému. Druhá část má na starosti



Obrázek 1.3: Struktura řadiče z pohledu datových toků

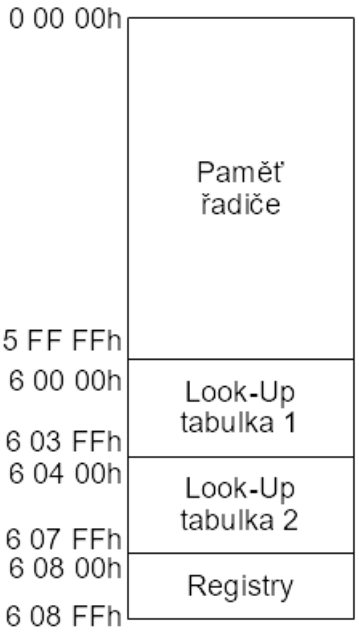
cyklické zpracovávání dat a vytváření výstupního signálu. V této části jsou řadičem paměti data z paměti čtena a následně předána patřičným jednotkám obrazových vrstev. Tyto jednotky na základě konfigurace v registrech a dat z Look-Up tabulek vytvářejí obrazová data jednotlivých vrstev. Tato data jsou následně předána do jednotky, která z obou vrstev na základě konfigurace složí výsledný snímek. Ten putuje do rozhraní LCD displeje, kde je z něj vytvořen signál pro displej. Tato druhá část datového toku je již pouze jednosměrná, data tečou pouze v popsaném směru. Všechny výkonné bloky (s výjimkou řadiče paměti) jsou řízeny konfigurací uloženou v registrech.

Kromě hlavního datového toku jsou v řadiči ještě dva vedlejší. Prvním vedlejším tokem je datový tok ze vstupního rozhraní do registrů obsahujících konfiguraci. Druhým pak je tok dat ze vstupního rozhraní do obou Look-Up tabulek. Všechny vedlejší datové toky jsou obousměrné, podle příkazů nadřazeného systému.

1.2.2.2 Uspořádání dat

Pohled na uspořádání dat je možný pouze ze směru nadřazeného systému, protože pouze tento systém může zapisovat a vyčítat data pomocí náhodného přístupu. Ostatní části přistupují do stejné struktury dat, nebo používají vlastní strukturu, která není výrobcem řadiče zveřejněna.

Všechna data, konfigurace i obě Look-Up tabulky jsou umístěny do společného souvislého adresního prostoru s adresami od 00000h do 608FFh. Tento prostor se dělí na VideoRAM obsahující vlastní obrazová data, dvě Look-Up tabulky a sadu registrů. Rozdělení adresního prostoru je zobrazeno na následujícím obrázku.



Obrázek 1.4: Adresní prostor řadiče

VideoRAM je jedinou částí adresního prostoru určenou k ukládání obrazových dat obou vrstev. Začíná adresou 00000h a končí 5FFFFh. Má tedy velikost 384 kB. Obrazová data obou vrstev se mohou vyskytovat jako souvislý blok ve kterékoliv části tohoto adresního prostoru. Jediným omezením je již zmíněná souvislost dat jednotlivých vrstev a dále ještě nutnost, aby oba bloky pro obě vrstvy začínaly na adrese dělitelné číslem 4. Velikosti bloků jsou přitom dány velikostí vrstvy (velikost hlavní vrstvy je shodná s velikostí displeje) a barevným režimem (barevné režimy jsou popsány v další části práce). Části paměti mimo tyto bloky nejsou zpracovávány pro účely výpočtu snímku, ale nadřazený systém do nich může libovolně zapisovat nebo z nich číst.

Look-Up tabulky jsou dvě, první tabulka pro hlavní obrazovou vrstvu se nachází mezi adresami 60000h a 603FFh. Druhá tabulka pro vrstvu obraz v obraze je mezi adresami 60400h a 607FFh. Každá tabulka je velká 1024 B. Význam tabulek je podrobněji rozepsán v další části práce zabývající se barevnými režimy.

V poslední části adresního prostoru mezi adresami 60800h a 608FFh jsou umístěny registry obsahující vlastní konfiguraci řadiče. Tento paměťový prostor již není z hlediska

významu zcela souvislý, některé adresy nejsou obsazeny. Všechny registry jsou 16bitové, takže zabírají dvě adresy, přičemž méně významné bity jsou na nižší adrese. Při 16bitovém přístupu je celý registr přístupný z adresy nižšího byte.

1.2.3 Režimy řadiče

Režimy řadiče lze rozdělit do dvou druhů, jde jednak o pracovní režimy a jednak o režimy barevné (rozdílné způsoby zpracování barev).

1.2.3.1 Pracovní režimy

Jde o tři režimy, přičemž první dva slouží k nastavení řadiče a třetí je pracovní. Tyto režimy se liší tím, které jednotky jsou funkční, přesněji, pro které jednotky je uvnitř řadiče zpřístupněno časování. Tím se také liší, ke kterým částem či nastavením je možné v daném režimu přistupovat. Mezi režimy se přechází zapsáním či smazáním příslušných bitů v registrech.

Prvním režimem je režim PSM0. V tomto režimu není časována ani paměť VideoRAM, ani rozhraní LCD displeje. Proto v tomto režimu není přístupná ani paměť, ani Look-Up tabulky. Přístupné jsou pouze registry a celý režim slouží k nastavení vnitřního časování. Poté co je časování nastaveno, je možné přejít do následujícího režimu.

Druhý režim nese označení PSM1 a je v něm již časována paměť řadiče včetně Look-Up tabulek. Neaktivní je stále rozhraní k LCD displeji. Tento režim je určen k nastavení parametrů pro generování výstupu do LCD displeje (například velikost displeje, nebo správné časování výstupního signálu). V tomto režimu již je možné zapsat obrazová data do paměti řadiče a také vyplnit Look-Up tabulky. V tomto režimu však stále není generován výstup. Dále také není možné změnit nastavení vnitřního časování.

Třetí režim již je pracovní, značí se NMM, časovány a tedy i dostupné jsou všechny jednotky. V tomto režimu však nelze měnit vnitřní časování ani některé parametry pro generování výstupního signálu.

1.2.3.2 Barevné režimy

Způsob, jakým je v obrazových datech reprezentována barva jednotlivých pixelů, je dán použitým barevným režimem. Řadič podporuje celkem 5 barevných režimů, přičemž každá vrstva (hlavní i obraz v obraze) může pracovat v jiném barevném režimu. Vždy platí, že

jednotlivé pixely jsou v paměti umístěny bezprostředně za sebou postupně po řádcích snímku. Celý snímek může mít různou datovou velikost při stejné obrazové velikosti v závislosti na použitém barevném režimu.

24bitový režim

Jde o základní režim, kdy jsou barvy příslušného pixelu popsány třemi byte, přičemž v prvním je hodnota modré barevné složky, ve druhém hodnota zelené barevné složky a ve třetím hodnota červené barevné složky. Tyto hodnoty v rozsahu 0 až 255 jsou přímo převedeny na výstup.

16bitový režim

V tomto režimu je každý pixel reprezentován jedním 16bitovým slovem (2 byte), kde nejvyšších 5 bitů udává hodnotu červené složky, prostředních 6 bitů zelené a nejnižších 5 bitů modré barevné složky. Tyto hodnoty v rozsahu 0 až 31 (u zelené 0 až 63) jsou převedeny do 8bitové podoby tak, že jsou zprava doplněny třemi (u zelené dvěma) zopakovanými nejvyššími bity příslušné barevné složky. Tyto hodnoty jsou následně přímo převedeny na výstup.

24bitový režim s Look-Up tabulkou

Zde stejně jako v 24bitovém režimu zabírá každý pixel tři byte, nejedná se zde o přímou hodnotu barevných složek ale o indexy do příslušné Look-Up tabulky. Zde byte odpovídající červené složce odkazuje na červenou složku patřičného záznamu v Look-Up tabulce, obdobně pro ostatní složky. Každá barevná složka každého pixelu má vlastní index do Look-Up tabulky. Na výstup jsou použity hodnoty barevných složek uložené na patřičných indexech Look-Up tabulky.

16bitový režim s Look-Up tabulkou

Tento režim je podobný 16bitovému režimu ve struktuře dat, i zde je pixel uložený v 16bitovém slově a na barevné složky připadá 5, 6 a 5 bitů. V tomto režimu nedochází k rozšíření těchto složek na 8 bitů, ale jednotlivé složky jsou, obdobně jako ve 24bitovém režimu s Look-Up tabulkou, použity jako index do patřičné Look-Up tabulky, ze které se následně

vyčte patřičná hodnota barevné složky pro výstup. I zde má každá barevná složka každého pixelu vlastní index do Look-Up tabulky. V tomto režimu ale není Look-Up tabulka plně využitelná, protože ta obsahuje 256 indexů pro každou barevnou složku, ze kterých je možno použít pouze prvních 32 (u zelené složky 64) hodnot.

8bitový režim s Look-Up tabulkou

Posledním použitelným barevným režimem je 8bitový režim s Look-Up tabulkou. V tomto režimu každému pixelu odpovídá jeden byte. V tomto byte je uložen index do Look-Up tabulky společný pro všechny tři barevné složky. Výstup pro tento pixel je generován ze všech tří barevných složek na daném indexu v příslušné Look-Up tabulce. V tomto režimu je možné použít pouze 256 barev, ale vybraných z celé 24bitové barevné škály.

1.2.4 Nastavení řadiče

Veškerá nastavení řadiče se provádějí pomocí zápisu do patřičných registrů. Řadič nemá pevnou paměť, a tak je nutné po každém přivedení napájecího napětí znovu do řadiče zapsat všechna nastavení.

V následujícím textu jsou stručně popsány jednotlivé registry, nejsou zde popsány konkrétní nastavovací bity, pouze co lze v registru nastavit. Konkrétní pozice bitu není pro analýzu dopadu poruchy bitu důležitá. Před názvem každého registru je uvedena jeho adresa v rámci registrů. K této adrese je třeba přičíst 60800h, aby vznikla adresa v adresním prostoru řadiče. Všechny registry jsou 16bitové, přičemž vyšší byte je umístěn na adrese o 1 vyšší.

1.2.4.1 04h – Power Save Configuration Register

Zde se nastavují pracovní režimy řadiče. Porucha může způsobit nechtěný přechod do jiného režimu.

1.2.4.2 06h – Software Reset Register

Tento registr obsahuje pouze bit způsobující zápisem logické 1 reset řadiče.

1.2.4.3 10h – PLL Settings Register 0

Registr obsahuje jeden stavový bit určující, zda je připraven interní hodinový signál z vnitřního fázového závěsu pro paměť a Look-Up tabulky. Dále jsou zde dva nastavovací bity. Jedním lze nastavit, že se místo vnitřního fázového závěsu použije pro paměť a Look-Up tabulky externí časovací signál. Druhým bitem se povoluje a zakazuje činnost interního fázového závěsu.

1.2.4.4 12h – PLL Settings Register 1 a 14h – PLL Settings Register 2

Zde se nastavuje převodový poměr vstupní časovací frekvence k interní časovací frekvenci. Nevhodná hodnota může způsobit nedostupnost, či přílišnou pomalost vnitřní paměti a Look-Up tabulek.

1.2.4.5 16h – Internal Clock Configuration Register

V tomto registru se nastavuje dělící poměr vnitřní frekvence a časovací frekvence výstupního signálu pro LCD displej. Nesprávná hodnota může způsobit rozsynchronizování řadiče a displeje.

1.2.4.6 18h, 1Ah a 1Ch – Reserved Register

Tyto registry nejsou v dokumentaci popsány, pouze je uvedeno že mají vliv na časování a také správná hodnota těchto registrů (je to též výchozí hodnota po restartu).

1.2.4.7 20h – Panel Setting Miscellaneous Register

Zde lze nastavit některé parametry výstupního signálu, jako je polarita a funkce signálu DE, polarita časovacího signálu. Dále povolit či zakázat celý výstup či jen datový tok pro LCD displej a nastavit šířku datové sběrnice k displeji. Šířka této sběrnice může být 24, 18 nebo 16 bitů. Nesprávné hodnoty ovlivňují výstupní signály a mohou zcela vyřadit či citelně zkreslit zobrazení.

1.2.4.8 22h – Display Settings Register

Jediný stavový bit v tomto registru obsahuje aktuální stav výstupu TE. Tento výstup se v tomto registru povoluje či zakazuje a konfiguruje se jeho funkce. Dále je zde možné přepnout výstup do stavu, kdy zobrazuje pouze celoplošně černý či bílý snímek, invertovat

všechny barvy, či zakázat funkci celého výstupního rozhraní k LCD displeji.

1.2.4.9 24h – Horizontal Display Width Register (HDISP)

Zde se nastavuje šířka displeje v pixelech.

1.2.4.10 26h – Horizontal Non-Display Period Register (HNDP)

Tento registr udává, kolik balastních pixelů je nutno odeslat na konci každého řádku, aby měl displej dostatek času na přechod na nový řádek.

1.2.4.11 28h – Vertical Display Height Register (VDISP)

Udává počet řádků displeje (výšku v pixelech).

1.2.4.12 2Ah – Vertical Non-Display Period Register (VNDP)

Zde se nastavuje kolik balastních řádků je nutno odeslat na konci každého snímku, aby měl displej dostatek času připravit se na příjem nového snímku.

1.2.4.13 2Ch – HS Pulse Width Register (HSW)

V tomto registru se nastavuje polarita a délka (v počtu pulzů výstupního časovacího signálu) horizontálního synchronizačního signálu.

1.2.4.14 2Eh – HS Pulse Start Position Register (HPS)

Uvádí začátek aktivace horizontálního synchronizačního signálu v pulzech výstupního časovacího signálu.

1.2.4.15 30h – VS Pulse Width Register (VSW)

Zde se nastavuje polarita a délka vertikálního synchronizačního pulzu v řádcích snímku.

1.2.4.16 32h – VS Pulse Start Register (VPS)

Hodnota v tomto registru udává pořadové číslo řádku, na kterém má začínat pulz vertikální synchronizace.

1.2.4.17 34h – TE Line Count Register

Pokud je signál TE v režimu, že je aktivován po určitém počtu řádků odeslaných během jednoho snímku do displeje, zde se nastaví právě tento počet řádků.

1.2.4.18 40h – Main Layer Settings Register

Zde se nastavuje, zda mají být zápisy do vícebyteových registrů obou vrstev synchronizovány, dále otočení a barevný režim hlavní vrstvy.

1.2.4.19 42h a 44h – Main Layer Start Address Register 0 a 1

Zde je spodních 16 bitů adresy v adresním prostoru, na které je první byte obrazových dat hlavní vrstvy (registr 0), a vrchní tři bity této adresy (registr 1).

1.2.4.20 46h – Main Layer Width Register

Šířka hlavní vrstvy v pixelech.

1.2.4.21 48h – Main Layer Height Register

Výška hlavní vrstvy v pixelech.

1.2.4.22 50h PIP Layer Settings Register

Zde se nastavuje otočení a barevný režim vrstvy obraz v obraze.

1.2.4.23 52h a 54h – PIP Layer Start Address Register 0 a 1

Zde je spodních 16 bitů adresy v adresním prostoru, na které je první byte obrazových dat vrstvy obraz v obraze (Register 0), a vrchní tři bity této adresy (registr 1).

1.2.4.24 56h – PIP Layer Width Register

Šířka vrstvy obraz v obraze v pixelech.

1.2.4.25 58h – PIP Layer Height Register

Výška vrstvy obraz v obraze v pixelech.

1.2.4.26 5Ah – PIP Layer X Start Position Register

Udává x-ovou pozici počátku vykreslení vrstvy obraz v obraze ve snímku.

1.2.4.27 5Ch – PIP Layer Y Start Position Register

Udává y-ovou pozici počátku vykreslení vrstvy obraz v obraze ve snímku.

1.2.4.28 60h – PIP Enable Register

Tento registr povoluje a zakazje vykreslování vrstvy obraz v obraze do snímku a řídí režimy tohoto vykreslování. Je zde možné nastavit periodu blikání, zda a jak má vrstva blikat. Pomocí příznaku zde lze ověřit, zda vrstva skutečně bliká.

