Механика Транспорт Комуникации

Научно списание

ISSN 1312-3823

том 12, брой 3/2, 2014 г.

статия № 1022

http://www.mtc-aj.com

ОПТИЧНА ПРЕНОСНА СРЕДА В ТЕЛЕКОМУНИКАЦИОННИЯ КАНАЛ НА ЖП ОСИГУРИТЕЛНИТЕСИСТЕМИ И АНАЛИЗ НА СЛЕДОТКАЗОВАТА МУ БЕЗОПАСНОСТ

Венцислав Трифонов, Христо Христов
vgt@tu-sofia.bgcac@tu-sofia.bg

Технически университет – София
БЪЛГАРИЯ

Ключови думи: *критични по безопасност системи,оптични преносни среди, безопасност след отказ, електронни схеми за контрол.*

Резюме: *При обновяване и осъвременяване на съществуващи жп осигурителни системи, ползващи комуникационни канали с електропреносни линии, се използва в замяна оптична преносна среда, която има редица нови качества и несъмнени достойнства. Същевременно възникват и проблеми, най-съществените от които са свързани с безопасността след отказ. В статията се предлага едно такова техническо решение, адресирано към далечно управление и контрол на автоматично прелезно устройство.Показана е и е анализирана безопасна след откази електронна схема за контрол на неизправностите в тракта. Извършен е анализ на безопасността и надеждността на телемеханичния канал.*

1. ПОСТАНОВКА НА ПРОБЛЕМА

В последните години се наблюдава нараснал интерес към подмяна на електропреносни линии в комуникационните канали на съществуващи жп осигурителни системи с оптична преносна среда. Използва се комплекс от технически и програмни средства на съвременната микропроцесорна техника, чрез които се изпълняват функциите на въвеждане, пренос, обработкаи визуализация на информацията. Достойнствата на това модерно решение са несъмнени. Оптичният кабел има несравнимо по-широка честотна лента, по-ниска цена, значително по-малъки габарити и е по-лек от електрическия. По оптичен кабел информацията е много по-добре защитена от всички видове смущения.

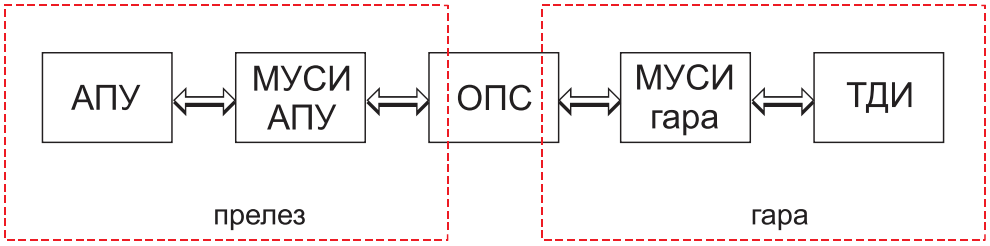
Същевременно възникват и проблеми, специфични за този клас технически устройства. Най-съществените от тях са свързани с безопасността след отказ. Тя трябва да се гарантира от системата като цяло и всички компоненти, в т.ч. от оптоелектронните и електрооптичните преобразуватели и микропроцесорни контролери.

Тук се предлага едно техническо решение за телемеханичен канал в замяна на електропроводната линия за контрол и далечно управление на автоматичното прелезно устройство (АПУ). С подмяната на съществуващия електропроводен канал с оптичен безопасността и надеждността по условие трябва да останат поне същите, както в старите системи. Допустимостта на новото техническо решение трябва да се докаже с научни средства. Това е и целта на настоящото изследване.

2. ПРЕДЛАГАНО ТЕХНИЧЕСКО РЕШЕНИЕ

Разгледано е техническо решение за далечно управление и контрол на АПУ, макар че каналът може да се прилага и за други високоотговорни трактове, ако обемът на пренасяната информация е от същия порядък. Телемеханичният канал с оптична преносна среда (ОПС) пренасяв гарата информация за състоянието наотдалечно АПУ, а в обратна посока - високоотговорна команда за далечно отваряне на прелеза.

Блоковата схема на телемеханичния канал с оптична съединителна линия е показана на Фиг. 1.



Фиг. 1 Блокова схема на телемеханичен канал за връзка между гара и АПУ

Както се вижда връзката между гарата и прелеза е дуплексна. ОПС служи за двупосочно пренасяне на информацията между микропроцесорно устройство за съгласуване на информацията(МУСИ-гара)и МУСИ АПУ, както и за преобразуването на интерфейса от електрически в оптичен и обратно.

