

DISTRIBUTED SYSTEM FOR MONITORING AND CONTROL IN INTERNET ENVIRONMENT

NIKOLAY KAKANAKOV¹, BORIS RIBOV²

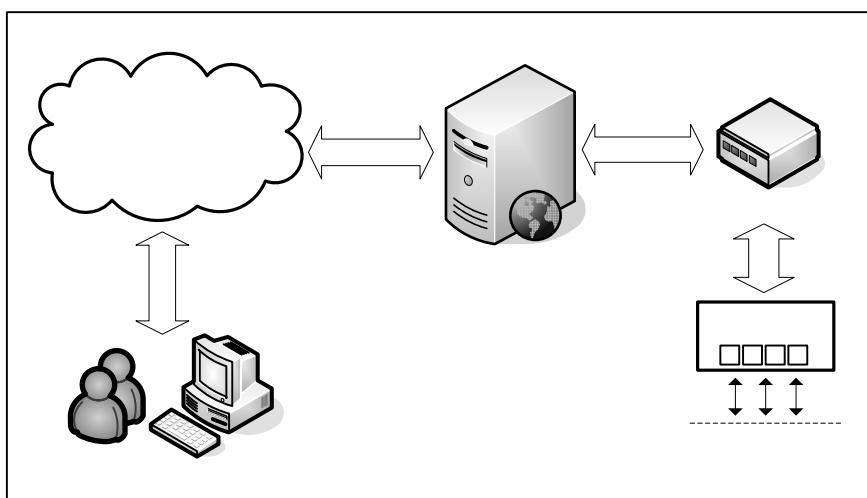
Abstract. The paper proposes a distributed system for monitoring and control in internet environment. The system is based on IPC@CHIP SC12 microcontroller as a “host” and PIC16F877A as a “controller”. IPC@CHIP SC12 has integrated Ethernet interface and TCP/IP stack with Web server. PIC16F877A can monitor sensor or control hardware signals. It supports 1-Wire communication protocol based on I²C through DS2482-100 chip (Dallas). It also has 6 ADC inputs (10bit) for monitoring analog signals, 4 temperature signals (resolution 0.0625°C), 12 discrete inputs and RFID card reader. The system implements three-tier client/server model. The interaction between the “host” and the “controller” is based on serial ASCII protocol.

Key words: Distributed Monitoring and Control, Sensors, Embedded Systems.

РАЗПРЕДЕЛЕНА СИСТЕМА ЗА МОНИТОРИНГ И КОНТРОЛ ПРЕЗ ИНТЕРНЕТ

1. Въведение

Общата архитектура на системата е показана на фигура 1. Тя се базира на многослоен модел клиент-сървър, приложим в системи за разпределена автоматизация [2]. На най-горният слой са потребителите, които се връзват към системата през Интернет, посредством стандартен Web браузер и HTTP.



Фиг. 1. Архитектура на системата.

Контролера следи дали параметрите на всички тези сензори са в нормите зададени предварително в конфигурационна таблица и сигнализира алармено събитие към хост системата при излизане от границите на параметрите. При възвръщане към допустимия интервал от стойности на дадения параметър отново се генерира събитие към хост системата за да се уведоми, че следения процес е в нормите.

Комуникацията между контролера и хост системата се осъществява посредством сериен RS232 интерфейс чрез ASCII команди. За тази цел в контролера работи команден интерпретатор, който обработва потока от символи и взема съответно решение за изпълнение на дадената команда.

Всички параметри на сензорите се записват в регистров файл, който може да бъде достъпен за четене от хост системата. От своя страна хост системата може да задава и запазва началните конфигурационни параметри за следене на всеки един сензор в EEPROM паметта на контролера, както и да включва или изключва даден сензор. Това става с команди за запис от хост системата към контролера.