1.2.4.29 62h – Alpha Blending Register

V tomto režimu se nastavuje mísení obou vrstev, lze zde nastavit počet kroků a úroveň mísení.

1.2.4.30 64h – Transparency Register

Zde se pouze povoluje aby jedna z barev vrstvy obraz v obraze byla považována za průhlednou.

1.2.4.31 66h a 68h – Transparency Key Color Register 0 a 1

Zde je udána barva, která má být považována ve vrstvě obraz v obraze za průhlednou. Pokud je vrstva obraz v obraze v některém z režimů využívajících Look-Up tabulku, použije se zde barva po převodu pomocí Look-Up tabulky (ne index či indexy do tabulky).

1.2.4.32 D0h – GPIO Configuration Register

V tomto registru je konfigurace obecných binárních vstupů/výstupů. Nastavuje se zde, zda je příslušný pin vstupní nebo výstupní.

1.2.4.33 D2h – GPIO Status and Control Register

Zde lze číst hodnoty obecných binárních vstupů a zapisovat hodnoty obecných binárních výstupů.

]

konfiguraci slouží konfigurační rozhraní. Bohužel právě možnost konfigurace zvyšuje počet potenciálních poruch zařízení o možnosti špatné konfigurace.

I tato součást bude popsána jak z vnějšího pohledu (rozhraní a komunikace), tak z vnitřního (vnitřní uspořádání a konfigurace). Opět zde bude brán zřetel především na ty části, které mohou způsobit některou z nebezpečných poruch celého zařízení.

1.4.1 Vnější pohled

Z vnějšího pohledu je zde popsáno především konfigurační rozhraní, neboť jak vstupní rozhraní videosignálu tak výstupní rozhraní k LCD panelu jsou popsána v předchozích kapitolách.

Ovladač displeje obsahuje tři rozhraní. Jde o vstupní rozhraní videosignálu, jehož principy jsou popsány u řadiče. Dalším rozhraním je výstup k LCD panelu. Toto rozhraní je dostatečně popsáno u displeje, proto obě rozhraní zde již dále popsaná nejsou.

Třetím rozhraním, které v jiných částech popsáno není, je konfigurační rozhraní SPI. Obecně je toto rozhraní z pohledu řadiče obousměrné, ale protože vodič směru z ovladače do nadřazeného systému není vyveden, lze ji považovat za pouze jednostrannou. Proto zde nebude popsáno ani čtení z ovladače, ani interní stavové příznaky. Z hlediska zapojení a nejnižší komunikační vrstvy se jedná o zcela standardní jednosměrné SPI, kdy signál CSB slouží k aktivaci zařízení, signál SCK zajišťuje časování a pomocí signálu SDI se přenášejí data z nadřazeného systému do ovladače.

Z hlediska komunikace se přenášejí vždy dvě 24bitová slova. Přenos každého slova začíná aktivací signálu CSB (přechod z vysoké na nízkou napěťovou úroveň, kterou drží do konce přenosu slova), následně se začnou generovat časový a datový signál. Po přenesení slova je nutné signál na minimálně předepsaný čas opět deaktivovat (z nízké na vysokou napěťovou úroveň).

Každé 24bitové slovo přenáší vždy 6bitovou identifikaci zařízení následovanou jednobitovým příznakem, zda jde o adresu nebo data a také jednobitovým příznakem, zda jde o čtení nebo zápis (zde vzhledem k jednosměrnosti komunikace má smysl pouze zápis). Následujících 16 bitů je adresa nebo data.

Pro zápis do registru, což je vzhledem k zapojení jediná smysluplná operace, je potřeba odeslat do ovladače dvě slova. V prvním slově je adresa registru, do kterého má být zapsáno, a ve druhém vlastní zapisovaná data.

1.4.2 Vnitřní pohled

Vnitřní struktura ovladače displeje je rozdělena do dvanácti jednotek. Ne všechny tyto jednotky jsou v rámci zadaného displeje využity, nevyužité jednotky nemohou způsobit nebezpečnou poruchu a proto nejsou blíže popsány. Jde v podstatě pouze o jednotku PWM, která má za úkol řídit úroveň jasu podsvícení displeje, zde však není použita a jas displeje je řízen z externího zdroje.

První jednotkou, kterou vstupují obrazová data, je jednotka vstupního rozhraní. Zde dochází k oddělení informací o řádcích a snímcích od informací o barvách a poloze v rámci řádku.

Data o barvách včetně synchronizace bodů putují do posuvného registru, v něm se ze sérioparalelně přenášených dat 320 bodů v RGB stane 960 paralelních informací o jasu. Původní barevné složky jsou v tomto registru prostřídány do uspořádání podle matice.

Informace o synchronizaci řádků a snímků putují do obvodu ovládajícího hradla TFT tranzistorů matice. Porucha tohoto obvodu se projeví v nesprávném řádkováni, či v nesprávné snímkové synchronizaci.

Do obvodu ovládajícího hradla TFT tranzistorů dále vstupuje ještě signál z posuvného registru řídícího směr řádkování.

Paralelizovaná data o úrovních jasu buněk aktuálního řádku jsou zachycena do zachycovací paměti. Tím je zafixován jeden řádek (posuvný registr může začít s plněním dalšího řádku). Od tohoto místa jednoduchá porucha působí v rámci sloupců, plošná záměna barev je nepravděpodobná.

Data ze zachytávací paměti jdou dále do převodní matice. V této matici jsou převedeny na příslušné napěťové úrovně, podle nastavení registrů a referenčních napěťových úrovní.

Takto získaná napětí pro jednotlivé LCD buňky dále putují přes výstupní rozhraní do LCD matice. Zde dochází již pouze k patřičnému vybuzení signálu pro výstup.

Do převodní matice vstupují také referenční napětí pro jednotlivé úrovně jasu z jednotky gamma korekcí. Ta má za úkol připravit právě tato napětí a zajistit korekci linearity jasu tak, aby byly maximálně kompenzovány nelinearity dané použitou technologií panelu.

Tato jednotka čerpá potřebné informace k nastavení korekcí ze dvou jednotek registrů. První jsou registry s pevnou, jednou programovatelnou pamětí (programování zajišťuje výrobce displeje podle kalibračních měření) a druhá obsahuje registry postavené na bázi energeticky závislé paměti, které je třeba po přivedení napájení nastavit pomocí SPI.

Komunikaci přes rozhraní SPI zajišťuje jednotka SPI. Přes ni se nastavují registry. Lze přes ni také programovat jednou programovatelnou paměť (OTP).

Poslední jednotkou je jednotka, která má na starosti přípravu referenčních napětí pro jednotku gamma korekcí a ovládacích napětí pro jednotku ovládající TFT hradla.

1.4.3 Nastavení ovladače

Nastavení se provádí pomocí registrů. V této části jsou uvedeny všechny registry a pouze u registrů, jejichž špatné nastavení může způsobit nebezpečnou poruchu, jsou popsány i významy jednotlivých nastavení.

1.4.3.1 R01h – Driver Output Control

Zde je bit povolující generování napětí pro řízení hradel TFT, bit který invertuje jas všech subpixelů, bit přepínající režimy RGB a BGR. Dále bit povolující prokládaný režim (v tomto režimu jsou ve snímcích nejprve všechny liché a následně všechny sudé řádky), bit ovládající směr řádkování a bit ovládající směr datového posuvného registru (zrcadlové otočení obrazu).

1.4.3.2 R02h – LCD-Driving-Waveform Control

Toto nastavení ovlivňuje načasování pravidelné inverze ovládacího signálu. Toto nastavení nezpůsobí nebezpečnou poruchu.

1.4.3.3 R03h – Power Control

V tomto registru se nastavují napětí pro ovládání gate TFT tranzistorů. Špatné nastavení může změnit jas všech buněk LCD matice. Dále zde lze nastavit možnosti přesnosti řízení napětí pro LCD buňky v 8bitovém režimu. Tento režim není zapojením v rámci displeje povolen. Jeho povolením vlivem poruchy by však došlo k výrazné změně obrazu nezávisle na dalším nastavení tohoto registru. Další nastavení je pro 24bitový barevný režim. Lze zde opět nastavit přesnost řízení napětí pro LCD buňky. Toto nastavení ovlivní vždy celý snímek. Posledním nastavením zde je proud produkovaný vnitřním proudovým zdrojem pro obvody zesilovačů. Toto nastavení ovlivňuje pouze přesnost nastavení jasů jednotlivých buněk, a to celoplošně.

O tomto registru lze říci, že ovlivňuje především přesnost nastavení jasů LCD buněk,

avšak vždy celoplošně, a dále, že dokáže řídit spotřebu řadiče. Tato nastavení nevedou k nebezpečným poruchám.

1.4.3.4 R04h – Input Data and Color Filter Control

V tomto registru jsou poměrně zásadní nastavení. Nastavuje se zde jednak podoba LCD panelu (pruhový, nebo s delta uspořádáním), také barevný režim (RGB, YUV, nebo podle CCIR 656) a režim přenosu dat (barevné složky sériově, nebo paralelně). Dále zde lze určit posun mezi lichým a sudým řádkem, počet automaticky generovaných černých snímků po přivedení napájení a počet řádků v PAL režimu.

Projev případné poruchou způsobené změny barevného režimu je velmi výrazný, protože kódování obrazu je v ostatních režimech než je RGB velmi odlišné. Takováto porucha je velmi snadno obsluhou rozpoznatelná a nezpůsobí tak nebezpečnou poruchu celého systému. Ostatní nastavení nemají v použitém RGB režimu žádný účinek na zobrazení.

1.4.3.5 R05h – Function Control

V tomto registru se nastavuje nepoužitý modul PWM, zapíná či vypíná funkce ditheringu zlepšující barevné přechody. Dále se zde nastavují polarity a význam synchronizačních signálů na obrazovém vstupu. Poslední nastavení se týkají signálů pro hradla TFT tranzistorů. Zde lze nastavit chování napájecího napětí pro hradla ve sleep módu, výši ovládacích napětí a zda mají být trvale všechna hradla připojena ke kladnému ovládacímu napětí.

Případné poruchy tohoto registru buď nepřinesou významnou změnu obrazu (dithering), nebo je změna celoplošná a stejná pro všechny barevné složky.

1.4.3.6 R0Ah – Contrast/Brightness Control

Zde se nastavuje jas a kontrast pro celý displej, změna ovlivňuje zobrazení celoplošně a ve všech barevných kanálech stejně.

1.4.3.7 R0Bh – Frame Cycle Control

Tento registr nastavuje časování vzhledem k LCD panelu. Toto nastavení má stejný vliv na celý panel, bez rozlišení barevných složek, nezpůsobí tedy nebezpečnou poruchu.

1.4.3.8 R0Dh a R0Eh – Power Control 2 a 3

Zde se nastavují úrovně napájení pro ovládání LCD matice. I toto nastavení působí celoplošně bez rozlišení barevných složek (na všechny složky stejně).

1.4.3.9 R0Fh – Gate Scan Position Control

V tomto registru se nastavuje, na který řádek LCD matice se má vykreslit první řádek příchozích dat, přičemž řádky, které se vlivem tohoto posunu na displej nevejdou, se vykreslí od horního řádku matice směrem dolů. Poslední řádek přijatých dat tak bude přímo o jeden řádek nad prvním řádkem přijatých dat. Případnou poruchu tohoto registru je nutno uvážit při návrhu zobrazované grafiky.

1.4.3.10 R16h – Horizontal Porch Control

Toto nastavení udává počet obrazových buněk (trojic LCD buněk s RGB filtry) v jednom řádku. Případná porucha se projeví bočním oříznutím obrazu.

1.4.3.11 R17h – Vertical Porch Control

Zde se nastavuje počet neplatných obrazových bodů na začátku řádku a počet neplatných řádků na začátku snímku. Obě nastavení můžou při poruše způsobit oříznutí snímku. Dále se zde nastavuje časování pro nepoužívaný způsob přenosu obrazových dat.

1.4.3.12 R1Eh – Power Control 4

V tomto registru je možné přepsat hodnotu napětí použitého pro ovládání hradla TFT tranzistorů. Výchozí hodnota je zapsána v jednou programovatelné paměti (OTP). Změna hodnoty ovlivní celý snímek, stejnoměrně všechny barevné složky.

1.4.3.13 R30h až R37h – Gamma Control 1

Zde se dají nastavit gamma korekce pro jas všech buněk LCD. Nastavení působí stejným způsobem na celý panel a na všechny barevné složky.

1.4.3.14 R3Ah a R3Bh – Gamma Control 2

I v těchto registrech se nastavují gamma korekce platné pro celou matici bez rozlišení barev.

2 Popis nebezpečných poruch zadaného systému a cílů bezpečnosti

V této kapitole jsou popsány poruchy, které mohou být v daném zobrazovacím systému z pohledu technické bezpečnosti považovány za nebezpečné. Nejprve je potřeba se krátce zamyslet, které poruchy mají být považovány za nebezpečné. Obecně lze říci, že jsou to takové poruchy, které způsobí, že obsluha dostane chybnou informaci, která méně omezuje činnost uživatele, než správná informace. Například pokud je zobrazena informace o vyšší povolené rychlosti než je skutečná, delší vzdálenost k rychlostnímu omezení, nebo když při nouzových obsluhách zabezpečovacího zařízení je kolejový úsek označen jako volný. V tomto případě, pokud není činnost obsluhy kontrolována, dochází k nebezpečí vzniku nepřijatelných následků.

Protože absolutní bezpečnost je reálně nedosažitelná a zpravidla s dalším zvyšováním bezpečnosti neúměrně rostou náklady, je nutné stanovit cíle bezpečnosti. Pokud zařízení splní tyto cíle, lze je považovat za dostatečně bezpečné. To neznamená absolutní bezpečnost zařízení, pouze neexistenci nepřípustného rizika vzniku škod vlivem činnosti zařízení.

2.1 Nebezpečné poruchy

Jak je napsáno výše, nebezpečné jsou ty poruchy, které způsobí chybné informování obsluhy, že může provést operaci, kterou by podle správných informací provést nemohla. Pokud je ovšem provedení takové operace dále hlídáno jiným systémem, který její provedení nedovolí, pak takovéto chybné informování není přímo nebezpečné, pouze provozně nepříjemné. Protože se zabezpečovací zařízení buduje, aby zabránilo nebezpečím vznikajícím z omylů obsluhy, je snaha většinu příkazů obsluhy kontrolovat na přípustnost, přesto v některých případech (například při nouzových obsluhách, nebo u vlakových zabezpečovačů s omezeným rozsahem informací z traťové části) tato kontrola není možná a je proto důležité v takovýchto aplikacích analyzovat nebezpečné poruchy a stanovovat postupy a opatření k jejich eliminaci.

Aby bylo možné stanovit nebezpečné poruchy, je třeba se také zamyslet nad způsoby kódování informace do obrazu. Jde o dva základní principy. Prvním principem je zakódo-

vání pomocí tvaru. To může být například osmiúhelník značky stop, ale i písmena či text (například omezení rychlosti na železnici či na silnicích v USA). Druhým principem je využití barvy, například červená s významem stůj na návěstidlech. Na grafických displejích se s oblibou využívá kombinace obou principů, tedy jak barvy, tak tvaru. Obzvlášť u bezpečného zobrazení je to vhodné, jednak pro lepší srozuminelnost vůči obsluze a jednak pro menší náchylnost takového zobrazení k nebezpečným poruchám.

Dalším důležitým faktem je také vztah zobrazovaných informací k času. Zde lze říci, že elektronická zobrazovací zařízení má smysl používat pouze u proměnných informací, tedy informací, které se v průběhu času mění.

Následující seznam uvádí možné nebezpečné poruchy zadaného systému. Poruchy vycházejí z výše uvedené slovní definice nebezpečné poruchy, základních principů grafického kódováni informací a vztahu těchto informací k času. Při stanovení nebezpečných poruch bylo také přihlédnuto k možnostem opatření eliminujících tyto poruchy, což vedlo k rozdělení některých poruch na dvě. Analýza vedoucí ke stanovení těchto poruch není součástí této práce, seznam poruch byl zadán společně s architekturou celého systému.