ОПС се състои от две световодни кабелни жила – всяко за съответната посока на пренасяне, които завършват в двата си края на оптоелектронни/електрооптични конвертори. Комплектът гарова апаратура получава от ОПС цифровата информация за състоянието на АПУ, преобразува я в светлинен и звуков вид и я извежда на табло за далечна информация (ТДИ). Информацията се експлицира чрез светодиодна индикация и чрез графичен терминал.

За обработката на информацията се прилагат доказано работещи в промишлени системи съвременни микроконтролери. В пилотното решение са използвани Microchip Technology – PIC18F97J60 в АПУ и PIC32MX795F512L в ТДИ.Операционната система за работа в реално време е FreeRTOS.

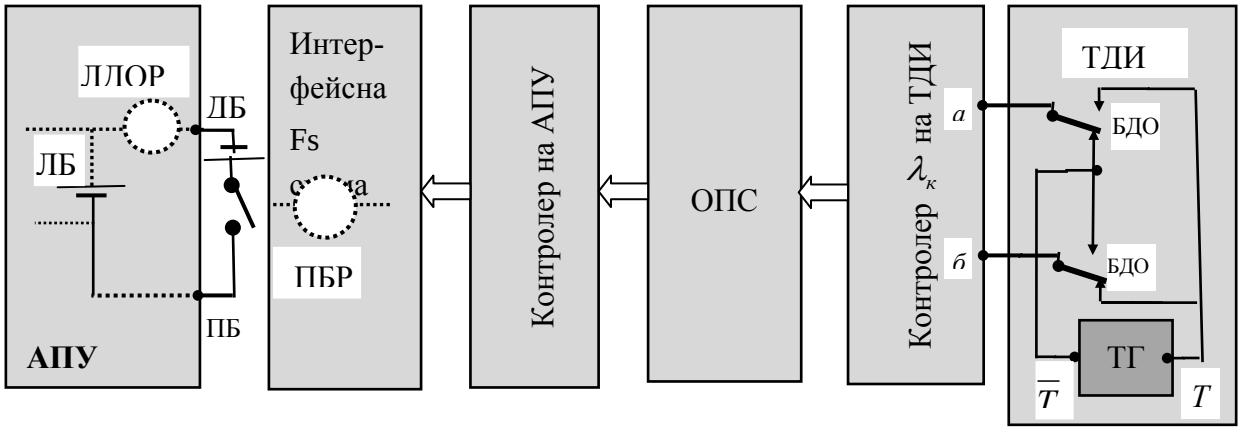
Трактът ТДИ – АПУ работи само когато има аварийно отваряне на прелеза. За да се повиши готовността на цялата система той се проверява на изправност и когато не работи. Между RTOS в контролера на ТДИ и RTOS на АПУ непрекъснато се обменя информация на база на протокол RFC 792 (Internet ControlMessageProtocol). Всяка секунда се изпращат по 4 пакета, както от единия, така и от другия контролер. При липса на отговор или липса на повикване, двете устройства преминават в защитен режим и се сигнализира прекъсване на линията.

В ТДИ непрекъснато работи тактов генератор ТГ, който формира тактови импулси T и $\overline{T}$ с честота $f_{mг}$ (фиг. 2). От двата изхода на генератора се извеждат инверсни тактови поредици, които постъпват в канала през контакти на бутона за далечно отваряне БДО. През тиловите контакти на вход *а* на контролера в ТДИ постъпва $\overline{T}$, а на вход *б* – *Т.*

През цялото време, докато бутонът е незадействан, информацията се чете, обработва и пренася по канала ТДИ – АПУ на далечното отваряне. Полученият в контролера на АПУ сигнал за изправност на канала се прочита и се остойностява. По обратния тракт АПУ - ТДИ се връща диагностична информация за готовността на далечното отваряне. За целта на ТДИ е предвидена допълнителна индикация, която своевременно оповестява за нередности в ОПС.

