Abstract

With rapid industrial development, safety-critical control applications are increasing in size and complexity. This has resulted in serious challenges for the development of a safety-critical system. E.g., nowadays applications usually have a set of components with different safety integrity levels (SIL). The certification cost of each component is in the direct proportion to its SIL. In order to integrate such applications into one platform, all components have to be certified to the highest SIL, if no sufficient isolation is provided between each other. Consequently, it increases the total certification cost. Meanwhile, hardware platforms with improved processing power are required to execute the applications of larger size.

To tackle the two issues mentioned above, the state of the art approaches are using more Electronic Control Units (ECU) in a federated architecture or increasing the frequency of a processor. In a typical federated architecture, each component of a specific SIL can be allocated on a dedicated ECU, and thus is isolated from components on other ECUs. However, using more ECUs has weaknesses such as error-prone inter-processor (off-chip) connections, large hardware weight and size, and high power consumption. Increasing the frequency of a processor is becoming painful now due to the explosive power consumption. Furthermore, components integrated into a single-core processor have to be certified to the highest SIL, due to that no isolation is provided in a traditional single-core processor. A promising alternative to improve processing power and provide isolation is to adopt a multi-core architecture with on-chip isolation. In general, a specific multi-core architecture can facilitate the development and certification of safety-related systems, due to its physical isolation between cores, low power consumption, on-chip interconnection and natural support to on-chip hardware diversity and redundancy at the inter-core level.

The objective of this dissertation is to propose a multi-core system architecture for safety-critical control applications with reduced certification cost. Partitioning architecture is definitely employed to provide sufficient temporal and spatial isolation between components with different SILs in the multi-core architecture, aiming to support modular certification. It prevents failure propagation between isolated components.

The dissertation focuses on partitioning design of both multi-core hardware and software architectures, in order to minimize efforts and cost of system certification at the integration time. Hardware architecture design concentrates on a firmware architecture on SoC platforms, providing separated hardware execution environments for the software executing on top. Software architecture design concentrates on software multi-core architectures, a multi-core real-time separation kernel and a paravirtualized hypervisor (trusted computing base). From a safety point of view, the multi-core system architecture shall be simple and certifiable, besides provide isolation between its hosted components. The isolation is a good base to implement safety patterns such as redundancy, diagnostics and diversity.

A separation kernel $\text{HARTEX}_{\text{safety}}$ and a paravirtualized hypervisor $\text{RodosViso}_{\text{sc}}$ are proposed to provide isolation mechanisms for small fine-gained applications and large coarse-grained applications respectively. The $\text{HARTEX}_{\text{safety}}$ is extended from a single-processor real-time kernel HARTEX, aiming to enable isolation at the task level and support multi-core platforms. The $\text{RodosVisor}_{\text{sc}}$ is a paravirtualized version from a full virtualization hypervisor RodosVisor, targeting minimized code size, overhead and complexity. It provides isolation between its hosting virtual machines (e.g., general-purpose operating systems, real-time kernels or bare-metal applications).

The proposed multi-core hardware and software architectures are evaluated by the ARTEMIS project RECOMP (Reduced Certification Cost for Trusted Multi-Core Platforms) which this PhD project is a part of, and are tested by a case study (Safe Stop Demonstrator) provided by a local company Danfoss Drives[1].

[1] http://www.danfoss.com/

Resumé

Med den hurtige udvikling i industrielle produkter, så forøges også størrelsen og kompleksiteten af sikkerhedskritiske kontrolsystemer. Dette har ført med sig alvorlige udfordringer for udviklingsprocessen for sikkerhedskritiske systemer. Nu til dags består softwareapplikationer af et sæt af komponenter med forskellige sikkerhedsintegretitetsniveauer forkortet (SIL(Safety Integrity Levels)). Certifikationsomkostningen for hver komponent er direkte proportional med dens SIL. Hvis et sæt af komponenter skal implementeres på en platform, så skal alle komponenterne certificeres til den højeste SIL af de indgående komponenter, hvis der ikke findes nogen isoleringsmekanisme mellem komponenterne. Resultat er forøgede omkostninger til certificering. Samtidig kræves der stadigt kraftigere hardware-platforme til at afvikle de stadigt større softwareapplikationer.

