1.Introdução à segurança em sistemas embarcados

1.1 Sistemas embarcados

São sistemas computacionais projetados para executar tarefas específicas dentro de um dispositivo ou sistema maior. Eles são caracterizados por serem integrados a um hardware específico e dedicados a executar funções pré-determinadas. Esses sistemas são projetados para serem eficientes em termos de recursos computacionais, energia e espaço físico.

Um sistema embarcado é composto por três elementos principais: hardware, software e firmware. O hardware é a parte física do sistema, incluindo o processador, memória, dispositivos de entrada/saída e sensores.

O software é responsável por controlar e coordenar as operações do sistema embarcado, definindo a lógica e as funcionalidades desejadas. Já o firmware é um software de baixo nível que está gravado em uma memória não volátil e é responsável por fornecer as instruções básicas para o funcionamento do hardware.

1.2 Capacidade de processamento

A capacidade de processamento em sistemas embarcados é geralmente limitada devido a uma série de razões:

- **Restrições de recursos:** Sistemas embarcados são projetados para serem eficientes em termos de recursos computacionais, energia e espaço físico. Isso significa que eles geralmente possuem recursos limitados, como processadores de baixo consumo de energia, memória limitada e espaço de armazenamento restrito. Essas restrições são necessárias para garantir que o sistema possa ser incorporado ao dispositivo ou sistema maior de forma econômica e eficiente.
- **Necessidades específicas de aplicação:** Os sistemas embarcados são desenvolvidos para atender a necessidades específicas de aplicação. Eles são projetados para executar funções pré-determinadas e não possuem a flexibilidade e a capacidade de processamento de sistemas de propósito geral, como computadores pessoais. Isso significa que o hardware e o software são otimizados para realizar tarefas específicas, muitas vezes em tempo real, em vez de oferecer um amplo poder de processamento.
- **Consumo de energia:** Muitos sistemas embarcados são alimentados por baterias ou fontes de energia limitadas. Portanto, a eficiência energética é uma consideração crucial. Processadores de baixa potência são preferidos para minimizar o consumo de energia e prolongar a vida útil da bateria. Isso resulta em uma capacidade de processamento reduzida em comparação com sistemas de propósito geral que têm acesso a uma fonte de alimentação constante.

1.3 Controladores lógicos para sistemas embarcados

Sistemas embarcados normalmente são baseados em firmware executado em um controlador lógico programável (PLC). Esses PLCs são construídos com componentes de hardware e sistema operacional diferentes dos encontrados em alguns PCs de mesa.

1.4 Sistemas em chip (SoC)

Sistemas em Chip (SoC, do inglês System on Chip) são dispositivos eletrônicos que integram diversos componentes e funcionalidades de um sistema completo em um único chip. Esses sistemas são projetados para oferecer alto desempenho, menor consumo de energia e menor custo em comparação com a implementação de cada componente separadamente.

Um SoC é composto por vários blocos funcionais, como um processador central (CPU), memória, controladores de periféricos, interfaces de comunicação, aceleradores gráficos, entre outros. Esses blocos são interconectados por meio de barramentos internos dentro do chip, permitindo a comunicação e o compartilhamento de dados entre os componentes.

A principal vantagem dos SoCs é a integração de várias funcionalidades em um único chip, reduzindo a complexidade do projeto, o tamanho físico do dispositivo e o consumo de energia. A integração em um único chip também permite um melhor desempenho, uma vez que a comunicação entre os componentes é mais rápida e eficiente, evitando gargalos devido à latência da comunicação externa.

Os SoCs são amplamente utilizados em uma variedade de dispositivos, como smartphones, tablets, dispositivos de Internet das Coisas (IoT), sistemas embarcados, consoles de videogame, sistemas de navegação veicular, entre outros.

O Raspberry Pi é um computador de placa única (single-board computer) que possui um SoC em seu coração. O SoC presente no Raspberry Pi combina um processador central (CPU), memória, controladores de periféricos, interfaces de comunicação, aceleradores gráficos e outros blocos funcionais em um único chip.

Essa integração permite que o Raspberry Pi funcione como um computador completo, oferecendo capacidades de processamento, armazenamento e conectividade.

Por outro lado, o Arduino também é um exemplo de SoC, embora sua arquitetura seja mais focada em sistemas embarcados e projetos de eletrônica. O Arduino possui um microcontrolador como seu SoC, que inclui uma CPU, memória, interfaces de entrada/saída e outros recursos essenciais para a execução de tarefas específicas.

Embora o Arduino seja menos poderoso em termos de processamento em comparação com o Raspberry Pi, ele é altamente otimizado para aplicações de controle e automação, além de consumir menos energia.