Исходните данни от сензорите, както и текущото състояние на алармения буфер се намират в регистров файл в RAM паметта на контролера, която може да бъде прочетена от хост системата във всеки един момент от време. Последната може периодично да чете състоянието на сензорите с цел статистическо натрупване на данни от тях. Контролера е длъжен да уведоми хост системата чрез заявка за прочитане на алармения буфер ако даден параметър излезне извън рамките на допустимите стойности (генериране на алармено събитие от сензор). След прочитане на алармения буфер следва процедура на потвърждение, инициатор на която е хост системата. В алармения буфер се съдържа информация за поредния номер на алармата и номера на сензора, който я поражда. Ако такава бъде породена от множество сензори то се отбелязва мулти-алармено събитие. В алармения буфер може да бъде прочетена и стойността на брояч показващ общия брой рестарти на системата. При всяко пускане този брояч се увеличава с единица и неговата стойност се запомня в енерго-независима памет. В системата е предвидена отказоустойчива проверка на контролера в реално време. Проверява се крехкостта на изпълнение на хода на програмата и ако възникне критична ситуация се взимат мерки централния микроконтролер да бъде рестартиран. При наличие на проблем породен от некоректно поведение на контролера последният се рестартира, като брояча на начални стартирания се увеличава с единица. Предвидена е и възможност хост системата да рестартира принудително контролера при загуба на комуникация с него. В този случай брояча на начални стартирания също се увеличава с единица.

В контролера е реализирана специфична операционна система, чрез която се следят всички процеси свързани с обработката на информацията от сензорите. Стартирани са множество процеси, някои от които са: комуникационен процес обслужващ серийния RS-232 интерфейс; опорен таймер; процес на АЦП; процес на следене на дискретните входове; процес на следене на температурните сензори; процес на следене на безжичния четец на карти и др. Специфичната операционна система е реализирана на езика асемблер (MPASM) с цел да се оптимизират процесите по оптимално използване на ограничения ресурс на микроконтролера.

3. Сензори

Типа на сензорите, които се поддържат от контролера е разнообразен с цел универсалност при приложението на системата. Това налага да бъдат използвани и различни интерфейси за връзка.

3.1 Дискретни сензори – нормален режим на работа

Дискретните сензори са галванично разделени и се следят по логически нива. Такъв тип сензори са например: сензор за врата, пожарен сензор, контактен сензор и др.

Предвидена е възможност да бъде задавано активното следящо ниво – дали генериращото аларма събитие да бъде изпълнявано по логическа нула или логическа единица. За всеки един от тези сензори е предвидено хистерезисно време (таймаут) за задействане, което да се изчака преди да се вземе решение за алармено състояние. Това време се задава в секунди (от 1 до 63) и се запазва в конфигурационната таблица на сензорите, като за всеки един вход то се задава независимо. Използуването на хистерезисно време на задействане е продиктувано от спецификата на работа на множество от дискретните сензори с цел отстраняване на фалшиви въздействия породени от случайни шумове.

3.2 Дискретни сензори – специален режим на работа

За всеки един дискретен вход може да бъде зададено да работи по специфичен алгоритъм, нужен за определен тип специални сензори. При тях няма твърдо изменение на сигнала с, което да се предизвика алармено събитие а се наблюдава определен закон от преходи от единица в нула. Такива са например обемните сензори. При тях когато има движещ се обект в активната зона се предизвиква моментално задействане на сензора, и след някакъв интервал от време отново се възобновява нормалното състояние. Към тази група сензори принадлежат и шоките сензори. За да може такива сензори да бъдат включвани към контролера е необходимо дадения дискретен вход към който е свързан такъв сензор да бъде конфигуриран да работи като “специален”. В този режим на работа не се проверява за хистерезисен интервал от време, като веднага се генерира аларма при поява на активно алармено ниво (то може да бъде задавано дали да е с високо или ниско логическо състояние). Ако сензор в този режим се задържи в активно състояние повече от 30 секунди се генерира ново алармено събитие за “липсващ сензор”. Това е индикация, че има окъсяване на сигналната линия или пък отпадане на сензора поради технически или умишлени причини.