P1 Uchování zastaralého neplatného obrazu na displeji

P2 Uchování zastaralých neplatných dat v paměti řadiče

P3 Chybná data v paměti řadiče způsobující zobrazení chybné informace

P4 Kompletní výpadek jedné barevné složky způsobující nebezpečnou změnu barev nebo kompletní chybná aktivace barevné složky způsobující nebezpečnou změnu barev

P5 Kompletní záměna barev způsobující nebezpečnou změnu informace

P6 Obsluhou nerozpoznatelná modifikace části obrazu způsobující chybnou interpretaci informace

V následujícím textu jsou tyto poruchy blíže popsány.

2.1.1 P1 – Uchování zastaralého neplatného obrazu na displeji

Tato porucha znamená, že přestože jsou do řadiče zapsána aktuální obrazová data, vlivem poruchy displej zobrazuje stále stejný, neaktuální snímek. Pokud došlo ke změně informace

na více omezující, obsluha stále vidí a jedná podle méně omezující zastaralé informace. Tím dojde k nebezpečí.

Tato porucha může nastat jak ve výkonné části řadiče, tak v displeji a jeho ovladači.

2.1.2 P2 – Uchování zastaralých neplatných dat v paměti řadiče

Tato nebezpečná porucha má stejné důsledky jako předchozí porucha, ale jiné příčiny a jiné postupy pro její eliminaci. Zde je základním mechanizmem poruchy situace, kdy nedojde k zápisu nového snímku do paměti řadiče. Řadič tedy stále generuje obrazový signál pro starý snímek a displej jej správně zobrazuje.

Tato porucha se může vyskytnout pouze v řadiči, nebo v komunikaci mezi řadičem a bezpečným výpočetním jádrem.

2.1.3 P3 – Chybná data v paměti řadiče způsobující zobrazení chybné informace

Vlivem této poruchy může dojít ke změně jak barvy, tak tvaru zobrazovaných indikátorů. Může zde dojít prakticky k jakékoliv modifikaci snímku, tedy nejen k drobným změnám na úrovni jednotlivých pixelů, ale také k zopakování části snímku, zrcadlení, nebo zobrazení zcela náhodné (i smysluplné) informace.

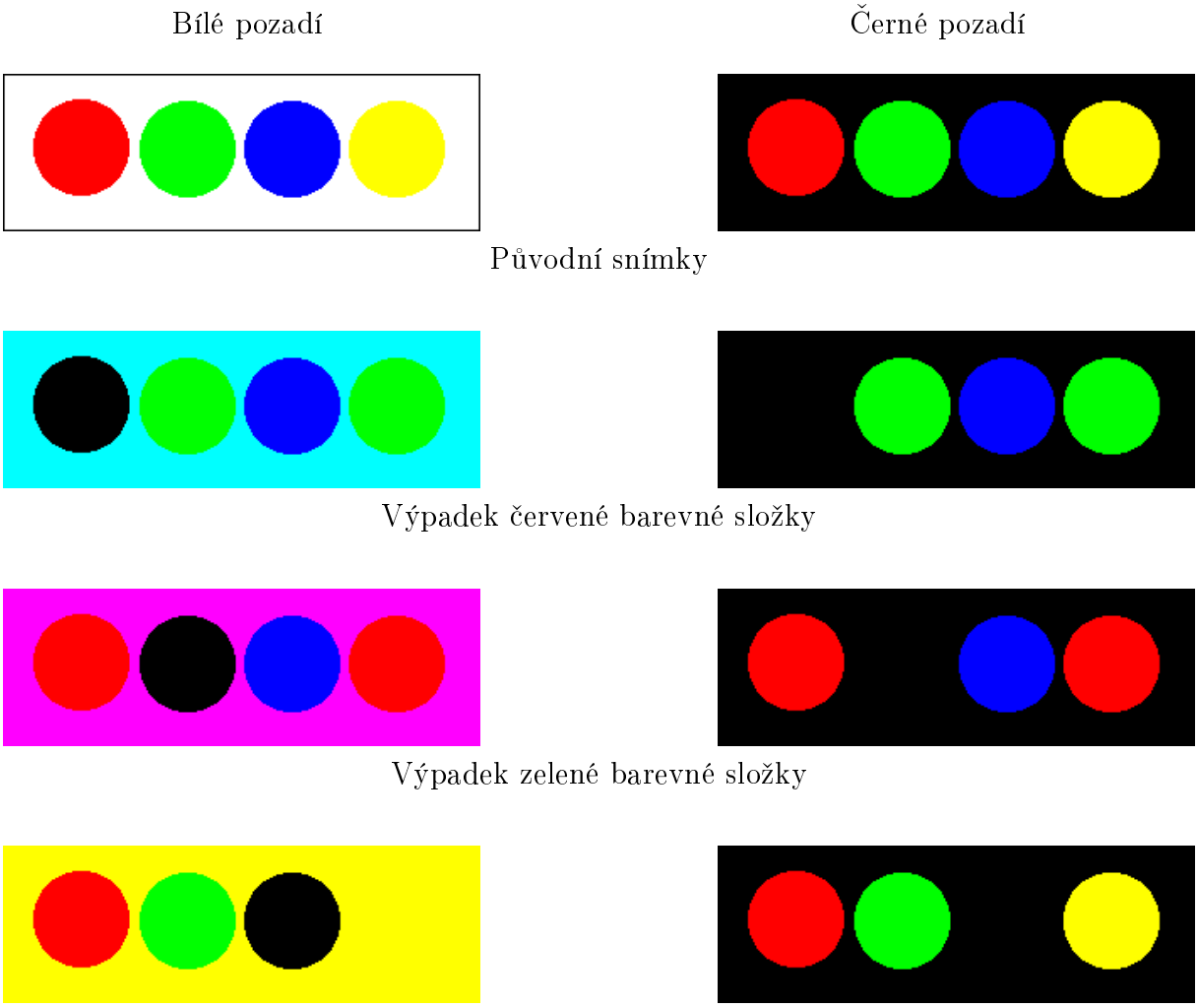
I tato porucha se může vyskytnout pouze v řadiči, nebo v komunikaci mezi bezpečným jádrem a řadičem.

2.1.4 P4 – Kompletní výpadek nebo kompletní chybná aktivace barevné složky

Kompletní výpadek či kompletní chybná aktivace barevné složky způsobí změnu některých barev snímku. Tato změna může být nebezpečná, pokud je informace zakódovaná pouze barvou indikátoru. Ovšem i v případě, že se indikátory liší i tvarově, je dobré považovat tuto poruchu za nebezpečnou, protože při potřebě rychlého rozhodování obsluhy a pouze letmém pohledu obsluhy na zařízení může dojít k omylu obsluhy jen na základě barvy. Ne všechny takto způsobené změny barev jsou nebezpečné, v některých případech dojde změnou barvy k zobrazení naopak více omezující informace, nebo se změna projeví velmi výrazně a na první pohled rozpoznatelně.

Následující příklady demonstrují změny snímků způsobené nežádoucím výpadkem či

aktivací jedné barvy a to jak s černým, tak s bílým pozadím. Pro jednoduchost jsou na snímku jako indikátory zobrazeny pouze barevné kruhy základních barev pro hlavní návěstidla, jde pouze o ilustraci čtenáři, jaký dopad může porucha mít. Při implementaci bezpečného zobrazení v reálném systému by bylo třeba analyzovat konkrétní případy zobrazovaných indikátorů.

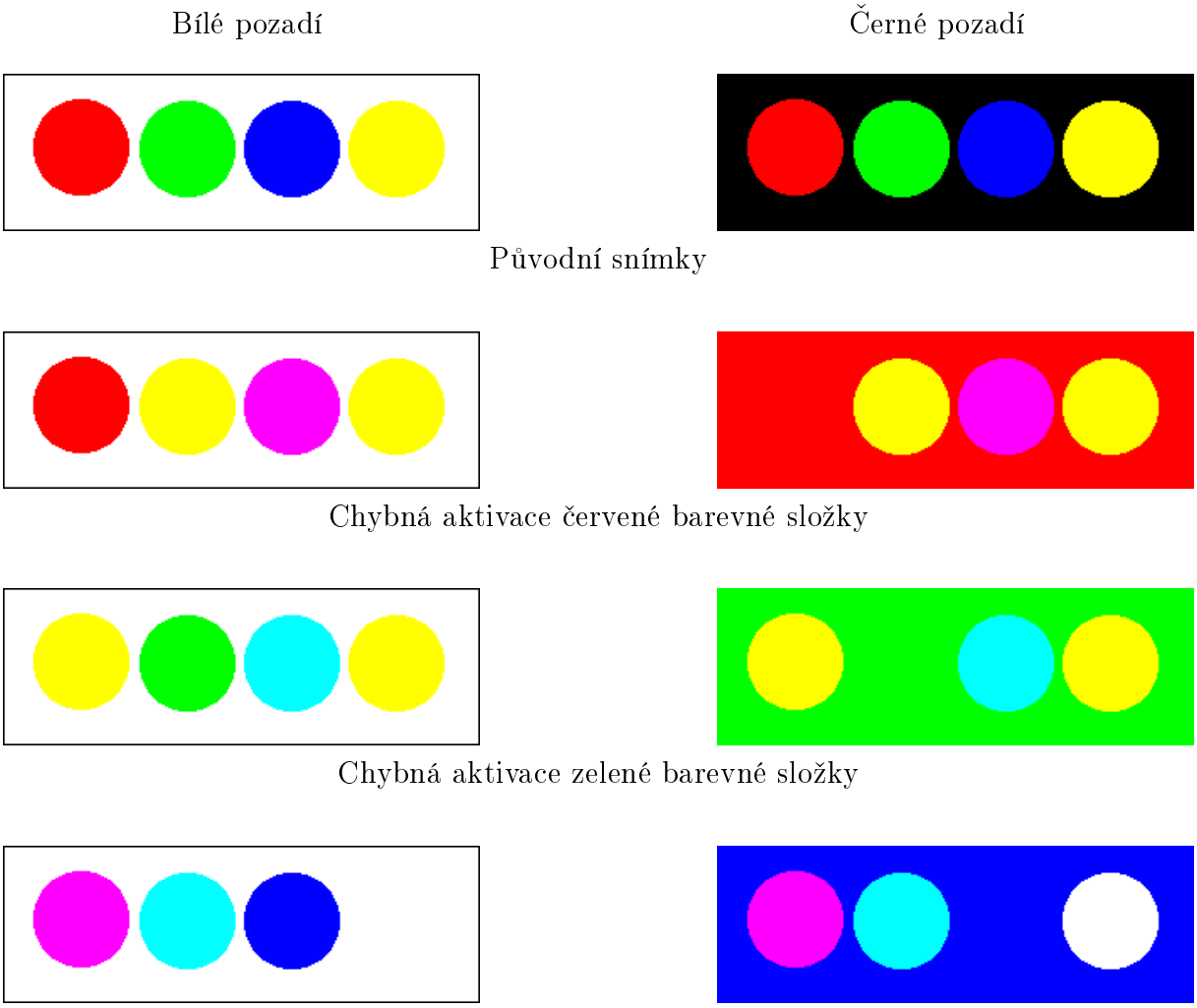


Obrázek 2.1: Ilustrace výpadků barevných složek

K této poruše může dojít ve výkonné části řadiče, nebo v displeji a jeho ovladači.

2.1.5 P5 – Kompletní záměna barev způsobí nebezpečnou změnu informace

Tato porucha je sice podobná předchozí poruše, ale liší se rozpoznatelností svého projevu. Zatímco v předchozím případě docházelo i k ovlivnění více barev, i černé či bílé barvy, v tomto případě budou ovlivněny pouze ty části snímku, kde je použita zaměněná



Obrázek 2.2: Ilustrace chybných aktivací barevných složek

barva, nebo v případě, že dojde k záměně barevných složek, ty části snímku, kde hodnoty zaměněných složek nebyly stejné, protože u ostatních nebude změna viditelná. Pokud budou hodnoty zaměněných složek vzájemně blízké, je možné, že změna bude velmi těžko postřehnutelná.

Následující obrázky demonstrují barevné změny v případě záměny barevných složek. Původní snímky jsou stejné jako v předchozím případě, nejsou proto znovu uvedeny. Snímky, kde by došlo k záměně jedné konkrétní barvy, zde uvedeny nejsou, možné důsledky této záměny není obtížné si představit.

K této poruše může dojít v přenosu mezi bezpečným výpočetním jádrem a řadičem, v řadiči, v přenosu mezi řadičem a displejem či v ovladači displeje. Ve vlastním LCD panelu je tato porucha vzhledem k jeho struktuře nepravděpodobná.

Bílé pozadí Černé pozadí

Pro zelenou složku jsou použita data pro červenou složku

Pro modrou složku jsou použita data pro červenou složku

Pro červenou složku jsou použita data pro zelenou složku

Pro modrou složku jsou použita data pro zelenou složku

Pro červenou složku jsou použita data pro modrou složku

Pro zelenou složku jsou použita data pro modrou složku

Obrázek 2.3: Ilustrace záměny barevných složek

Bílé pozadí

Černé pozadí

Zelená a červená složka jsou vzájemně prohozeny

Modrá a červená složka jsou vzájemně prohozeny

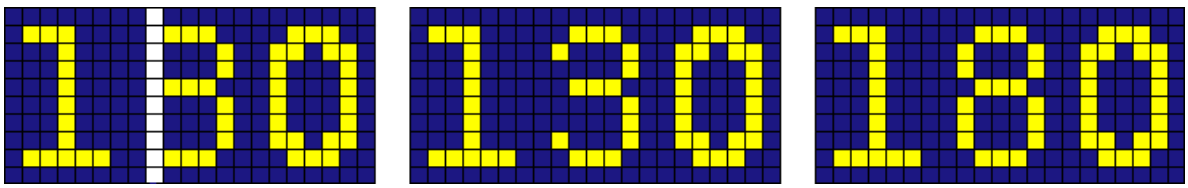
Zelená a modrá složka jsou vzájemně prohozeny

Obrázek 2.4: Ilustrace záměny barevných složek

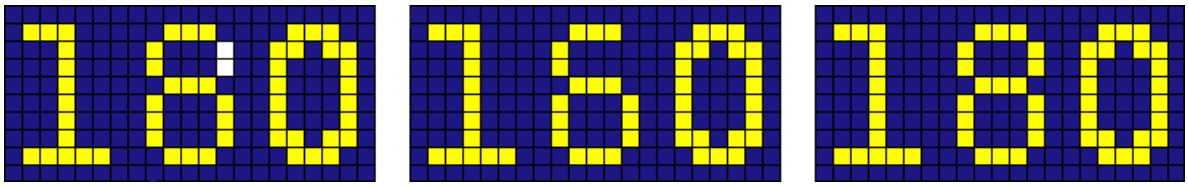
2.1.6 P6 – Obsluhou nerozpoznatelná modifikace části obrazu

Tato porucha je sice podobná nežádoucí modifikaci dat ve videoRAM, její příčiny, důsledky a především možnosti eliminace jsou odlišné a proto je zde zkoumána odděleně.

Projevy této poruchy budou především drobné výpadky částí obrazu, jako jsou spíše výpadky či chybná aktivace jednotlivých LCD buněk, řádků či sloupců, nebo různě velkých shluků. Tato porucha může být nebezpečná především u informací kódovaných tvarem, zejména písmen či číslic, případně drobnými grafickými elementy. Následující obrázky demonstrují možný nebezpečný projev této poruchy, kdy původní číslo 130 lze snadno zaměnit za 180, nebo číslo 160 za 180.



Obrázek 2.5: Chybná aktivace sloupce LCD buněk může vést k záměně čísla 130 za 180



Obrázek 2.6: Chybná aktivace dvou LCD buněk může vést k záměně čísla 160 za 180

2.2 Cíle bezpečnosti

V této části jsou specifikovány cíle, kterých je potřeba dosáhnout, aby zařízení s přihlédnutím k vývojovým, výrobním a provozním nákladům, ale také ke spolehlivostním požadavkům a požadavkům na ergonomii, splňovalo požadované bezpečnostní standardy. Jsou zde popsány cíle ze všech zmíněných oblastí, přičemž pouze bezpečnostní cíle je nutno naplnit beze zbytku. Ostatní nemusí být zcela naplněny (v některých případech to není možné, protože jsou cíle vzájemně protichůdné), ale vždy je třeba se snažit o co největší míru naplnění všech cílů.