2.Field Programmable Gate Array (FPGA)

Um Field Programmable Gate Array (FPGA) é um dispositivo eletrônico que consiste em uma matriz de blocos lógicos programáveis (logic blocks) interconectados. Esses blocos lógicos podem ser configurados e reconfigurados para implementar diferentes funções lógicas

e circuitos digitais personalizados. Dessa forma, os FPGAs oferecem uma solução flexível e altamente customizável para a implementação de circuitos digitais.

Os FPGAs são programados usando linguagens de descrição de hardware (HDL, do inglês Hardware Description Language), como VHDL (VHSIC Hardware Description Language) ou Verilog. Essas linguagens permitem descrever a função lógica desejada em um nível abstrato, especificando as interconexões dos blocos lógicos e seus comportamentos.

Ao programar um FPGA, o projeto é sintetizado em uma configuração específica que define a conexão dos blocos lógicos e os elementos de roteamento. Essa configuração é então carregada no FPGA, permitindo que ele execute a função lógica desejada. A flexibilidade dos FPGAs permite a criação de circuitos altamente personalizados e adaptáveis para uma ampla gama de aplicações.

3.Real-Time Operating Systems (RTOS)

Um Real-Time Operating System (RTOS) é um sistema operacional projetado para lidar com tarefas em tempo real, ou seja, tarefas que possuem requisitos de tempo estritos e devem ser concluídas dentro de prazos determinados.

Ao contrário dos sistemas operacionais de propósito geral, os RTOS são altamente determinísticos e fornecem recursos para o agendamento e a execução precisa de tarefas em tempo real.

Os RTOS são projetados para oferecer garantias de tempo de resposta previsíveis e confiáveis. Eles fornecem mecanismos de priorização de tarefas, agendamento de tempo real, compartilhamento de recursos, gerenciamento de eventos e comunicação entre tarefas. Eles podem oferecer serviços de temporização, sincronização, semáforos, filas de mensagens e gerenciamento de memória.

Um exemplo popular de RTOS é o FreeRTOS, que é um sistema operacional de tempo real de código aberto amplamente utilizado em sistemas embarcados e IoT. Outros exemplos incluem o eCos, VxWorks, QNX Neutrino RTOS e Micrium µC/OS-II.

Esses sistemas operacionais são projetados para oferecer baixa latência, escalabilidade e confiabilidade, atendendo aos requisitos de tempo real de uma variedade de aplicações, como automóveis, dispositivos médicos, robótica, sistemas de controle industrial e aeroespacial.

4.Tecnologías de sistemas embarcados - Protocolos Z-wave e Zigbee

Os protocolos Z-Wave e Zigbee são dois protocolos de comunicação sem fio amplamente utilizados em aplicações de automação residencial e Internet das Coisas (IoT). Embora tenham objetivos semelhantes de conectar dispositivos e permitir comunicação entre eles, existem diferenças em sua arquitetura e implementação.

O protocolo Z-Wave é um protocolo de rede de baixa potência (LPWAN) projetado para comunicação de curto alcance em redes domésticas inteligentes. Ele opera na faixa de frequência de rádio de 800-900 MHz e utiliza a tecnologia de malha de rede (mesh network) para permitir que os dispositivos se comuniquem entre si.

Isso significa que os dispositivos Z-Wave podem atuar como repetidores, estendendo o alcance da rede. O Z-Wave é conhecido por sua confiabilidade, segurança e interoperabilidade entre diferentes dispositivos de diferentes fabricantes.

O protocolo Zigbee também é um protocolo de rede de baixa potência (LPWAN), mas opera na faixa de frequência de 2,4 GHz. Ele também utiliza a tecnologia de malha de rede, permitindo que os dispositivos se comuniquem diretamente entre si ou através de dispositivos intermediários.

O Zigbee é altamente eficiente em termos de consumo de energia e suporta redes maiores, com milhares de dispositivos interconectados. Ele também oferece recursos avançados de segurança e possui perfis padronizados para garantir a interoperabilidade entre diferentes dispositivos.

Tanto o Z-Wave quanto o Zigbee são projetados para fornecer comunicação sem fio confiável e segura para sistemas de automação residencial e IoT. Eles permitem o controle e a interação de dispositivos como lâmpadas, sensores, termostatos e fechaduras inteligentes.

A escolha entre os protocolos Z-Wave e Zigbee geralmente depende das preferências do fabricante, da disponibilidade de dispositivos compatíveis e dos requisitos específicos de cada aplicação.

5.Controller Area Network (CAN)

Controller Area Network (CAN) é um protocolo de comunicação serial usado em sistemas embarcados para permitir a comunicação confiável e robusta entre dispositivos. Foi originalmente desenvolvido para uso em aplicações automotivas, mas agora é amplamente utilizado em diversos setores, como automação industrial e equipamentos médicos.