3.3 Аналогови входове/сензори и АЦП

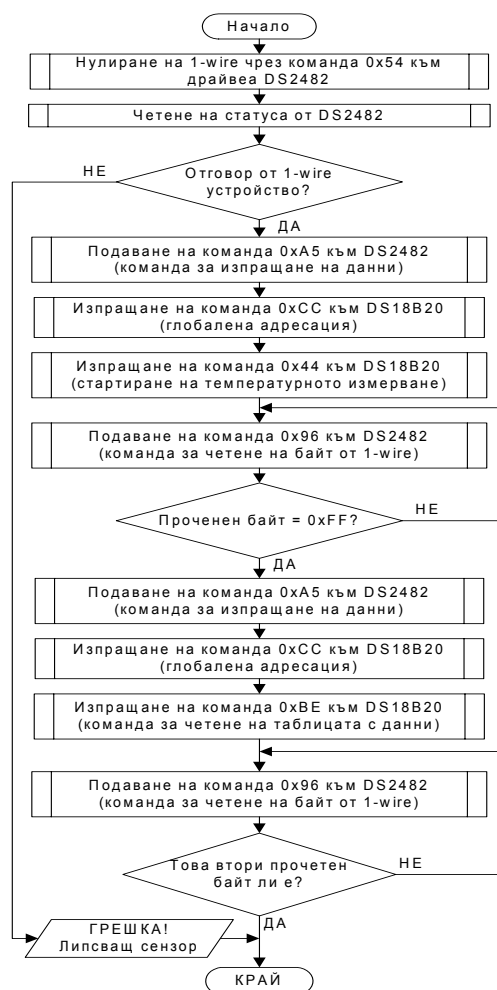
Обхвата на преобразуване е от 0 до +5V, като разделителната способност е 10 бита. Поради необходимостта крачетата на микроконтролера да бъдат използвани за множество други входно/изходни шини се използва само един входен аналогов сигнал и външен аналогов мултиплексор. За аналогов мултиплексор е използван 4051, като се реализира динамично във времето сканиране на всички 8 аналогови сигнали. За измерванията е използван алгоритъм отстраняващ грешката. За целта се измерват 10 поредни отчета на стойността на всеки един от входовете, отстранява се най-малката и най-голямата стойност и се осреднява стойността от останалите 8 измервания. Това гарантира получаването на значителна точност и отстраняване на грешката от случайни шумове. Измерената стойност се сравнява с реперните за минимална и максимална допустими граници и при излизане от тези граници за определен времеви период се генерира алармено събитие. В статуса на аларменото събитие е достъпна информация дали то е породено от спадане на напрежението на дадения аналогов сензор под минималния репер или е породено от превишаване над максималния репер.

Хистерезисния времеви интервал е предвиден за да може бързо изменящи се процеси (шумове) да не генерират случайни сработвания на алармено събитие. Хистерезисния период се задава в конфигурационната таблица в секунди, като той е общ за всички аналогови входове и е в границите от 1 до 255 секунди.

В схемата са предвидени два коригиращи аналогови входа чрез които се отчита реперната нулева стойност от която да започне измерването. Това се налага поради наличието на потенциали породени от токови контури при връзката на външни аналогови сензори. От отчетената стойност за всеки вход се изважда измерената реперна стойност и по този начин се получава действителната, която подлежи на последващо сравнение дали принадлежи на интервала от допустими стойности зададен в

конфигурационния файл. При необходимост може двата входа, измерващи реперните напрежения да бъдат свързани към нулевата шина, с което да се разреши измерването на пълния диапазон от стойности и да се изключи корекцията.

3.4 Температурни сензори и интерфейс за връзка с тях



Контролера позволява измерването на четири независими температури чрез интелигентни цифрови сензори DS18B20 производство на фирмата Dallas/Maxim [5]. Самите сензори са компактни в 3-краков корпус TO92 и измерват температура в диапазона от -55 градуса до $+125$ градуса и разделителна способност от $0,0625$ градуса (12 бита). Интерфейса за връзка на температурните сензори към контролера е 1-Wire [5] и се характеризира с двупосочен трансфер на команди и данни по 2 линии (маса и данни).

За да може да бъде изпълнен комуникационния протокол изискващ се от 1-wire стандарта и да се разтовари централния микроконтролер от допълнителни задачи е използван външен драйвер, който формира времедиаграмите на сигналите по шината. Този драйвер поема комуникацията по 1-wire шината, като към него му се подават команди от контролера посредством I²C интерфейс. Използвания чип за драйвер на 1-Wire е DS2482-100 [5] и позволява реализирането на мрежа от 1-wire сензори свързани в паралел към шината. Всеки един сензор в шината има уникален адрес, чрез който се

адресира при обмен на информация (данни или команди).