2.2.1 Bezpečnostní cíle

Základním bezpečnostním požadavkem u železničního zabezpečovacího zařízení je bezpečná reakce v případě, že je detekována potenciálně nebezpečná porucha. Při této bezpečné reakci musí být zaveden buď degradovaný režim zařízení nebo jeho bezpečná odstávka, tak aby byla zachována bezpečnost. Tyto degradované režimy, či stav kdy je část či celé zařízení bezpečně odstaveno, není možné dlouhodobě používat při běžném provozu, protože tyto režimy jsou často silně provozně omezující (často vlivem tohoto stavu dochází k úplnému přerušení železničního provozu). V případě zadaného systému lze za takovouto bezpečnou reakci považovat navození situace, kdy na displeji není zobrazena žádná informace a obsluha se dále řídí administrativními opatřeními pro tuto situaci. Touto bezpečnou reakcí ve smyslu výše uvedené definice je v případě zadaného systému bezpečné odpojení napájecího napětí displeje, jeho podsvětlení a řadiče, protože tím nejsou generovány signály pro nastavení jednotlivých buněk LCD panelu a po krátké době dojde k návratu tekutých krystalů do výchozího uspořádání, čímž dojde ke smazání snímku z displeje. Navíc odpojením napájení LED podsvícení dojde ke zhasnutí displeje. Důležité je zařídit, aby se zařízení nemohlo vrátit z degradovaných režimů, či z bezpečné odstávky do běžného provozního či méně degradovaného režimu jinak než řízeným způsobem. Pro

vyvození bezpečné reakce v zadaném systému je možné použít existující bezpečné zdroje napětí, jejichž bližší popis je již nad rozsah této práce.

Dalším obecným požadavkem je snížení intenzity výskytu nebezpečných poruch. Obecně je třeba snažit se vždy o maximální snížení této intenzity, ale to není vždy ekonomicky rozumné, protože náklady na další snižování této intenzity prudce stoupají. Proto je nutné stanovit některou z vhodných metodik pro každou bezpečnostní funkci nejvyšší tolerovatelnou intenzitu poruch (THR). Toto stanovení je nad rámec této práce, pro zadané zařízení bylo stanoveno $THR = 10^{-7}\ h^{-1}$.

Protože není možné kvantifikovat všechny možné typy poruch, především pak poruchy systematické, stanovují normy opatření a postupy, které je doporučeno během návrhu a vývoje použít, aby bylo v dostatečné míře zabráněno vzniku těchto typů poruch. Normy ČSN EN 50 126, ČSN EN 50 128 a ČSN EN 50 129 tato opatření dělí do čtyř skupin, podle požadovaného THR, takzvané úrovně integrity bezpečnosti, zkráceně SIL. Pro zadaný parametr $THR = 10^{-7}\ h^{-1}$ odpovídají opatření na úrovni SIL 2.

Zadané THR a jemu příslušná úroveň SIL navíc můžou být nejvyšší rozumně dosažitelnou úrovní bezpečnosti, protože zařízení je sestaveno z běžných součástek, které samy o sobě nezajišťují vyšší bezpečnostní standardy, a protože nelze na celý systém použít postupy složené, reaktivní či inherentní bezpečnosti při poruše. Další zvýšení úrovně bezpečnosti by tak bylo velmi obtížné nebo nemožné.

Dalším základním bezpečnostním parametrem v případě použití reaktivní bezpečnosti při poruše je nejdelší přípustná doba výskytu potenciálně nebezpečného stavu. Bezporuchový stav musí být s dostatečnou intenzitou kontrolován a je-li detekována porucha, musí být včas zavedena negace vedoucí k znovuzavedení bezpečného stavu (například bezpečnou odstávkou části zařízení zasažené poruchou), aby nedošlo k nadlimitnímu trvání nebezpečného stavu. Tento čas se označuje jako maximální doba do detekce a negace nebezpečné poruchy a pro zadané zařízení lze uvažovat vzhledem k předpokládanému použití nejdelší přípustnou dobu pro trvání přechodného potenciálně nebezpečného stavu v jednotkách sekund.

2.2.2 Ostatní cíle

Dalším cílem je, aby bylo zařízení co nejjednodušší, čímž se sníží náklady na vývoj, výrobu a provoz. Také to většinou příznivě ovlivňuje dostupnost zařízení.

Z hlediska ergonomie je cílem používat dobře rozpoznatelné a obtížně zaměnitelné grafické prvky pro zobrazení informací. Je třeba se z tohoto hlediska také pokud možno vyvarovat použití speciálních, především dynamických indikátorů značících stav zařízení, protože tyto indikátory po nějaké době obsluha přestává vnímat a nekontroluje tedy jejich správnou podobu.

3 Identifikace poruchových módů systému vedoucích k nebezpečným poruchám

V této kapitole jsou pomocí FTA stromů k nebezpečným poruchám nalezeny poruchové módy, které mohou danou nebezpečnou poruchu způsobit. Tyto poruchové módy jsou následně popsány tak, aby mohla být navržena opatření k jejich eliminaci, či včasné detekci.

3.1 Identifikátory

Aby bylo snadné dohledat, který poruchový mód patří ke které nebezpečné poruše a kterých částí systému se týká, jsou zavedeny jednoznačné identifikátory. Každý identifikátor začíná označením poruchy, ke které přísluší (P1 až P6), za kterým následují podtržítky oddělená označení součástí a jejich dílčích celků. Označení končí identifikátorem události způsobující nebezpečnou poruchu sestávajícím se z písmene E a pořadového čísla v rámci součásti či dílčího celku. Lze tak vždy dohledat dílčí celek součásti, součást a nebezpečnou poruchu, k níž daná událost patří. Použitá označení součástí a jejich dílčích celků jsou uvedeny v následující tabulce.

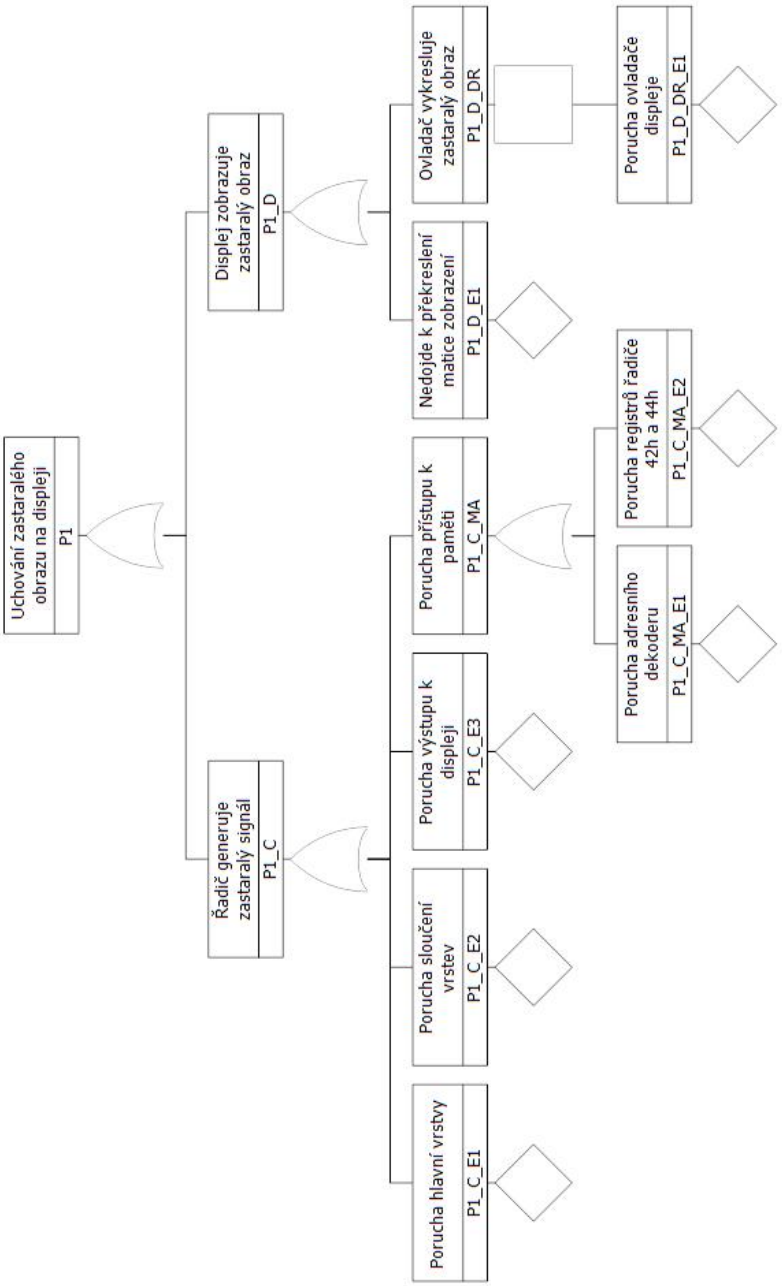
Řadič displeje	C
Výpočetní jádro	K
Displej	D
Vlastní LCD matice	LCD
Multiplexer	M
Ovladač	DR
Paměť řadiče displeje	ME
Řadič paměti řadiče displeje	MA
SPI rozhraní řadiče displeje	SPI
Registry řadiče či ovladače displeje	R
Přenosová cesta mezi výpočetním jádrem a řadičem displeje	IFKC
Přenosová cesta mezi řadičem displeje a displejem	IFCD

Tabulka 3.1: Označení součástí a jejich funkčních celků v identifikátorech

3.2 Poruchové módy pro jednotlivé poruchy

Zde jsou uvedeny diagramy s FTA stromy pro jednotlivé nebezpečné poruchy a popsány jednotlivé události vedoucí k těmto poruchám.

3.2.1 P1 – Uchování zastaralého neplatného obrazu na displeji



Obrázek 3.1: FTA strom nebezpečné poruchy P1 – Uchování zastaralého neplatného obrazu na displeji

3.2.1.1 P1_C_E1 – Porucha hlavní vrstvy

Tato událost způsobí, že řadič nebude převádět data uložená v paměti řadiče displeje na grafický výstup k řadiči, ale sestaví jiný obraz, například z neaktuálních dat uložených ve své pracovní paměti.

3.2.1.2 P1_C_E2 – Porucha sloučení vrstev

Zde může dojít také k tomu, že řadič vygeneruje nesprávný videovýstup, například použitím dat z pracovní paměti jednotky pro slučování vrstev, nebo použitím dat z chybně aplikované vrstvy obraz v obraze.

3.2.1.3 P1_C_E3 – Porucha výstupu k displeji

V tomto případě opět bude řadič displeje generovat nesprávný videovýstup, zde však vlivem jednotky generující tento výstup, například pokud by jednotka použila zastaralá data ze své pracovní paměti.

3.2.1.4 P1_C_MA_E1 – Porucha adresního dekoderu

Vlivem této poruchy může dojít k situaci, kdy výpočetní jádro zapíše aktuální obrazová data na jiné místo do paměti řadiče displeje, než odkud je čtou jednotky generující videovýstup. Tím by došlo k zobrazení zastaralých dat.

3.2.1.5 P1_C_MA_E2 – Porucha registrů řadiče 42h a 44h

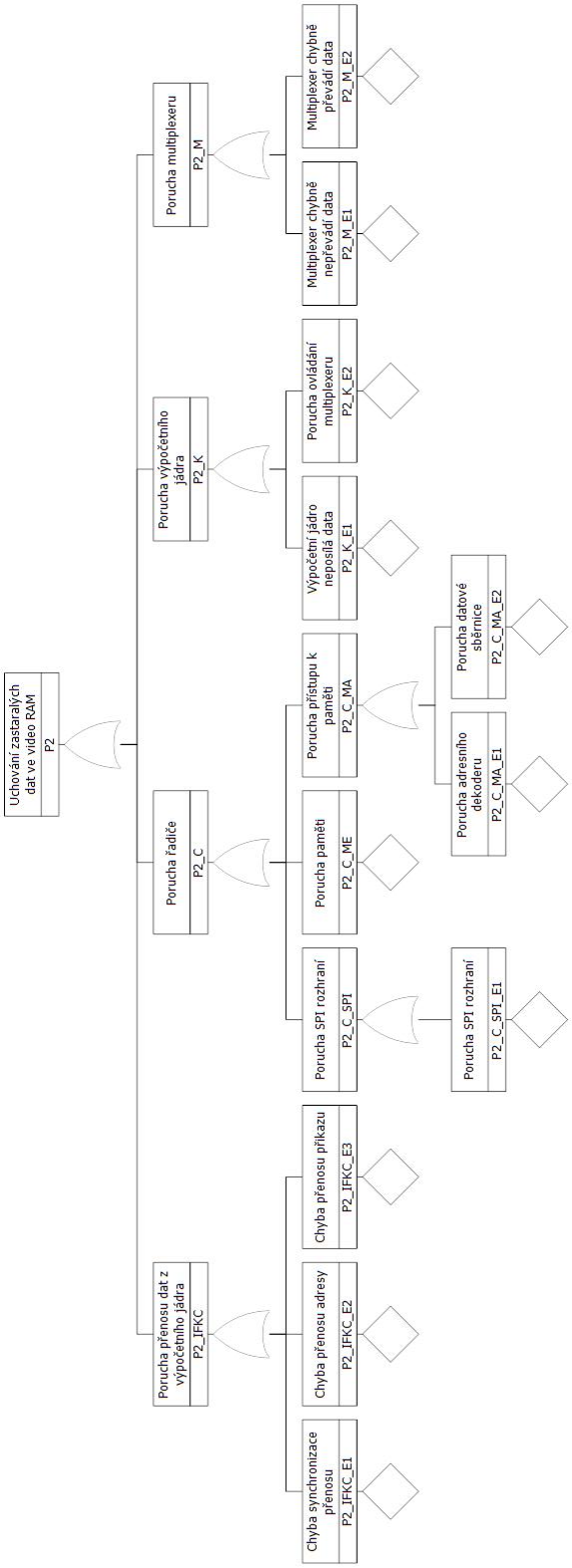
Tato porucha by mohla způsobit, že jednotky generující videovýstup čtou data z jiné oblasti paměti, než kam je ukládá výpočetní jádro. Pokud by na takovém místě byla zastaralá data, bude z nich vygenerován chybný videovýstup.

3.2.1.6 P1_D_E1 – Nedojde k překreslení matice zobrazení

V tomto případě i přes správné generování signálů pro LCD matici nedojde ke změně natočení krystalů a tím zůstane zobrazen zastaralý obraz.

3.2.1.7 P1_D_DR_E1 – Porucha ovladače displeje

Zde by došlo vlivem poruchy k situaci, kdy ovladač displeje dostává aktuální obrazový signál, ale generuje signály pro ovládání LCD matice se zastaralým obrazem.



Obrázek 3.2: FTA strom nebezpečné poruchy P2 – Uchování zastaralých neplatných dat v paměti řadiče

3.2.2 P2 – Uchování zastaralých neplatných dat v paměti řadiče

3.2.2.1 P2_IFKC_E1 – Chyba synchronizace přenosu

Chybou synchronizace přenosu může dojít k neočekávanému zkrácení přenosu, nebo k příjmu nesmyslných dat. Nedojde tak k přepsání části či celého obrazu v paměti řadiče displeje, nebo je obraz přepsán chybnými daty. Výpočetní jádro tuto chybu nedokáže během přenosu zjistit.

3.2.2.2 P2_IFKC_E2 – Chyba přenosu adresy

Pokud je přenesená adresa zatížena chybou, budou data zapsána na chybné místo v paměti řadiče displeje, obraz tak nebude přepsán, nebo bude přepsán pouze částečně a to daty prostorově posunutými. Výpočetní jádro tuto chybu nedokáže během přenosu zjistit.