Когато се задейства бутон БДО, тактовите поредици си разменят местата. В

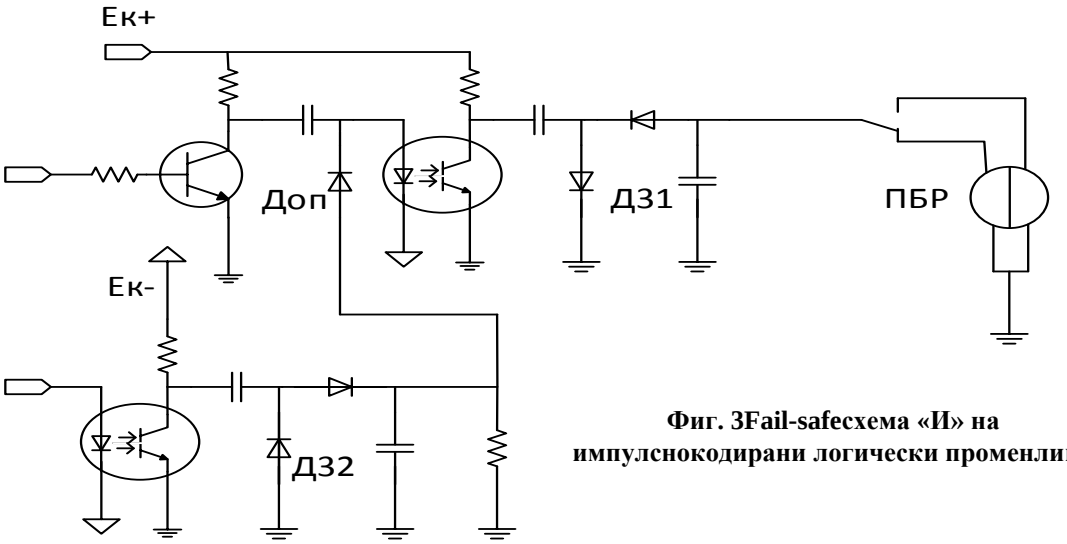
контрорлера на АПУ (фиг. 2) изходите на двете четения (task1 и task2), изпълнени по една и съща програма FreeRTOS, извеждат 16 битови вектори в МУСИ АПУ, които носят информация за състоянието на бутона БДО. Ако и двата контакта са правилно включени, правилно прочетени и информацията е приета правилно, на изходите на МУСИ АПУ се получават тактови поредици. Единият от тези сигнали се формира от първата задача - task1, а вторият от task 2. Хардуерно информацията на двата task-а минава по различно време през стековете и паметта на съответния контролер.



Фиг. 2 Структура на телемеханичния канал

Ключов компонент на тази система, отговорен за безопасността след отказ, е интерфейсната fail-safe на фиг. 3. Тя работи по следния начин:

Тактът на първата задача task1 се превръща в пиков импулсен сигнал през диода на оптрона, който, тактувайки, захранва кондензаторния дешифратор с управляваното далечното отваряне реле ПБР. Но за да стане това възможно, е необходимо опорния му диод $Д_{оп}$ да получи захранване от втория канал на схемата, който контролира редовната работа на task 2. Чрез тази схема на практика се извършва сравнение на резултатите от двете обработки по task1 и task2 като се решава логическата задача fail-safe«И».



Фиг. 3Fail-safeсхема «И» на импулснокодирани логически променливи

3. ДОКАЗАТЕЛСТВО ЗА БЕЗОПАСНОСТ

По принцип безопасността след откази може да се докаже *количествено* (Quantitative) и *логически*(Quality).

1. Анализират се възможните неизправности в изследвания обект като се отчита недопустимостта по условие на някои повреди [1]. При анализа се установява, че има неизправности и съчетания от тях, при които може да се създаде опасен отказ. Намира се вероятността за такива съчетания. След това се отчита интензивността на експлоатационната дейност, т.е на събитията (брой маршрути в гаровите централизации, цикли на автоматична блокировка, преминаване през прелези), при които тази потенциално опасна ситуация може да се превърне в реалност. По така получения комплексен модел се изчислява вероятността Q_d това да се случи. След това тя се съпоставя с нормите за допустимост. Когато е по-малка от допустимата граница $Q_d \le Q_{d.доп}$, където нормите се задават от стандарта [3], безопасността на изследваното устройство се счита за доказана. Говори се за количествено (Quantitative) доказателство.

2. При условие, че не се отчитат недопустимите откази, и се установи, че опасни откази или съчетания от тях липсват и опасна ситуация не се създава $Q_d = 0$ - се говори за логическо (качествено, Quality) доказателство, което е най-доброто възможно.

Една голяма част от осигурителните устройства и системи от старо и ново поколение се подчиняват на философията за *първия открит отказ*. Тя се основава на разбирането, че ако всяка повреда или грешка веднага след активирането (откриването) си бъде забелязана и устройството гарантирано премине в безопасно състояние, то няма как да се състои опасен отказ. В такива случаи не се разглеждат съчетания (натрупвания) на причини за откази. Преходът в защитно състояние принуждава да се премине към ремонт и възстановяване, през което време устройството безопасно не работи. Натрупване и на други повредине вероятно, тъй като преходът в защитно състояние е практически незабавен.