3.5 Четец за безжични карти по RFID стандарта

Контролера позволява четенето на идентификационните номера от безжични RFID карти. Това прави системата много атрактивна за реализиране на постоянен контрол и наблюдение в реално време на процеси в необслужваеми обекти и зони, изискващи контрол на достъпа. За безконтактни идентификационни карти са използвани TEMIC-5557, работещи на 125kHz. За четец на транспондерите на RFID картите се използва чипа U2270B, като декодирането и формирането на комуникационния протокол се изпълнява от допълнителен микроконтролер от серията PIC16F84. Изхода на последния е по стандарта RS232 с канална скорост 9600bps-8N1, като се предават прочетените 5 идентификационни байта от безконтактната карта.

В контролера е предвидена функция за мултиплексиране на серийния интерфейс поради необходимостта той да бъде използван за комуникация и с хост системата. Данните от четеца за карти се протичат еднократно при доближаване на нова карта след което комуникацията се предава към хост системата. Контролера позволява да бъде въведено побитово маскиране на прочетените 5 байта (използуване на маска). Това дава възможност идентификацията да бъде реализирана само по определена част от информационните данни съдържащи се в картата.

4. Заключение и бъдещо развитие

Към проекта ще бъде включена възможност за дистанционен контрол на крайни устройства. В контролера се предвижда да има 8 галванично разделени дискретни изхода, които да управляват консуматори от различен тип и с различна мощност; 2 аналогови галванично разделени изхода и интерфейс за комуникация с външен димер, който може да управлява консуматори на ~220V безжично посредством радио-канал на 433MHz. За целта ще бъдат използвани съвременни сигурни техники за достъп до средата [6]. Допълнителна функционалност ще даде модула за контрол на консуматори, управлявани по захранващата ел. мрежа.

Друго важно допълнение към системата ще бъде възможността за автоматично конфигуриране на всеки „хост“ чрез зареждане на конфигурационен файл от сървъра на втория слой [2]. Така във всеки един момент на сървъра ще има картина на: всички „хостове“, връзката между тях, конфигурацията им и включената към съответния им „контролер“ периферия (сензори, четци, управляеми устройства и др.). Това ще позволи самодиагностика на системата и ще гарантира увеличена надеждност.

Като заключение може да се каже, че системата представлява завършена единица способна да поеме управлението, следенето и контрола на различни процеси, както и контрола на достъпа до помещения и зони.

ЛИТЕРАТУРА

1. *Beck's IPC@Chip homepage*, Beck IPC GmbH, <http://www.beck-ipc.com/>
2. **Kakanakov, N., M. Shopov, G. Spasov**, *A New Web-based Multi-tier Model for Distributed Automation*, Journal of "Information technology and Control", b.2/2006.
3. **Kakanakov, N., I. Stankov, M. Shopov, G. Spasov**, *Controller Network Data Extracting Protocol – Design and Implementation*, Proc. of CompSysTech'06, V. Tarnovo, Bulgaria, 2006, pp. IIIA.14-1 IIIA.14-6.
4. *Microchip PIC16F87XA Data Sheet*, Microchip Technology Inc., 1998; <http://www.microchip.com/>
5. Maxim Integrated Products Inc., <http://www.maxim-ic.com/>
6. **Ribov, B.**, *Introducing the newest Philips' microcontrollers into secured telemetry wireless applications*, Proc. of CompSysTech'06, V. Tarnovo, Bulgaria, 2006, pp.I.4-1 I.4-6.

¹ Dept. Computer Systems and Technologies
Technical University of Sofia, Branch Plovdiv
25, Tsanko Dystabanov Str.
4000 Plovdiv
BULGARIA
E-mail: kakanak@tu-plovdiv.bg

² Space Research Institute
Bulgarian Academy of Science
6, Moskovska Str.
1000 Sofia
BULGARIA
E-mail: ribov@developer.bg