O CAN funciona por meio de um barramento de comunicação compartilhado, onde vários dispositivos podem transmitir e receber mensagens. Cada dispositivo conectado ao barramento possui um identificador único, que permite a diferenciação das mensagens transmitidas.

O protocolo CAN utiliza uma abordagem de comunicação de multi-acesso, ou seja, vários dispositivos podem transmitir dados simultaneamente no barramento, usando um mecanismo de detecção de colisão para resolver possíveis conflitos.

O funcionamento do CAN envolve a troca de mensagens entre os dispositivos conectados. Um dispositivo pode enviar uma mensagem no barramento, que é recebida por todos os outros dispositivos conectados.

No entanto, apenas os dispositivos com o identificador correspondente à mensagem irão processá-la, enquanto os outros dispositivos a ignoram. As mensagens do CAN são organizadas em pacotes de dados chamados frames. Cada frame contém um identificador, que indica o tipo e a prioridade da mensagem, e os dados associados à mensagem. Os dispositivos conectados podem transmitir mensagens de forma assíncrona ou síncrona, permitindo a troca de informações em tempo real.

O CAN é conhecido por sua confiabilidade, imunidade a interferências e escalabilidade. Ele suporta velocidades de transmissão variáveis, desde taxas de transmissão baixas até velocidades de vários megabits por segundo.

Além disso, o protocolo CAN pode ser estendido com funcionalidades adicionais, como o CAN FD (Flexible Data-Rate), que permite taxas de transmissão ainda mais altas.

6.Sistemas de Controle Industrial (ICS)

Os Sistemas de controle industrial, também conhecidos como Industrial Control Systems (ICSs), são sistemas computacionais projetados para monitorar e controlar processos e operações em ambientes industriais.

Eles desempenham um papel fundamental em setores como manufatura, energia, petróleo e gás, automação predial e muitos outros, onde é necessário controle e automação de sistemas complexos.

Os ICSs são compostos por três componentes principais: dispositivos de campo, controladores e sistemas de supervisão. Os dispositivos de campo, como sensores e atuadores, coletam dados do ambiente físico e interagem com os processos industriais. Os controladores, como Controladores Lógicos Programáveis (PLCs) ou Sistemas em Chip (SoCs), executam algoritmos e lógica de controle para operar os dispositivos de campo com base nas instruções recebidas.

Os sistemas de supervisão, como os sistemas SCADA (Supervisory Control and Data Acquisition), fornecem interfaces de monitoramento e controle para os operadores humanos.

7.Supervisory Control and Data Acquisition (SCADA)

Os Supervisory Control and Data Acquisition (SCADA) são sistemas de controle e aquisição de dados que permitem monitorar e controlar processos industriais e infraestruturas críticas. O SCADA é amplamente utilizado em setores como energia, água, transporte, manufatura e muitos outros, onde é necessário supervisão e controle centralizado.

Os sistemas SCADA consistem em três principais componentes: unidades de aquisição de dados, unidade de supervisão e estação de controle. As unidades de aquisição de dados são responsáveis por coletar informações de sensores e dispositivos de campo, como temperatura, pressão, fluxo, entre outros.

Esses dados são transmitidos para a unidade de supervisão, que processa e exibe as informações em tempo real. A estação de controle é onde os operadores humanos podem interagir com o sistema, monitorar os processos, ajustar parâmetros e enviar comandos para dispositivos de campo.

A comunicação entre os componentes do SCADA ocorre geralmente por meio de uma rede de comunicação, como redes Ethernet ou redes sem fio. Os dados coletados dos dispositivos de campo são enviados para a unidade de supervisão, que realiza o processamento e a análise dos dados.

Os dados podem ser apresentados aos operadores em interfaces gráficas, como telas de computador ou painéis de controle.

O SCADA permite o controle remoto de dispositivos e processos. Os operadores podem enviar comandos para dispositivos de campo por meio do sistema SCADA, permitindo ajustes e intervenções em tempo real.

Isso proporciona maior eficiência operacional e facilita a tomada de decisões. Os sistemas SCADA também incorporam recursos de segurança, pois são críticos para a operação segura de infraestruturas e processos industriais. São implementadas medidas de segurança, como autenticação de usuários, criptografia de dados e proteção contra ameaças cibernéticas, para garantir a integridade e a confiabilidade dos sistemas SCADA.

8.Internet das Coisas (IoT)

A Internet das Coisas (IoT) é um conceito que se refere à interconexão de dispositivos físicos, como eletrodomésticos, veículos, sensores e outros objetos, por meio da internet. Esses dispositivos são equipados com sensores, atuadores e conectividade de rede, permitindo que eles coletem, troquem e processem dados de forma autônoma ou interativa.