3.2.2.3 P2_IFKC_E3 – Chyba přenosu příkazu

Vlivem chyby přenosu příkazu nedojde vůbec k zápisu aktuálních obrazových dat do paměti řadiče displeje. Výpočetní jádro tuto chybu nedokáže během přenosu zjistit.

3.2.2.4 P2_C_SPI_E1 – Porucha SPI rozhraní

Porucha SPI rozhraní může způsobit, že i přes správně přijatý příkaz a adresu nedojde k zápisu aktuálních dat do paměti řadiče displeje, případně budou zapsána chybná data, nebo budou zapsána data na chybnou adresu v paměti řadiče.

3.2.2.5 P2_C_MA_E1 – Porucha adresního dekoderu

Vlivem poruchy adresního dekoderu řadiče paměti řadiče displeje může dojít k zápisu dat na špatnou adresu v paměti řadiče displeje, což může způsobit poškození, nebo úplné nepřepsání dat v oblasti, ze které je generován obraz.

3.2.2.6 P2_C_MA_E2 – Porucha datové sběrnice

Poruchou datové sběrnice řadiče paměti řadiče displeje může dojít k zanesení chyby do zapisovaných dat, nebo i nezapsání dat.

3.2.2.7 P2_C_ME – Porucha paměti

I zde může dojít k tomu, že vlivem poruchy paměti nebudou data zapsána, nedojde tedy k aktualizaci obrazových dat a tím i obrazu.

3.2.2.8 P2_K_E1 – Výpočetní jádro neposílá data

V tomto případě vlivem poruchy výpočetní jádro vůbec nevysílá aktuální data k zápisu do paměti řadiče displeje, nebo je vysílá s chybným příkazem, či adresou. Do této události spadá také situace kdy výpočetní jádro vysílá data takovým způsobem, že je řadič displeje není schopen přijmout (například při příliš vysoké datové rychlosti).

3.2.2.9 P2_K_E2 – Porucha ovládání multiplexeru

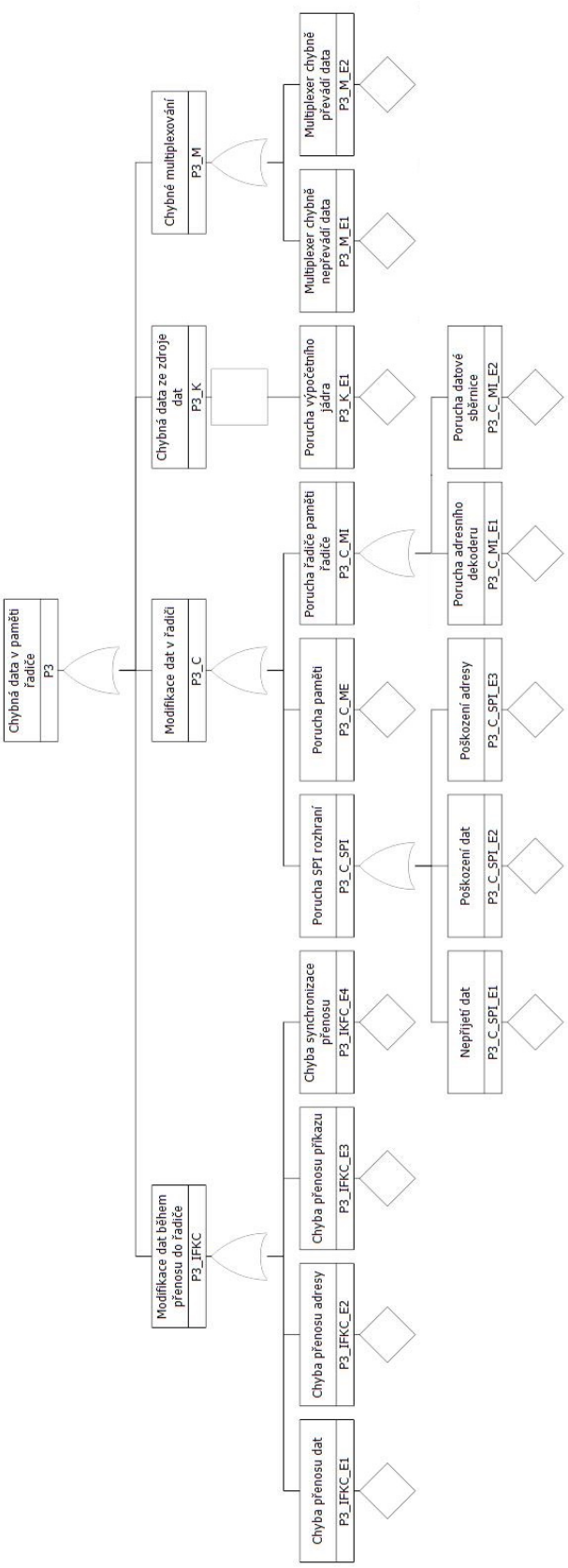
Tato porucha nastane, pokud výpočetní jádro chybným způsobem ovládá multiplexer. Mikrokontroler, který má zapsat data do paměti řadiče displeje, je odpojen od SPI sběrnice řadiče displeje, nebo jsou připojeny oba mikrokontrolery a dochází tak k rušení komunikace. Přenos dat se neuskuteční a data nejsou zapsána do paměti řadiče displeje, nebo dojde k poškození příkazu, adresy či přenášených dat. Tím může být způsobeno, že jsou zapsána chybná data, nebo jsou data zapsána na jinou adresu v paměti řadiče displeje, či dokonce nejsou data zapsána vůbec.

3.2.2.10 P2_M_E1 – Multiplexer chybně nepřevádí data

V tomto případě se nemůže uskutečnit datový přenos, aktuální data tedy nejsou zapsána do paměti řadiče displeje.

3.2.2.11 P2_M_E2 – Multiplexer chybně převádí data

Zde jsou převáděna data z jiného mikrokontroleru než by měla být, může tak dojít k rušení signálů správného mikrokontroleru, což může znemožnit komunikaci, či poškodit přenášený příkaz, adresu či data. Tím může dojít k zápisu chybných dat, zápisu dat na chybnou adresu či k zápisu vůbec nedojde.



Obrázek 3.3: FTA strom nebezpečné poruchy P3 – Chybná data v paměti řadiče způsobující zobrazení chybné informace

3.2.3 P3 – Chybná data v paměti řadiče způsobující zobrazení chybné informace

3.2.3.1 P3_IFKC_E1 – Chyba přenosu dat

Chyba přenosu dat způsobí, že jsou do paměti řadiče displeje zapsána chybná data.

3.2.3.2 P3_IFKC_E2 – Chyba přenosu adresy

Zde dojde k zápisu dat na chybnou adresu. Tím může dojít buď k částečnému přepsání obrazových dat daty prostorově posunutými, nebo k nepřepsání obrazových dat.

3.2.3.3 P3_IFKC_E3 – Chyba přenosu příkazu

Vlivem chybného přenosu příkazu nedojde k přepsání obrazových dat, nebo budou data zapsána v nesprávném pořadí.

3.2.3.4 P3_IKFC_E4 – Chyba synchronizace přenosu

Tato chyba může způsobit úplné, či částečné nepřepsání obrazových dat v paměti řadiče displeje.

3.2.3.5 P3_C_SPI_E1 – Nepřijetí dat

Porucha SPI jednotky řadiče displeje může způsobit, že nelze přijímat data k zápisu do paměti řadiče displeje.

3.2.3.6 P3_C_SPI_E2 – Poškození dat

Pokud dojde vlivem poruchy jednotky SPI k poškození dat, budou tata poškozená data zapsána do paměti řadiče displeje a obrazová data tak budou chybná.

3.2.3.7 P3_C_SPI_E3 – Poškození adresy

Při poškození adresy v SPI přenosu budou data zapsána na jiné místo v paměti řadiče displeje, čímž může dojít k pouze částečnému přepisu obrazových dat daty prostorově posunutými.

3.2.3.8 P3_C_MI_E1 – Porucha adresního dekoderu

Vlivem poruchy adresního dekoderu může dojít k zápisu dat na špatnou adresu, ale také k promíchání dat.

3.2.3.9 P3_C_MI_E2 – Porucha datové sběrnice

Porucha datové sběrnice řadiče paměti řadiče displeje způsobí, že budou do paměti řadiče displeje zapsána chybná data.

3.2.3.10 P3_C_ME – Porucha paměti

Projevem této obecné poruchy paměti řadiče displeje může být nemožnost zapsat data, nebo zápis poškozených dat, či samovolná modifikace dat.

3.2.3.11 P3_K_E1 – Porucha výpočetního jádra

Vlivem této poruchy může dojít k situaci, kdy výpočetní jádro posílá chybná data do řadiče displeje přes SPI.

3.2.3.12 P3_M_E1 – Multiplexer chybně nepřevádí data

V tomto případě se nemůže uskutečnit datový přenos, aktuální data tedy nejsou zapsána do paměti řadiče displeje.

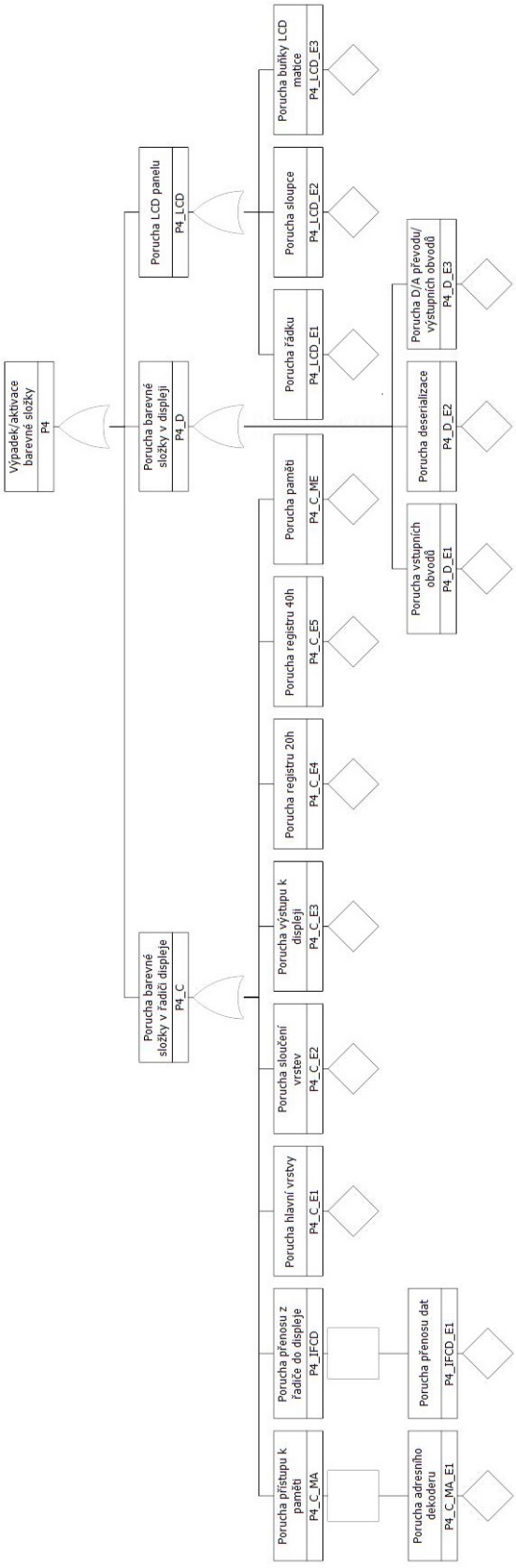
3.2.3.13 P3_M_E2 – Multiplexer chybně převádí data

Zde jsou převáděna data z jiného mikrokontroleru, než by měla být, může tak dojít k rušení signálů správného mikrokontroleru, což může znemožnit komunikaci, či poškodit přenášený příkaz, adresu či data. Tím může dojít k zápisu chybných dat, zápisu dat na chybnou adresu či k zápisu vůbec nedojde.

3.2.4 P4 – Kompletní výpadek nebo kompletní chybná aktivace barevné složky

3.2.4.1 P4_C_E1 – Porucha hlavní vrstvy

Při zpracování dat hlavní vrstvy může dojít vlivem poruchy k výpadku či chybné aktivaci barevné složky.



Obrázek 3.4: FTA strom nebezpečné poruchy P4 – Kompletní výpadek nebo kompletní chybná aktivace barevné složky

3.2.4.2 P4_C_E2 – Porucha sloučení vrstev

Také při slučování hlavní vrstvy s vrstvou obraz v obraze může dojít k výpadku či chybné aktivaci barevné složky.

3.2.4.3 P4_C_E3 – Porucha výstupu k displeji

Porucha výstupních obvodů řadiče displeje může vést k chybě na výstupní datové sběrnici, kdy některé vodiče budou trvale přenášet chybnou hodnotu. Protože jsou jednotlivé vodiče sběrnice při paralelním přenosu barevných složek pevně spojeny s patřičnou barevnou složkou, dojde vlivem této poruchy k aktivaci či výpadku (částečnému nebo i celkovému) patřičné barevné složky.

3.2.4.4 P4_C_E4 – Porucha registru 20h

Poruchou tohoto registru může dojít ke změně šířky výstupní sběrnice. Tím dojde, v závislosti na ostatních nastaveních, k výpadku či aktivaci červené barevné složky.

3.2.4.5 P4_C_E5 – Porucha registru 40h

Tato porucha může způsobit chybnou aktivaci či deaktivaci Look-up tabulky a tím i výpadek či chybnou aktivaci barev.

3.2.4.6 P4_C_ME – Porucha paměti

Tato porucha může při použití Look-up tabulky způsobit, že pro správný barevný index jsou dodány chybné hodnoty barevných složek.

3.2.4.7 P4_C_MA_E1 – Porucha adresního dekoderu

Vlivem této poruchy může dojít k situaci, kdy jsou z paměti čtena některá data z nesprávných adres paměti, což může vést k chybné aktivaci či výpadku barevné složky. Při použití Look-up tabulky může také dojít k načtení hodnoty barevných složek z jiného umístění než udává barevný index v paměti.

3.2.4.8 P4_IFCD_E1 – Porucha přenosu dat

Zde může dojít ke klasické poruše na paralelní sběrnici. Protože jsou vodiče této sběrnice pevně přiřazeny jednotlivým barevným složkám, může vlivem této poruchy dojít k chybné

aktivaci či výpadku barevné složky.

3.2.4.9 P4_D_E1 – Porucha vstupních obvodů

Tato porucha je podobná předchozí poruše přenosu dat, i zde může dojít k poruše na části paralelní sběrnice přenášející data do ovladače displeje. Může zde také dojít k poruše převodu signálů na data.

3.2.4.10 P4_D_E2 – Porucha deserializace

Při deserializaci vstupních dat může také dojít k výpadku či chybné aktivaci barevné složky.

3.2.4.11 P4_D_E3 – Porucha D/A převodu nebo výstupních obvodů

Porucha D/A převodu může vést k výpadku či chybné aktivaci sloupce subpixelů v zobrazení. Každý subpixel má svoji základní barvu (RGB, stejnou pro celý sloupec) a tak může dojít k výpadku či chybné aktivaci barevné složky sloupce pixelů.

3.2.4.12 P4_LCD_E1 – Porucha řádku

Touto poruchou může dojít k výpadku jednoho řádku displeje, nebo také k situaci kdy jsou postupně na tomto řádku, během jednoho snímku, zobrazeny všechny řádky.

3.2.4.13 P4_LCD_E2 – Porucha sloupce

Zde může dojít k chybnému konstantnímu zobrazení v jednom sloupci (přesněji v jedné jeho barevné složce).