4. ИЗСЛЕДВАНЕ НА СЛЕДОТКАЗОВАТА БЕЗОПАСНОСТ НА ПРЕДЛАГАНОТО ТЕХНИЧЕСКО РЕШЕНИЕ

Отказите могат да има две групи причини: грешки на сфотуераи повреди на хардуера.

4.1 Софтуер

Грешките на софтуера трябва да бъдат открити още при тестването и пускането на системата – иначе тя няма да заработи. Изхожда се от благоприятното обстоятелство, че се пренася само един бит високоотговорна информация - команда за далечно отваряне. Всяка грешка ще доведе до изходен вектор (в случая еднобитова 1), различен от работния, от който не може да произтече високоотговорно действие.

За разлика от апаратните средства, софтуерът е идеален и «не се чупи». Ако е изправен и перфектен, това е завинаги. Ето защо се приема, че приложният софтуер не създава проблеми за безопасността. Системният софтуер FreeRTOSпък е доказано безгрешен в много промишлени приложения в много страни на света.

4.2 Хардуер

Както бе отбелязано в т.3 трябва да се анализират възможните неизправности в изследвания обект като се отчита недопустимостта на някои откази: къси съединения в опроводяването на монтажа, между кабелни жила на съединителни кабели в помещение, пробиви «светоизточник – фотоприемник» на оптрон, късо съединение между тоководещите следи на печатните платки и др.

Методът и съставеният по него алгоритъм на изследване, избран за случая, е *Дърво на откриващите набори от повреди* ДОНП [2]. Задават се последователно всички допустими повреди и се търси реакцията на схемата. Ако след първата повреда няма функционален отказ, тя остава скрита. Към нея се наслагва следващанеизправност. Отново се търси има ли следотказово различно поведение от функционалното. Ако няма, търсенето продължава, докато отказът се изяви. След това за първа се приема друга повреда и търсенето продължава и т.н.

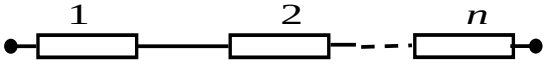
В разглеждания случай не се налага трудоемко и сложно изследване, тъй като проблемът за следотказовата безопасност в системата се решавачрез непрекъсната циклична работа на телемеханичния канал в безконечен цикъл от порядъка на части от секунда. Независимо от работния информационен статус всички елементи на канала (фиг.2) участват в този цикъл и евентуалната повреда, която има устойчив характер («заспиване» в логическа 0 или логическа 1), се открива незабавно. Каналът се привежда в неработно защитно състояние, което се индицира чрез подсистемата за диагностика и забранява високоотговорни команди. Използва се подходът «до първи открит отказ» - всяка повреда се забелязва незабавно и привежда в защитно състояние. За да се реши задачата по този начин обаче е необходима fail-safeинтерфейсна схема (фиг.3).

Допустимите повреди в интерфейсна схема са къси съединения, прекъсвания и електрически смущения. Всички прекъсвания водят до защитен отказ, тъй като сигнал към релето ПБР, изпълзяващо високоотговорното действие, не може да се изведе. Същото се отнася и до пробивите на диодите и прехода «емитер-колектор» на оптроните. Импулсният такт стига до мястото на повредата и по-нататък не може да се пренесе. Пробивите на диоди $Д_{оп}$, $Д_{з1}$ и $Д_{з2}$ водят до нарушаване на нормалната работа и защитен отказ, тъй като преходните кондензатори към колекторите се разреждат по шунтиращи вериги, а не както е предвидено.Неизгладено пулсиращо напрежение към плюс $+E_к$ и минус $-E_к$ на интерфейсната схема, което може да се появи в токозахранването поради откази на токоизточника, не са опасни. В този случай преходните кондензатори се зареждат или разреждат не директно, а през колекторното съпротивление, съответните импулси са многократно по-слаби, отколкото е необходимо за да работи схемата. Спорадичните импулсни смущения не са опасни, тъй като работата на схемата почива на устойчиви потенциали, получени от заряд на кондензатори, който не може да се случи от спорадичен импулс, а само от поредица импулси.

Резултатите показват, че всяка повреда с появата си предизвиква функционален отказ, който е защитен. При тези резултати не се налага да се търси количествена безопасност. безопасността се доказва качествено по принципа «до първи отказ».