For at håndtere disse to ovennævnte problemer, så er den fremherskende tilgang enten at forøge processortakten (clockfrekvensen) i en enkelt central processeringsenhed eller bruge flere beregningsenheder, de såkaldte ECUere (ECU - Electronic Control Unit), i en distribueret arkitektur. Men svagheden ved at bruge flere ECUere er, at der skal bruges potentielt fejlbare forbindelser mellem dem, hardware af forøget størrelse med deraf følgende højere vægt, derudover følger også højere strømforbrug. Forøgelsen af processortakten er blevet smertelig, fordi den leder til et eksplosivt stigende strømforbrug. Ydermere skal alle komponeænter implementeret på en enkeltkerne-processor certificeres til det højeste SIL af de indgående komponenter, fordi der ikke findes isoleringsmekanismer på en standard enkeltkerne-processor. Et lovende alternativ til at forbedre beregningskraften og indføre isolering af komponenter er at anvende flerkerne-processorarkitektur med indbygget isoleringsmekanisme på chippen. Helt generelt, så kan en specifik multikerne-arkitektur understøtte udviklingen og certificeringen af sikkerhedskritiske

systemer på grund af den indbyggede isolering mellem kernerne, det lave strømforbrug, de indbyggede forbindelser mellem kernerne, og den iboende hardware diversitet, redundans og systemopdeling på inter-kerne niveauet.

Opgaven for denne afhandling er at foreslå og frembringe en flerkerne systemarkitektur for sikkerhedskritiske kontrolapplikationer med reducerede certificeringsomkostninger. Opdelingsarkitekturprincipper er ganske afgjort anvendt for at sørge for tilstrækkelig tidsmæssig og pladsmæssig adskillelse mellem komponenter med forskellige sikkerhedskritiske niveauer (SILs) i flerkerne-arkitekturen. Formålet er at understøtte en modulær certificeringsproces. Opdelingsarkitekturen forebygger fejludbredelse mellem de isolerede komponenter.

Denne afhandling fokuserer på partitioneringsdesign (isolationsdesign) af både flerkerne hardware og softwarearkitekturer med det formål at minimere certificeringsarbejdet og certificeringsomkostningen ved systemintegrationen. Hardwarearkitektur-designet fokuserer på firmware arkitekturer på SOC (system-on-chip) platforme. Med firmware menes her hardwarenær konfigurering og hardwareudlæg samt datastrømshåndtering i hardwaren. Målet er at tilvejebringe et eksekveringsmiljø for softwareapplikationer på platformen. Softwarearkitekturdesign fokuserer på software for flerkernearkitekturer, et separationsunderstøttende flerkerne realtids-operativsystem samt en paravirtualiseret hypervisor (et lavtliggende softwarelag, som muliggør samtidig tilstedeværelse af flere operativsystemer på en platform). Fra et sikerhedskritisk sysnpunkt, så skal flerkernearkitekturen være enkel og certificerbar, foruden at den sørger for isolering mellem de komponenter, som eksekveres på den. Isolationen er et godt udgangspunkt for at implementere sikkerhedskritiske udviklingsmønstre (patterns) såsom redundans, diagnostificering og diversitet defineret i den sikkerhedskritiske standard IEC 61508.

En separationsoperativssystemkerne $\text{HARTEX}_{\text{safety}}$ og en paravirtualiseret hypervisor $\text{RodosVisor}_{\text{sc}}$ er kandidater til at sørge for isolationsmekanismer for respektive finkornede og grovkornede applikationer. $\text{HARTEX}_{\text{safety}}$ er en videreudvikling af den enkelt-kernede realtidsoperativsystemkerne HARTEX. Formålet med denne er at understøtte isolation på trådniveau (en tråd

er en programafvikling) og at understøtte flerkerne-arkitekturplatforme. RodosVisor$_{sc}$ er en paravirtualiseret version af hypervisoren RodosVisor, som er en fuld virtualisering af platformen (paravirtualisering er virtualisering af en delmængde af platformsfunktionaliteten). Formålet er at sørge for isolation mellem de virtuelle maskiner, som er anbragt på platformen (det være sig almindelige operativsystemer, realtidskerneoperativsystemer eller programmer, som kører direkte på hardwaren uden mellemled).

De frembragte flerkerne hardware- og softwarearkitekturer er blevet evalueret i ARTEMIS-projektet RECOMP(REduced Certification Cost for trusted Multi-core Platforms), som dette Ph.D.projekt er en del af. De er blevet testet i en demonstrationsopstilling udgivet af Danfoss Drives (nu en del af Danfoss Power Electronics)