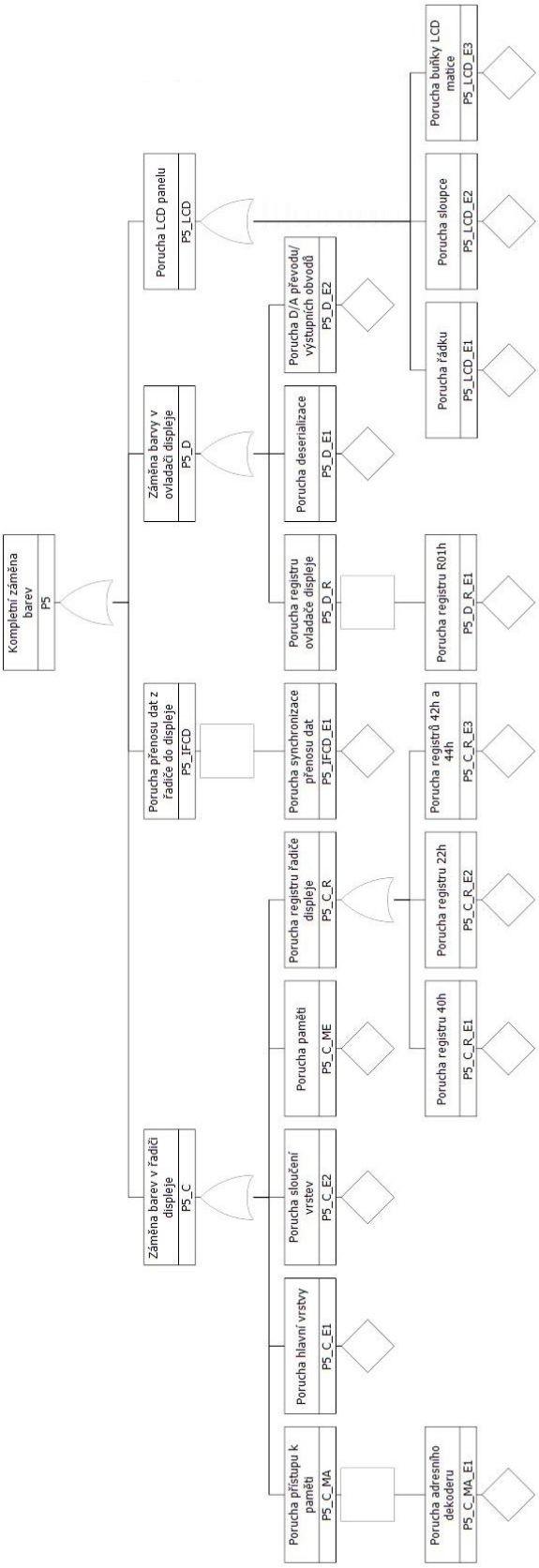
3.2.4.14 P4_LCD_E3 – Porucha buňky LCD matice

Porucha buňky LCD matice se projeví jako konstatntní chybná jasová hodnota jednoho subpixelu (jedné barevné složky jednoho obrazového bodu).

3.2.5 P5 – Kompletní záměna barev způsobí nebezpečnou změnu informace

3.2.5.1 P5_C_E1 – Porucha hlavní vrstvy

Při zpracování dat hlavní vrstvy může dojít vlivem poruchy k záměně barev.



Obrázek 3.5: FTA strom nebezpečné poruchy P5 – Kompletní záměna barev způsobí nebezpečnou změnu informace

3.2.5.2 P5_C_E2 – Porucha sloučení vrstev

Také při slučování hlavní vrstvy s vrstvou obraz v obraze může dojít k záměně barev.

3.2.5.3 P5_C_R_E1 – Porucha registru 40h

Tato porucha může způsobit chybnou aktivaci či deaktivaci Look-up tabulky a tím i záměnu barev.

3.2.5.4 P5_C_R_E2 – Porucha registru 22h

Poruchou tohoto registru může dojít k inverzi barev.

3.2.5.5 P5_C_R_E3 – Porucha registrů 42h a 44h

Vlivem poruchy především registru 42h může dojít k posunu začátku obrazového bufferu. V některých barevných režimech může při určitých posunech dojít k záměně jednotlivých barevných kanálů.

3.2.5.6 P5_C_ME – Porucha paměti

Tato porucha může při použití Look-up tabulky způsobit, že pro správný barevný index jsou dodány chybné hodnoty barevných složek.

3.2.5.7 P5_C_MA_E1 – Porucha adresního dekoderu

Vlivem této poruchy může dojít k situaci, kdy jsou z paměti čtena některá data z nesprávných adres paměti, což může vést k záměně barevných složek. Při použití Look-up tabulky může také dojít k načtení hodnoty barevných složek z jiného umístění, než udává barevný index v paměti.

3.2.5.8 P5_IFCD_E1 – Porucha synchronizace přenosu dat

Vlivem poruchy synchronizace přenosu dat do ovladače displeje může při sériovém režimu přenosu barevných složek dojít k záměně barevných složek.

3.2.5.9 P5_D_E1 – Porucha deserializace

Při deserializaci vstupních dat může také dojít k záměně barevných složek.

3.2.5.10 P5_D_E2 – Porucha D/A převodu nebo výstupních obvodů

Poruchou D/A převodu může vést k chybné hodnotě jasu sloupce subpixelů v zobrazení. Každý subpixel má svoji základní barvu (RGB, stejnou pro celý sloupec) a tak může dojít k záměně barev v rámci jednoho sloupce.

3.2.5.11 P5_D_R_E1 – Porucha registru R01h

Poruchou tohoto registru může dojít k prohození červeného a modrého barevného kanálu, nebo k inverzi všech barev.

3.2.5.12 P5_LCD_E1 – Porucha řádku

Touto poruchou může dojít k zobrazení chybné hodnoty jasu v jednom řádku.

3.2.5.13 P5_LCD_E2 – Porucha sloupce

Zde může dojít k chybné hodnotě jasu v jednom sloupci (přesněji v jedné jeho barevné složce).

3.2.5.14 P5_LCD_E3 – Porucha buňky LCD matice

Porucha buňky LCD matice se projeví jako konstatntní chybná jasová hodnota jednoho subpixelu (jedné barevné složky jednoho obrazového bodu).

3.2.6 P6 – Obsluhou nerozpoznatelná modifikace části obrazu způsobující chybnou interpretaci informace

3.2.6.1 P6_C_E1 – Porucha hlavní vrstvy

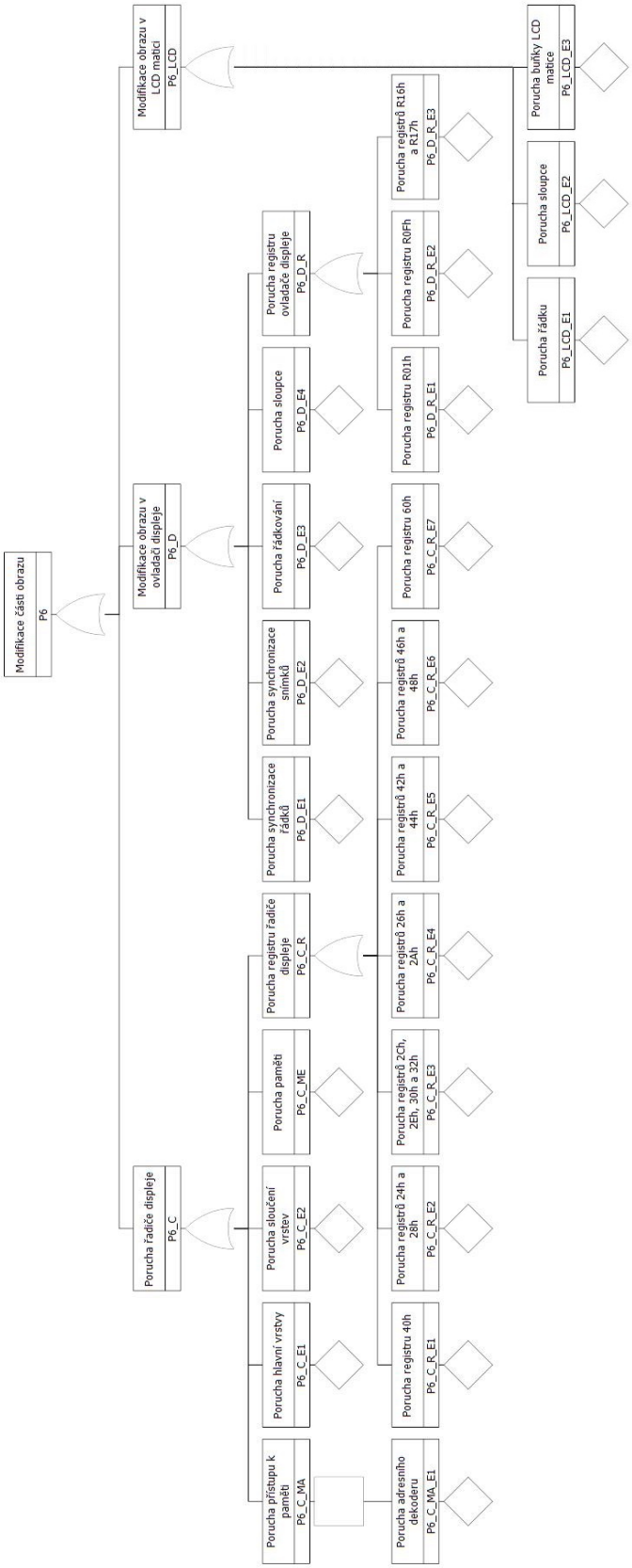
Při zpracování dat hlavní vrstvy může dojít vlivem poruchy k modifikacím obrazu.

3.2.6.2 P6_C_E2 – Porucha sloučení vrstev

Také při slučování hlavní vrstvy s vrstvou obraz v obraze může dojít k modifikaci obrazu.

3.2.6.3 P6_C_R_E1 – Porucha registru 40h

Tato porucha může způsobit otočení a tím také deformaci obrazu.



Obrázek 3.6: FTA strom nebezpečné poruchy P6 – Obsluhou nerozpoznatelná modifikace části obrazu způsobující chybnou interpretaci informace

3.2.6.4 P6_C_R_E2 – Porucha registrů 24h a 28h

Poruchou těchto registrů dojde ke změně šířky či výšky obrazu v generovaném videosignálu. Tímto může dojít k ořezání zobrazení.

3.2.6.5 P6_C_R_E3 – Porucha registrů 2Ch, 2Eh, 30h a 32h

Následkem poruchy těchto registrů by mohl být posun obrazu na displeji.

3.2.6.6 P6_C_R_E4 – Porucha registrů 26h a 2Ah

Zde může vlivem poruchy dojít k situaci, kdy displej nezvládne řadičem generovaný signál správně zpracovat. Tím může dojít také k deformaci celého obrazu.

3.2.6.7 P6_C_R_E5 – Porucha registrů 42h a 44h

Vlivem poruchy především registru 42h může dojít k posunu začátku obrazového bufferu. Tím dojde k nezobrazení některých (případně i všech) dat a zobrazení obsahu jiné části paměti řadiče displeje. Pokud by v této části byla smysluplná data, byla by korektně zobrazena.

3.2.6.8 P6_C_R_E6 – Porucha registrů 46h a 48h

Zde vlivem poruchy může dojít ke změně velikosti obrazu generovaného ze vstupních dat a tím k deformaci obrazu (přeskládání nesprávně dlouhých řádků) či dokonce zobrazení dat uložených v paměti řadiče displeje až za platnými obrazovými daty.

3.2.6.9 P6_C_R_E7 – Porucha registru 60h

Poruchou tohoto registru může dojít k zobrazení vrstvy obraz v obraze, čímž může dojít k nebezpečné změně zobrazení. Záleží na dalším nastavení vrstvy obraz v obraze a datech, která by tato vrstva zobrazovala.

3.2.6.10 P6_C_ME – Porucha paměti

Tato porucha může způsobit, že některý obrazový bod má nesprávnou barvu. Tím může dojít k modifikaci obrazu.

3.2.6.11 P6_C_MA_E1 – Porucha adresního dekoderu

Vlivem této poruchy může dojít k situaci, kdy jsou z paměti čtena některá data z nesprávných adres paměti. Porucha se projeví u obrazových bodů na adresách v paměti řadiče ovlivněných poruchou.

3.2.6.12 P6_D_E1 – Porucha synchronizace řádků

Při poruše synchronizace řádků, může dojít ke zkrácení či ke ztrátě části dat z řádků a tím k modifikaci obrazu.

3.2.6.13 P6_D_E2 – Porucha synchronizace snímků

Touto poruchou může dojít k ořezání snímku či ztrátě části snímkových dat a tím k modifikaci obrazu.

3.2.6.14 P6_D_E3 – Porucha řádkování

Při poruše řádkování může dojít k zpřeházení řádků, nezobrazení řádku či zobrazení více datových řádků na jednom řádku LCD matice.

3.2.6.15 P6_D_E4 – Porucha sloupce

Vlivem poruchy sloupce dojde k výpadku jednoho sloupce v LCD matici.

3.2.6.16 P6_D_R_E1 – Porucha registru R01h

Poruchou tohoto registru může dojít k aktivaci či deaktivaci prokládaného režimu, nebo k zrcadlovému či vertikálnímu překlopení obrazu.

3.2.6.17 P6_D_R_E2 – Porucha registru R0Fh

Tato porucha může způsobit, že se obraz začne vykreslovat od jiného než prvního řádku LCD matice. Po dosažení posledního řádku obraz plynule pokračuje na prvním řádku.

3.2.6.18 P6_D_R_E3 – Porucha registrů R16h a R17h

Porucha těchto registrů může způsobit oříznutí obrazu.

3.2.6.19 P6_LCD_E1 – Porucha řádku

Touto poruchou může dojít k výpadku jednoho řádku displeje, nebo také k situaci kdy jsou postupně na tomto řádku, během jednoho snímku, zobrazeny všechny řádky.

3.2.6.20 P6_LCD_E2 – Porucha sloupce

Zde může dojít k chybnému konstantnímu zobrazení v jednom sloupci (přesněji v jedné jeho barevné složce).

3.2.6.21 P6_LCD_E3 – Porucha buňky LCD matice

Porucha buňky LCD matice se projeví jako konstatntní chybná jasová hodnota jednoho subpixelu (jedné barevné složky jednoho obrazového bodu).

4 Koncepce bezpečnosti zadaného systému

V rámci návrhu koncepce bezpečnosti zadaného systému je navržena množina opatření působících proti identifikovaným poruchovým módům dříve popsaných nebezpečných poruch. Protože jedním z cílů této práce je poskytnout dostatečně širokou paletu realizovatelných opatření pro posílení technické bezpečnosti zadaného systému, aby mohla být v případě realizace systému vybrána podmnožina z těchto opatření vhodná pro dané použití systému a přitom zajišťující požadovanou úroveň technické bezpečnosti, nelze zde uvedenou množinu považovat za úplný výčet všech možných opatření, ani za výčet, která všechna opatření musí být použita, aby byla požadovaná úroveň bezpečnosti zajištěna.

4.1 Základní principy

Tak jako jsou v normách definovány tři základní přístupy k zajištění technické bezpečnosti vůči náhodným poruchám, i zde se opatření dají rozdělit do tří skupin, které jsou analogické k normou popsaným přístupům. Z pohledu normy ale většina opatření spadá pod princip reaktivní bezpečnosti, kde navíc správnou funkčnost kontroluje uživatel. Navíc nelze vždy zcela jednoznačně přiřadit navržené opatření k jednomu principu.

Vzhledem ke skutečnosti, že u většiny navržených opatření je pro zjištění poruchy nezbytná účast obsluhy zařízení, musí být správná reakce této obsluhy na rozpoznanou poruchu stanovena administrativními opatřeními nadřazeného systému využívajícího zadaný zobrazovací systém.

Následují stručné popisy těchto tří základních přístupů k návrhu opatření podporujících technickou bezpečnost systému. Záměrně pro pojmenování nejsou použity normou zavedené termíny, aby nevznikal mylný dojem, že jde o principy zavedené normou. Analogie s normou je však zřejmá. V textu je použit termín chybná nikoliv nebezpečná informace, ve smyslu zobrazení jiné než požadované informace vlivem jiné než nebezpečné poruchy, u které obsluha ve všech provozních režimech rozpozná, že jde o chybnou informaci. Dále také termín chybné potenciálně nebezpečné informace, která vznikne jako následek nebezpečné poruchy a obsluha ji mylně může považovat za správnou.

4.1.1 Vyhýbání se nebezpečným projevům poruch

Zde je hlavní snahou pomocí vhodných nastavení a použitím vhodných dat zajistit, aby projev opatřením ovlivňovaného poruchového módu nevedl k nebezpečné poruše, ale k co nejlépe uživatelem rozpoznatelné poruše. Tento princip lze rozdělit na dva podprincipy.