5. ИЗСЛЕДВАНЕ НА НАДЕЖДНОСТ

Тъй като в системата (фиг.2) няма резервиране, надеждността се моделира по форма́та на серийната в надеждностно отношение схема (фиг.4). Всеки отказ на кой да е елемент води до отказ в цялата система.



Фиг. 4

Вероятността за безотказна работа на последователната система е равна на:

(1) $$P(t) = p_1(t)\,p_2(t)\ldots p_n(t) = \prod_{i=1}^{m} p_i(t)\,,$$

При експоненциално разпределение на отработката до отказ интензивността на отказите $\lambda(t) = \lambda = const.$, а вероятността за безотказна работа на системата $P(t) = e^{-(\lambda_1\lambda_2...\lambda_n)t}$. Коефициентът й на готовност е

(2) $K_{гs} = K_{г1}K_{г2}...K_{гm} = \dfrac{\mu_1\mu_2...\mu_n}{(\mu_n+\lambda_n)(\mu_n+\lambda_n)...(\mu_n+\lambda_n)}$, където

$K_{гi} = \dfrac{T_{ср.i}}{T_{ср.i}+T_{в.i}}$ - готовност на *i*-я компонент, $\lambda_1, \lambda_2, ...\lambda_n$ и $\mu_1, \mu_2, ...\mu_n$ - интензивности на отказите, респ. на възстановяванита на отделните й компоненти. Средното време между отказите й:

(3) $MTBF_s = \dfrac{(\mu_1+\lambda_1)(\mu_2+\lambda_2)...(\mu_n+\lambda_n)}{\mu_1\mu_2...\mu_n(\lambda_1+\lambda_2+...\lambda_n)}$.

Всички компоненти на разглежданата система са MTTF/MTBF > $1.10^6$1/h. [4] Това означава, че може да се работи с приблизителната формула на базата на (3), по която за тракт телесигнализация се получава:

(4) $MTBF_{ts} = \dfrac{1}{(\lambda_{АПУ}+\lambda_M+\lambda_o+\lambda_{TDI}+\lambda_{ИВ})} \approx \dfrac{1}{5.10^{-6}} = 20.10^4 h$,

а за тракт телеуправление:

(5) $MTBF_{tu} = \dfrac{1}{(\lambda_{АПУ}+2\lambda_M+\lambda_o+\lambda_{TDI}+2\lambda_{фк})} = \dfrac{1}{7.10^{-6}} = 14{,}2.10^4 h$

Направени са аналогични изчисления на старото техническо решение, използвано в експлоатация, които показват, че средните времена на сравняваните части от системите в новото техническо решение и за двата тракта са два-три пъти по-големи.

ЗАКЛЮЧЕНИЕ

Претенциите са за научно-приложни резултати както следва:

1. Оригинално техническо решение на преносния канал с оптична среда, използващо известни и доказани промишлени контролери.

2. Нова оригинална оптоелектронна конюнктивна схема за контрол на импулсното действие на системата с оптичен канал, която допуска само защитни откази.

3. Доказателство за необходимата безопасност и надеждност на предложените технически решения.

4.

ЛИТЕРАТУРА:

[1] Христов, Х.А. В.Г. Трифонов. Надеждност и сигурност на комуникациите. Нови знания 2005.

[2] Христов, Х.А. Основи на осигурителната техника Техника 1990.

[3] *EN50126* “Thespecificationanddemonstration of Reliability, Availability, Maintainabilityand Safety - *RAMS*»

[4] http://www.theriac.org/productsandservices/products/downloads/content/EPRD%20Sample.pdfc, http://izt.bgdocs.org/docs/index-254736.html?page=2 .

OPTICAL TRANSMISSION CHANEL FOR RAILWAY SYGNALING SYSTEM AND SAFETY FAILURE ANALYSES

Ventsisalv Trifonov, Hristo Hristov
vgt@tu-sofia.bgcac@tu-sofia.bg

Technical University of Sofia
BULGARIA

Key words: *safety-criticalsystem, optical networks, fail-safe, safety control devices.*

Abstract: *In renovation and modernization of existing railway signaling systems, based on communication channels with transmission lines transported high responsibility information old lines area exchanges with new optical transmission medium, which has a number of new the quality and undoubted merits. While problems arise, the most notable of which are related to safety after a failure. This article provides such a technical decision addressed to a remote management and control of automatic crossing devices. The paper presents analyses and fail-safe electronic circuit to control the faults tract. Ananalys is of the safety and reliability of telecommunication channel is present.*