O funcionamento da IoT envolve várias etapas. Primeiro, os dispositivos IoT são equipados com sensores que coletam dados do ambiente ou do usuário. Esses sensores podem medir parâmetros como temperatura, umidade, movimento, localização, entre outros.

Os dados coletados pelos dispositivos são então processados internamente ou enviados para a nuvem, onde podem ser armazenados e processados em servidores remotos. O processamento pode incluir análise de dados, aplicação de algoritmos de aprendizado de máquina e extração de insights úteis.

A comunicação é um aspecto fundamental na IoT. Os dispositivos IoT podem se comunicar entre si por meio de redes locais sem fio, como Wi-Fi, Bluetooth ou Zigbee. Eles também podem se conectar à internet por meio de tecnologias de comunicação, como 4G, 5G ou protocolos específicos para IoT, como o LoRaWAN e o NB-IoT.

Uma vez conectados, os dispositivos IoT podem trocar dados e comandos com outros dispositivos ou com sistemas centrais. Isso permite a automação de processos, a coleta contínua de dados e a tomada de decisões em tempo real com base nas informações coletadas.

A IoT oferece uma ampla gama de aplicações em diversos setores, como saúde, agricultura, indústria, transporte e cidades inteligentes. Exemplos incluem monitoramento remoto de pacientes, agricultura de precisão, automação industrial, veículos conectados, iluminação inteligente, entre muitos outros.

9.Sistema de Automação Predial (BAS)

Também conhecido como Building Automation System (BAS), é um sistema computacional que controla e gerencia diversos sistemas e dispositivos dentro de um edifício, visando melhorar a eficiência operacional, a segurança e o conforto dos ocupantes.

O BAS integra sistemas como iluminação, HVAC (Heating, Ventilation and Air Conditioning - aquecimento, ventilação e ar-condicionado), controle de acesso, segurança, monitoramento de energia, entre outros.

O funcionamento de um BAS envolve a coleta de dados dos diferentes sistemas e dispositivos conectados no edifício. Sensores são utilizados para medir informações como temperatura, umidade, qualidade do ar, níveis de iluminação, presença de pessoas e consumo de energia. Esses dados são enviados ao sistema central do BAS, onde são processados e analisados.

Com base nas informações coletadas e em algoritmos de controle pré-definidos, o sistema central toma decisões e emite comandos para os dispositivos conectados. Por exemplo, se os sensores detectarem uma temperatura acima do limite desejado em uma sala, o BAS pode enviar um comando para o sistema de ar-condicionado ajustar a temperatura.

A interface do BAS é geralmente acessada por meio de um painel de controle centralizado, onde os operadores podem monitorar e controlar os sistemas e dispositivos conectados. Também é possível acessar o BAS remotamente por meio de aplicativos ou interfaces web.

Os benefícios de um BAS incluem a redução de custos operacionais, o aumento da eficiência energética, a melhoria do conforto e produtividade dos ocupantes, além do monitoramento e gerenciamento centralizado das operações do edifício.

10.Medidores inteligentes

Smart Meters, também conhecidos como medidores inteligentes, são dispositivos utilizados para medir o consumo de energia elétrica, água ou gás em residências, edifícios comerciais e industriais. Eles são uma evolução dos medidores tradicionais, pois possuem recursos avançados de comunicação e coleta de dados.

O funcionamento dos Smart Meters envolve a coleta de dados de consumo em tempo real. Eles são capazes de registrar e transmitir informações sobre o consumo de energia, água ou gás em intervalos frequentes, geralmente em intervalos de 15 minutos a uma hora. Esses dados são enviados por meio de uma rede de comunicação, como a rede elétrica, redes de comunicação sem fio ou redes de dados dedicadas.

A comunicação dos Smart Meters permite que as empresas de serviços públicos coletem dados de consumo de forma mais eficiente, eliminando a necessidade de leitura manual dos medidores. Os consumidores também podem acessar informações detalhadas sobre seu consumo em tempo real, geralmente por meio de aplicativos ou interfaces online.

Além da coleta de dados, os Smart Meters também podem oferecer recursos adicionais, como tarifação diferenciada, permitindo que os consumidores sejam cobrados com base no horário de uso da energia elétrica. Isso incentiva a adoção de práticas de consumo consciente, ajudando a reduzir a demanda de pico e otimizar o uso dos recursos.

Os Smart Meters também facilitam a detecção de falhas e o diagnóstico de problemas na rede elétrica. Por meio da comunicação bidirecional, eles podem enviar informações sobre interrupções no fornecimento de energia, permitindo uma resposta rápida das empresas de serviços públicos para solucionar problemas.

Em termos de segurança, os Smart Meters possuem recursos de criptografia e autenticação para garantir a integridade e a confidencialidade dos dados transmitidos. Isso protege as informações do consumidor e evita interferências e manipulações indesejadas.