První je statický a opatření podle něj navržená se snaží zajistit situaci, aby projev poruchového módu vedl ke statickému zobrazení chybné ale nikoliv nebezpečné informace (tedy projev nevedl k nebezpečné poruše).

Druhý podprincip je dynamický, při kterém sice může být zobrazena chybná potenciálně nebezpečná informace, ale toto zobrazení není statické, zobrazovaná informace se v krátkých intervalech střídá s jinou, dostatečně odlišnou informací tak, aby na základě tohoto střídání rozeznal uživatel vznik poruchy. Zde je nutné zajistit, aby vlivem další poruchy se společnou příčinou nedošlo k trvalému zobrazení nebezpečné informace.

Velkou výhodou tohoto pincipu je, že opatření, která jej využívají, jsou poměrně snadno realizovatelná a pokrývají nebezpečné poruchy ve velké části systému.

4.1.2 Kontrola správné funkčnosti

Tento princip staví na průběžném ověřování, že se v systému nevyskytla nebezpečná porucha. I tento princip lze rozdělit na dva podprincipy.

První z nich pracuje samočinně, je tedy ke kontrole bezporuchové činnosti systému využit technický prostředek. Tento podprincip je z bezpečnostního hlediska nejlepší, protože umožňuje automatickou reakci systému na výskyt poruchy bez přispění uživatele. Bohužel pomocí opatření navržených na základě tohoto principu není možné kontrolovat celý systém.

Druhý podprincip staví na kontrole bezporuchového stavu uživatelem, takto lze kontrolovat prakticky celý systém. Na druhou stranu je zde asi největší riziko omylu obsluhy.

Opatření navržená podle tohoto principu jsou obecně nejvíce pokrývající jak celý systém, tak nebezpečné poruchy, jsou však obtížněji realizovatelná a vyžadují poměrně velkou pozornost obsluhy.

4.1.3 Současné využití různých projevů poruchy

Zde je snahou využít skutečnosti, že některé poruchy mají různé projevy například podle umístění dat v paměti. Toho je možné využít a zorganizovat paměť tak, aby se tyto různé projevy setkaly ve výsledném zobrazení, což umožňuje uživateli rozpoznat poruchu. Při poruše jsou totiž jedním způsobem ovlivněny vybrané části zobrazení a ostaní části jsou ovlivněny druhým způsobem. Zobrazená informace je tak zřetelně chybná.

4.2 Základní požadavky pro výběr opatření k realizaci

Základními požadavky pro výběr vhodných opatření pro podporu technické bezpečnosti jsou jednak co nejširší pokrytí systému a nebezpečných poruch vybranými opatřeními, ale také dostatečně snadná realizovatelnost těchto opatření. Některá opatření totiž mohou být, přes svůj velký přínos k technické bezpečnosti, velmi náročná na výpočetní výkon, či na přenosy dat. Je tedy vždy nutné zvážit, zda je navržené opatření realizovatelné při přiměřených nákladech, či zda je možné příliš náročná opatření nahradit jinými, méně náročnými. U některých opatření je třeba zvážit, zda jejich přínos k technické bezpečnosti není příliš malý na to, aby měla jejich realizace ekonomický smysl.

Dále je také nutno přihlédnout k uživatelskému hledisku. Zde je nutné zohlednit konkrétní užití zadaného systému, protože například výpravčí či dispečer věnují zobrazení jinou pozornost než strojvedoucí jedoucího vozidla. Některá opatření proto mohou být méně vhodná pro určitá užití systému, protože u nich hrozí, že obsluha omylem včas nerozpozná vzniklou nebezpečnou poruchu. Toto zohlednění je důležité, protože jednou z hlavních funkcí zabezpečovacího zařízení je snižovat rizika plynoucí z lidských omylů.

4.3 Tabulka pokrytí nebezpečných poruch

V této tabulce jsou k jednotlivým poruchovým módům přiřazena opatření, která na tyto módy působí. Lze tak snáze vybrat soubor opatření pokrývající co možná nejvíce nebezpečné poruchy.

U jednotlivých opatření jsou uvedena také opatření, která nejsou realizovatelná společně s daným opatřením (například pro nutnost použít pro tato opatření různé zobrazovací režimy).

[7] Ovladač displeje musí v pravidelném intervalu generovat signál pro LCD matici, jinak dojde ke ztrátě obrazu na matici. Protože ovladač displeje obsahuje pouze paměť na jeden obrazový řádek, nemůže vlivem poruchy generovat zastaralý obrazový výstup.

[8] Porucha je řešena v rámci výpočetního jádra architekturou 2oo2.

[9] Porucha je řešena v rámci výpočetního jádra architekturou 2oo2.

[10] Tato porucha se projeví na omezeném počtu sloupců v matici, nebo na pruhu displeje, proto není realizace opatření ve všech aplikacích nezbytná.

[11] Tato porucha se projeví na omezeném počtu řádků v matici, nebo na celé ploše displeje, proto není realizace opatření ve všech aplikacích nezbytná.

[12] Tato porucha se projeví na omezeném počtu bodů v matici, nebo na celé ploše displeje ve všech barevných kanálech, proto není realizace opatření ve všech aplikacích nezbytná.

Tabulka 4.1: Pokrytí poruchových modů opatřeními

[13] Tato porucha se projeví na omezeném počtu řádků v matici, nebo na celé ploše displeje, proto není realizace opatření ve všech aplikacích nezbytná.

[14] Tato porucha se projeví na omezeném počtu sloupců v matici, nebo na pruhu displeje, proto není realizace opatření ve všech aplikacích nezbytná.

[15] Tato porucha se projeví na omezeném počtu bodů v matici, nebo na celé ploše displeje ve všech barevných kanálech, proto není realizace opatření ve všech aplikacích nezbytná.

.

Typ opatření Toto opatření se řadí i z pohledu normy k reaktivní bezpečnosti, kdy je činnost zařízení zpětně kontrolována. Vlastní kontrolu zajišťuje bezpečné výpočetní jádro, které je z pohledu normy dostatečně nezávislé.

Provedení Toto opatření rozšiřuje komunikaci mezi bezpečným výpočetním jádrem a řadičem displeje. Pro pouhé zobrazení grafických dat stačí vždy při změně tato data zapsat pomocí SPI sběrnice do paměti řadiče. Opatření tuto komunikaci rozšiřuje o pravidelné zpětné vyčítání obrazových dat z paměti řadiče displeje zpět do bezpečného výpočetního jádra a kontrolu, zda se takto vyčtená data shodují s daty, která byla zapisována. Při bezporuchovém stavu zařízení musejí být zapsaná a zpětně vyčtená data shodná.

Toto zpětné vyčítání paměti řadiče displeje je vhodné rozšířit o vyčtení a kontrolu správnosti obsahu Look-up tabulek a také všech registrů. Dále je také vhodné vyčítat a kontrolovat obsah nepoužité paměti řadiče displeje. Zde je důležité především ověřovat, že tato nepoužitá paměť neobsahuje data, jejichž zobrazení by vedlo k nebezpečné poruše.

účinně detekuje výskyt velkého počtu poruchových módů, může se stát, že vlivem poruchy selže. Mechanizmus selhání tohoto opatření je takový, že bezpečné jádro při vyčítání paměti řadiče nevyčte data aktuálně obsažená v paměti řadiče, ale získá starší data, která následně kontroluje. Pokud by tato starší data byla shodná s daty, která mají být aktuálně v paměti řadiče displeje, mohla by tato porucha zakrýt jinou poruchu, vlivem které by došlo ke změně dat v paměti řadiče displeje. Tuto poruchu lze snadno odhalit tím, že jsou data v paměti řadiče pravidelně záměrně měněna, i když to není třeba pro změnu zobrazení. Tím je zajištěno, že poruchou načtená stará data neprojdou ověřením a porucha je včas detekována.

Typ opatření Také toto opatření se řadí z pohledu normy k reaktivní bezpečnosti, kdy je činnost zařízení zpětně kontrolována. Vlastní kontrolu zajišťuje bezpečné výpočetní jádro, které je z pohledu normy dostatečně nezávislé.

[16] Při stejné datové propustnosti a vyšším nároku na přenos dat se prodlužuje doba, za kterou se datový přenos provede a tak klesá maximální frekvence, se kterou může být datový přenos zopakován.

[17] V některých barevných režimech se do paměti řadiče displeje vejde obrazový buffer několikrát. Na zápis jednoho snímku tedy stačí přenést několikanásobně méně dat, než na zápis obrazového bufferu a přečtení celé paměti řadiče displeje.

Provedení Toto opatření lze realizovat několika způsoby, závislými na použitém barevném režimu. Vždy je možné provádět potřebné změny v nevyužité části paměti řadiče displeje. Na druhou stranu toto opatření nelze použít u registrů. U části paměti, kde jsou aktuálně zobrazovaná grafická data, je žádoucí, aby tyto změny co nejméně ovlivnily výsledné zobrazení.

První možností, jak provést změny v paměti obsahující obrazová data, je použít dvě oblasti s obrazovými daty v paměti řadiče displeje, kdy jsou zobrazována data vždy právě z jedné z nich, a zobrazování přepínat. To umožní provádět změny v druhé, nezobrazené oblasti. Hlavní nevýhodou tohoto řešení je nutnost spravovat dvě oblasti s obrazovými daty a jejich přepínání. V případě, že jsou v paměti řadiče displeje dvoje obrazová data, hrozí dále zobrazení nesprávných dat. Výhodou je možnost použití tohoto postupu ve všech barevných režimech, pokud je dostatečně velká paměť řadiče displeje.

Druhou možností je zanášet pouze malé změny jasu barevných složek, pouze na úrovni nejnižšího bitu, které jsou dostatečně malé, aby je obsluha nepostřehla. Nevýhodou tohoto řešení je jednak možnost, že obsluha se silnějším barvocitem změnu zaznamená, nebo že tato změna způsobí vyšší namáhání očí uživatele. Nevýhodou je dále také skutečnost, že změna je omezena na jeden a vždy stejný (nejnižší) bit barevných složek. Je také nutné analyzovat vliv tohoto opatření na LCD matici, především změnu pozorovacího úhlu. Výhodou je opět možnost použití ve všech barevných režimech, bez omezení velikostí paměti řadiče displeje. Pokud by opatření mělo být realizováno v barevném režimu s Look-up tabulkou, je vhodnější použít třetí možnost.

Třetí možnost je použitelná pouze v režimech s Look-up tabulkou. Zde je možné mít pro každou použitou barvu více různých indexů do této tabulky (v tabulce jsou na více místech shodné hodnoty barevných složek). Je tak možné každou použitou barvu vyjádřit různou hodnotou v obrazových datech a právě střídání těchto hodnot způsobí změnu obrazových dat. Dalším důsledkem použití stejných hodnot barevných složek na více indexech v Look-up tabulce je, že je možné použít v obrazových datech takové indexy, aby část Look-up tabulky nebyla využita. V této části je následně možné provádět libovolné změny potřebné k realizaci popisovaného opatření. Navíc při správném postupu se po každé úmyslně zanesené změně v obrazových datech nepoužívá jiná část tabulky. Je tak možné postupně zkontrolovat funkčnost dohledu celé Look-up tabulky. Datová redundance v Look-up tabulce je méně problematická, než datová redundance obrazových dat,

.

V tom případě zvyšuje přínos tohoto opatření k technické bezpečnosti. Je nutno zvolit vhodnou variantu realizace. Opatření se obejde bez spolupráce s obsluhou zařízení, jedna z variant však může být obsluhou postřehnutelná, což není žádoucí.

4.4.3 O3 – Statický indikátor

Opatření používající statický indikátor již vyžaduje spolupráci obsluhy. Statický indikátor je neměnný obrazec zobrazený trvale na displeji. Obrazec je sestaven tak, aby se některé nebezpečné poruchy, či jejich módy, projevily znatelnou změnou tohoto obrazce či jeho barev. Obsluha má organizačními opatřeními uloženu povinnost sledovat tento obrazec a v případě jeho změny předpokládat výskyt nebezpečné poruchy a splnit další organizační opatření z toho plynoucí (například vyřadit zařízení z činnosti).

Typ opatření Toto opatření spadá do „nenormativní“ kategorie kontrola správné činnosti obsluhou.

Provedení Realizace opatření je poměrně technicky nenáročná, stačí do obrazových dat vložit indikátor. Složitější je návrh takového indikátoru, kdy je vhodné použít například barevnou škálu, ale také piktogram vhodného tvaru. Je tak možné kromě kontroly správného zobrazení barev indikovat například poruchou aktivované nebo naopak deaktivované prokládané řádkování. Indikátor musí být dostatečně velký a výrazný na to, aby byl obsluhou dostatečně vnímán, přitom nesmí omezovat zobrazení provozních informací.

provedení tohoto opatření náročnější. I zde je nutné vybrat správný indikátor, a také je nutné zohlednit, že vlivem animace bude obsluha vnímat méně detailů. Pozornost je třeba věnovat také rychlosti animace a její délce. Obojí je z jedné strany omezováno maximální dobou, kterou se obsluha může indikátorem zabývat, z druhé strany schopností obsluhy rozeznat chyby v animaci a také dosažitelnou snímkovou frekvencí systému.

.

.

Výhody Velmi nenáročné na realizaci.

Nevýhody Opatření může zvýšit nároky na dohled paměti řadiče displeje, je zde také nepříliš velké pokrytí poruchových módů a zvýšení nároků při aplikaci jiných opatření.

Zhodnocení Pro svoji nenáročnost je opatření vhodné realizovat, pokud příliš nezvýší náročnost jiných, důležitějších opatření. V některých případech vhodným výběrem bezpečných hodnot je možné náročnost jiných opatření nezvýšit.

4.4.6.2 O7 – Hummingova vzdálenost

Zde, jako v předchozím opatření, je snahou pomocí vhodného uspořádání dat zařídit aby jedna porucha v přístupu k paměti nevedla k potenciálně nebezpečnému zobrazení. Zde je využita takzvaná Hummingova vzdálenost dvou čísel vyjádřených v binárním tvaru. Tato vzdálenost se rovná počtu bitů, kterými se tato dvě čísla liší. Tedy například čísla $00000000b$ a $00000001b$, nebo i $0111111b$ a $11111111b$ mají Hummingovu vzdálenost 1. Zato třeba čísla $00000000b$ a $1111111b$ nebo $01111111b$ a $1000000b$ mají Hummingovu vzdálenost 8. Je jasné, že čím větší je Hummingova vzdálenost dvou čísel, tím více poruch jednotlivých bitů musí nastat, aby byla tato čísla vlivem těchto poruch zaměněna. Dále je vhodné se zamyslet nad směrem těchto změn, zda z $0 \rightarrow 1$ nebo $1 \rightarrow 0$, protože poruchový děj způsobující tyto změny je různý.

Typ opatření Toto opatření spadá do „nenormativní“ kategorie vyhýbání se nebezpečným projevům poruch.

Provedení Provedení opět není příliš náročné, je jen třeba stanovit minimální Hummingovu vzdálenost, kterou je třeba dodržet mezi indexy do Look-Up tabulky barevných hodnot, jejichž záměna by způsobila nebezpečnou poruchu zobrazovacího systému. Vhodné také je aby tato vzdálenost byla alespoň 2, přičemž je vhodné volit taková umístění, aby pro záměnu byla nutná alespoň jedna změna z $0 \rightarrow 1$ a alespoň jedna změna z $1 \rightarrow 0$.

Výhody Nenáročnost provedení a při kombinaci s předchozím opatřením možnost detekce jedné poruchy uživatelem.

Nevýhody Opatření může zvýšit náročnost některých jiných opatření, dále snižuje možný počet barev pro použití v grafice.

Zhodnocení I toto opatření je pro svou nenáročnost vhodné realizovat i přes poměrně malé pokrytí poruchových módů. Omezení počtu použitelných barev není v technickém

. I přes

vyšší výpočetní náročnost než předchozí opatření je vhodné toto opatření také realizovat. Velkou jeho výhodou je při správném nastavení prostřídání indexů dobrá zřetelnost

poruchy. Omezení možného počtu barev je na polovinu maxima, tedy na 128, což je pro technické zobrazení dostačující. Zvýšení náročnosti některých opatření však může být až na dvojnásobek, protože pro každou barvu jsou třeba dva barevné indexy, tedy každá barva je umístěna (a v obrazových datech použita) v Look-Up tabulce dvakrát.

4.4.6.4 O9 – Dynamické změny LUT tabulky

Zatímco funkce a projevy předchozích opatření jsou statické, toto opatření se realizuje a projevuje dynamicky. Základní myšlenkou je, že porucha přístupu k paměti, nebo porucha paměťové buňky se projeví buď stejně na celé paměti, nebo pouze na některé části paměti. Pokud se porucha projevuje pouze na části paměti, pak pokud budeme data pravidelně po paměti stěhovat, bude se porucha projevovat pokaždé na jiné části dat a obraz tak začne blikat. Tohoto principu lze využít i u Look-Up tabulek, kde lze celou tabulku pravidelně přeuspořádávat.

Typ opatření Toto opatření spadá do „nenormativní“ kategorie kontrola správné činnosti obsluhou.

Provedení Toto opatření je náročnější na výpočetní výkon a hlavně přenos dat, než ostatní opatření týkající se Look-Up tabulek, na druhou stranu ve srovnání s byť jen zápisem obrazových dat příliš náročné není. V rámci tohoto opatření je v pravidelných intervalech měněna Look-Up tabulka tak, že se jednotlivé barvy stěhují na jiná místa v rámci tabulky. Současně s tím jsou adekvátně upravena i obrazová data v paměti řadiče displeje. Četnost těchto změn musí být dostatečně malá, aby byl dostatečně zřetelný projev případné poruchy, a přitom dostatečně vysoká, aby se případná porucha projevovala dostatečně často.

Výhody Hlavní výhodou opatření je, že uživateli usnadní rozpoznání poruchy na kterémkoliv užívaném místě Look-Up tabulky.

Nevýhody Nevýhodou může být obtížnější nalezení optimální četnosti změn, někdy může být u tohoto opatření výhodné použít nižší než maximálně možný počet barev a zmenšit tak používanou oblast Look-Up tabulky. Další nevýhodou je nutnost současné změny obrazových dat se změnou Look-Up tabulky a to tak, aby nedošlo k přechodovému ději. I tak je opatření poměrně snadno realizovatelné.

Zhodnocení Toto opatření je vhodné realizovat pouze pokud je realizovatelná optimální četnost změn. Pokud toto není možné, nebo pokud by bylo opatření příliš výkonově či datově náročné, je vhodné místo něj volit jiná opatření.

4.4.7 Použití vhodných grafických symbolů

I zde se opatření rozpadá na několik jednotlivě realizovatelných opatření. Vzhledem k jejich podobnosti budou jednotlivě pouze popsána, zhodnocení bude provedeno pro všechna opatření najednou.

4.4.7.1 O10 – Použití symbolů složených z dostatečně velkého počtu bodů

Je třeba volit grafické symboly tak, aby výpadek jednoho nebo několika málo bodů, celých řádků či celých sloupců nezpůsobil zmizení symbolu. Pokud je při návrhu symbolů zohledněna potřeba, aby byly symboly dostatečně výrazné pro obsluhu, nebývá problém s jejich velikostí, porucha obrazového bodu, řádku či sloupce však může způsobit také změnu příliš drobné části symbolu. Takto změněný symbol může obsluha obtížně rozpoznávat a proto je důležité, aby i všechny klíčové tvary symbolů byly složeny z dostatečného počtu bodů.

4.4.7.2 O11 – Nepoužití vzájemně inverzních symbolů

Protože už jednou poruchou může dojít k inverzi zobrazení, přestože je tato inverze dobře rozpoznatelná, je vhodné, aby se symboly lišily i tvarem, ne jenom inverzí barevných složek. V případě poruchy tak nedojde k záměně.

4.4.7.3 O12 – Použití dostatečně rozdílných symbolů

Jednotlivé grafické symboly by se měly dostatečně tvarově lišit, aby nemohlo vlivem jednoduché poruchy dojít k záměně. Jednoduchá porucha může způsobit jak změnu jednoho obrazového bodu, tak také změnu celého řádku, či sloupce, rozdíly mezi symboly by i při těchto poruchách měly být dostatečně zřetelné. Z toho důvodu by se grafické symboly neměly lišit pouze v jednom či v několika málo řádcích, sloupci či obrazovém bodu. Protože je při návrhu symbolů třeba zohlednit, kolik pozornosti musí obsluha věnovat jejich rozeznání, bývají většinou navrženy dostatečně rozdílné i při zohlednění možných poruch.

Typ opatření Toto opatření spadá do „nenormativní“ kategorie vyhýbání se nebezpečným projevům poruch.

Provedení Všechna tři opatření jsou nenáročná na technické provedení, je třeba stanovit vhodná pravidla pro návrh grafických prvků a tato pravidla následně při návrhu grafických prvků dodržet.

Výhody Výhodou všech tří opatření je jednak jejich technická nenáročnost a jednak to, že pokrývají jinak těžko pokrytelné poruchové módy vlastního LCD panelu.

Nevýhody Společnou nevýhodou je omezení „jemnosti“ grafiky, což se může projevit například absencí vyhlazování, či drobných detailů.

Zhodnocení Pro svou nenáročnost a zajímavé pokrytí poruchových módů LCD panelu by všechna tato opatření měla být realizována. Jejich společná nevýhoda v systémech technického zobrazení prakticky není omezující, navíc dostatečně rozdílné grafické prvky vyžadují méně pozornosti obsluhy a hrozí menší riziko omylu obsluhy při určování významu symbolů.

4.4.8 Informační redundance

Informační redundanci lze zajistit různými kombinacemi zakódování informace do obrazových dat. Záleží zde na tom, co může být vhodným nositelem bezpečnostně relevantní informace.

Protože i tato opatření jsou si velmi podobná, budou také jednotlivě pouze popsána a následně společně zhodnocena.

4.4.8.1 O13 – Kombinace tvaru a barvy

Kombinace tvaru (textu) a barvy je poměrně vhodná informační redundance, ovšem za předpokladu, že je dostatečně bezpečné barevné zobrazení. Lidé vnímají samotnou barvu o něco rychleji než tvar, a tak se při zběžném pohledu může stát, že uživatel reaguje pouze na barvu, nikoliv na tvar (text). Přestože je možné ošetřit tuto skutečnost předpisově, je vhodné přihlédnout k užití zobrazovacího systému a v případech, kdy je očekávána snížená pozornost obsluhy, volit buď jinou informační redundanci, nebo velmi výrazně rozdílné tvary symbolů.

Typ opatření Toto opatření spadá do „nenormativní“ kategorie kontrola správné funkčnosti obsluhou.

Provedení Všechna tato opatření jsou nenáročná na technické provedení, opatření se aplikují při přípravě grafických prvků. Některé způsoby informační redundance vyžadují stanovení předpisových pravidel pro činnost obsluhy v případě, že dojde k výpadku jednoho ze způsobů zakódování informace a informace tak není k uživateli přenesena celá.

Výhody Výhodou je, že i v případě výpadku jednoho způsobu zakódování informace je uživatel schopen rozpoznat zobrazené informace a tak také rozpoznat potenciálně nebezpečnou poruchu.

Nevýhody Větší složitost a tím také velikost zobrazení je jednou z nevýhod. Další nevýhodou je, že obsluha pro zjištění informace nemusí vnímat celý symbol a tak si nemusí všimnout vzniklé poruchy v redundantním zobrazení.

Zhodnocení Protože jsou tato opatření snadná na realizaci, je vhodné je aplikovat. Protože tato opatření staví na pozornosti obsluhy, která v tomto případě časem ochabuje, je vhodné současně realizovat i další vhodná opatření na eliminaci stejných nebezpečných

[23] Vrstva obraz v obraze (zkráceně PIP) je překryvná vrstva, která umožňuje zobrazení obsahu druhého obrazového bufferu přes část nebo celou hlavní vrstvu. Dále lze nastavit, která barva má být průhledná, či různé efekty zobrazení jako je blikání či „vynořování“ PIP vrstvy. Protože lze těžko ověřovat, zda je tato vrstva skutečně aktuálně zobrazena, není vhodné ji používat v bezpečnostně relevantních aplikacích, a proto zde není blíže popsána.

. Tento efekt naštěstí není trvalý a vyžaduje velmi dlouhý čas stále stejného zobrazení, než se rozvine do pozorovatelné podoby. Pro eliminaci tohoto efektu stačí ve vhodném intervalu zařadit zobrazení plně černého a plně bílého obrazu. Tímto způsobem dojde k vymazání paměťového efektu LCD matice.

Typ opatření Toto opatření spadá do „nenormativní“ kategorie vyhýbání se nebezpečným projevům poruch.

Provedení Provedení je poměrně nenáročné, stačí v daném intervalu na vhodnou dobu několikrát prostřídat zobrazení plně černého a plně bílého obrazu. Nejobtížnější je stanovení intervalu a vhodných dob mazání paměťového efektu. Zde je nejlepší vycházet z doporučení výrobce, nebo z experimentů. U zadaného displeje nebyl ani při několikadenním zobrazení stejného obrazu efekt pozorován, proto lze za vhodný interval považovat nižší jednotky dní. Vzhledem k tomu, že v tomto intervalu není paměťový efekt ještě rozvinut, postačí jako preventivní opatření i jen několikavteřinové doby zobrazení plně bílého nebo plně černého snímku. Je však vhodné v rámci jiných opatření sledovat výskyt paměťového efektu.

Výhody Výhodou tohoto opatření je jeho nenáročnost a poměrně velká účinnost proti paměťovému efektu.

[24] Jas jednotlivých subpixelů se řídí natočením tekutých krystalů. Toto natočení se řídí napětím přivedeným na elektrody, mezi kterými jsou tyto krystaly. Pokud jsou napětím velmi dlouhou dobu drženy v určitém natočení, dojde k částečné polarizaci a takovému uspořádání, že se krystaly obtížněji natáčejí do jiné polohy. Pokud však dojde k natočení do jiné polohy, dojde tím ke změně polarizace a uspořádání, tekuté krystaly se poté již natáčejí standardně.

Provedení Provedení je poměrně nenáročné, lze provést během testů, které zařízení vykonává po spuštění.

Výhody Otestování celého systému, nepříliš velká náročnost realizace.

Nevýhody Hlavní nevýhodou je mnohořádově delší doba mezi okamžiky, kdy může obsluha rozpoznat poruchu v porovnání s jinými opatřeními stejného typu, a také nutnost zařídit, aby tato doba nepřekročila maximální dobu do detekce a negace poruchy systému.

Zhodnocení Přestože opatření pokrývá širokou škálu poruchových módů, vzhledem k dlouhým časům mezi jednotlivými testy je vhodné současně realizovat ještě další opatření. V případě realizace je nutné zajistit maximální dobu provozu systému mezi dvěma testy tak, aby tato doba nepřekročila maximální dobu do detekce a negace poruch, které (či jejich módy) toto opatření pokrývá.

– Statický indikátor

Problematika statického indikátoru je poměrně rozsáhlá, protože dva základní požadavky na něj jsou protichůdné. Základními požadavky jsou maximální rozsah indikace, na druhou stranu jednoduchost a malá velikost. Statický indikátor by pro maximální pokrytí poruchových módů měl zasahovat přes všechny řádky a přes všechny sloupce. To lze splnit, pokud je statickým indikátorem rámeček kolem obrazu, nebo mřížka oddělující jednotlivá pole pro indikaci. Ohledně barev by ideální indikátor měl zobrazovat všechny barvy. Takový indikátor by byl příliš složitý a tak je lepší použít základní barevné složky (pro kontrolu výpadku, chybné aktivaci či záměny barev) a dále bílou a černou barvu (pro kontrolu chybné hodnoty jasu řádku nebo sloupce, ale také výpadku či chybné aktivaci barvy). Z tohoto pohledu se jako vhodný statický indikátor jeví například bílá mřížka na černém pozadí doplněná oblastí se vzorkem červené, zelené a modré barvy. Tento indikátor ale není použitelný ve všech možných aplikacích, neboť například na vozidlech je nežádoucí použití zelené barvy. V takovýchto případech je nutné analyzovat riziko záměny zelené barvy za jinou barvu. Pokud chybné zobrazení jiné barvy místo zelené barvy nezpůsobí nebezpečnou poruchu, je možné zobrazit indikaci pouze červené a modré barvy. Zobrazení barevnvých složek může být v podobě barevných obdélníků, ale také v podobě loga výrobce, loga zařízení a podobně.

Následuje ukázka možného statického indikátoru pro použití v aplikacích, kde může být zobrazena zelená barva a v aplikacích, kde je zobrazení zelené barvy v tomto indikátoru nežádoucí a případné zobrazení jiné barvy místo zelené nezpůsobí nebezpečnou poruchu.

– Vzájemně inverzní indexy v Look-Up tabulce

– Použití dostatečně rozdílných symbolů – odlišnost jedním sloupcem

Další nevhodně málo rozdílné symboly jsou třeba prosté šipky ukazující směr, zobrazena je také vhodnější informační redundance pomocí doplňujícího textu „vlevo“ a

.

Poslední ilustrace zobrazuje položky v menu, kdy je vybraná či aktivní položka označena jiným řezem písma (kurzívou) a grafickým symbolem. Zde jde o kombinaci opatření

– Zkušební obrazce

Zkušební obrazce jsou opět velmi rozsáhlou oblastí, komplexní popis by byl nad rámec této práce. Proto zde budou uvedeny pouze některé možnosti umožňující detekci vybraných poruchových módů.

– Zkušební obrazce – poruchy řádků

Závěr

Práce ve svých prvních dvou kapitolách nejprve popisuje komponenty zadaného zobrazovacího systému, především jejich vlastnosti důležité pro zajištění technické bezpečnosti, následně potenciálně nebezpečné poruchy tohoto systému a stanovuje cíle bezpečnosti kladené na tento systém. V další kapitole práce analyzuje jednotlivé nebezpečné poruchy a popisuje jednotlivé poruchové módy, které dané poruchy způsobují. Ve čtvrté kapitole stanovuje práce koncepci technické bezpečnosti a navrhuje paletu opatření, jejichž realizací lze zvýšit úroveň technické bezpečnosti. V poslední, páté kapitole, práce demonstruje vybraná opatření a jejich vliv na některé poruchové módy.

V rámci práce není popsána reálná aplikace zobrazovacího systému ani stanoveno, která z navržených opatření musejí být pro dosažení dostatečné úrovně technické bezpečnosti realizována. Způsob zajištění technické bezpečnosti pomocí navržených opatření by v případě realizace systému musel být volen podle konkrétních požadavků na zobrazovací systém. Práce plní cíl daný zadáním, analyzovat možné nebezpečné poruchy a stanovit opatření pro eliminaci jejich vlivu, protože nabízí dostatečný výběr z navržených opatření, která společně pokrývají všechny z analýzy vzešlé poruchové módy. Velká část poruchových módů je navíc pokryta více opatřeními, proto není u konkrétní realizace zadaného zobrazovacího systému nutné realizovat všechna navržená opatření.

Na tuto práci by bylo možné dále navázat hledáním dalších opatření v rámci zadaného systému, nebo snahou najít modifikace zadaného systému umožňující návrh dalších opatření. Dále by bylo možné zobecnit problematiku na obecný grafický zobrazovací systém a srovnat možnosti opatření na podporu technické bezpečnosti zobrazovacích systémů různých architektur sestavených z různých komponent.

[9] KYOCERA DISPLAY CORPORATION. *3.5 inch QVGA transmissive color TFT with LED backlight: Datasheet.* Spec No. TQ3C-8EAF0-E1YAD25-00.

[10] HIMAX TECHNOLOGIES INC. *HX8238-A: 960 x 240 TFT LCD Single Chip Digital Driver*. Preliminary version 03 September, 2007. 2007. HX8238-A-DS.

. 90