新一代汽车电子系统满足可靠性目标的资源最小化研究

姓名：袁娜
导师：李仁发教授
日期：2017.07.04

目录

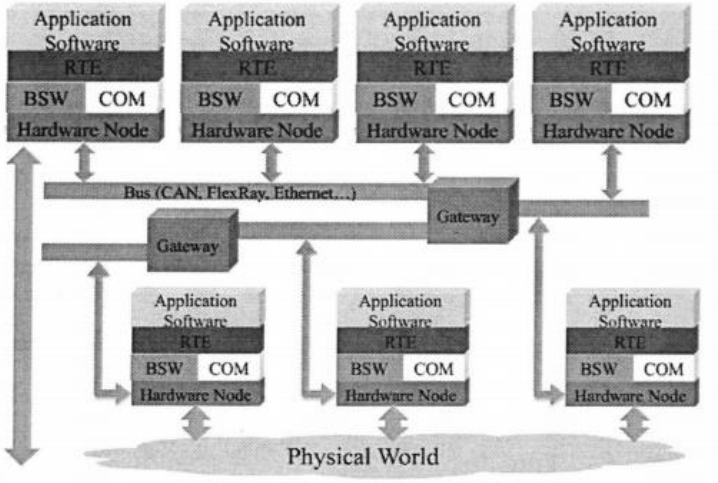
CONTENTS

研究背景（1/2）

➢汽车电子系统—典型的异构分布式嵌入式计算系统

- 为了满足人们在安全性和驾驶性能上提出的更高要求，汽车电子系统的体系结构日益复杂，遍布车内的ECU个数达到100多个，并通过多种车辆网络总线和网关实现互联，系统复杂性骤增；
- 汽车电子系统软件规模骤增，车内的电子化功能个数达到800多个；

汽车产业带来新经济增长方向的同时也在不断革新人们对汽车的认识，汽车已由“会走的一堆钢铁”变成“会走的计算机”。



汽车电子系统的系统结构

现代汽车电子系统中的传感器等处理设备通过与物理世界实现动态交互，通过网络总线交由相应的计算单元处理，并作出正确的行驶、刹车和转向等功能。

因此，异构网络化汽车电子系统是一个同时集成了计算系统、网络系统和物理系统的复杂分布式系统。

研究背景（2/2）

➢汽车嵌入式系统—资源有限的分布式可靠嵌入式系统

- 汽车功能可能随时遭受随机硬件失效、电磁干扰、温度升高、故障传播等安全风险问题，其面临的可靠性问题日益严峻。
- 根据道路车辆-功能安全(Road Vehicles-Functional Safety)标准规范ISO26262，要求设计人员提前评估功能的可靠性，并采取适当的措施最大可能地满足功能所认证的可靠性目标(Reliability Goal)，特别是主动安全功能（如防抱死制动、车身电子稳定、电子制动力分配、前方防撞警示、车道维持、车道偏移警示、驾驶者状态监控、指纹辨识免钥、盲点侦测与开门警示、自动停车导引等）的可靠性目标。
- 嵌入式系统往往资源是有限的，需要在设计阶段进行优化。

研究内容

➢研究的主要内容是基于异构汽车电子系统功能应用的DAG抽象模型，在满足分布式功能可靠性目标上，研究DAG调度的资源最小化问题。

主要研究可以概括为：

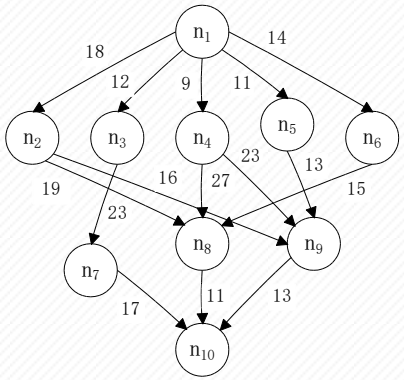
1.非容错情况下，在满足分布式功能可靠性目标基础上，以最小化系统的资源消耗成本；

2.基于容错技术，满足分布式功能可靠性目标下，以最小化资源冗余。

目前研究进度

➢非容错可靠性目标下，资源成本最小化

●分布式汽车功能抽象—DAG模型



●功能可靠性模型

$$R(n_i, u_k) = e^{-\lambda_k \times w_{i,k}},$$

●资源消耗成本模型

$$\cos t(n_i, u_k) = w_{i,k} \times \gamma_k + \sum_{n_x \in pred(n_i)} c'_{x,i} \times \gamma_{\text{comm}},$$

目前研究进度

➢相关最新研究

- 采用一种预分配机制，将功能的可靠性目标转换为每个任务的可靠性目标；在满足任务可靠性条件下，将任务调度至资源消耗最小的处理器上。

$$R_{seq(j)}(G)=\prod_{x=1}^{j-1}R(n_{seq(x)},u_{proc(seq(x))})\times R(n_{seq(j)},u_{proc(seq(j))})\times\prod_{y=j+1}^{|N|}R_{\max}(n_{seq(y)})\geq R_{\text{goal}}(G),$$

$$R_{seq(j)}(G)=\prod_{x=1}^{j-1}R(n_{seq(x)})\times R(n_{seq(j)},u_k)\times\prod_{y=j+1}^{|N|}\sqrt[|N|]{R_{\text{goal}}(G)}\geq R_{\text{goal}}(G),$$

- 问题：预设值过于悲观 消耗过多不必要的资源

目前研究进度

➢算法改进

- 定义两类几何平均值，功能及任务

$$R_{\text{gmf}}(G)=\sqrt[|N|]{R_{\max}(G)}\times\sqrt[|N|]{R_{\min}(G)} \qquad R_{\text{gmt}}(n_{seq(y)})=\sqrt{R_{\max}(n_{seq(y)})\times R_{\min}(n_{seq(y)})}$$

- 改进预分配机制

$$R_{seq(j)}(G)=\prod_{x=1}^{j-1}R(n_{seq(x)},u_{proc(seq(x))})\times R(n_{seq(j)},u_{proc(seq(j))})\times\prod_{y=j+1}^{|N|}R_{\text{gmpr}}(n_{seq(y)})$$

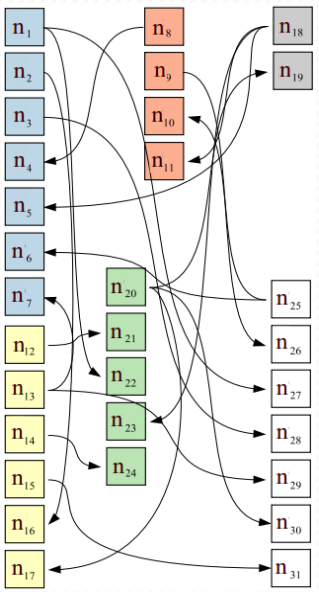
其中，$R_{\text{gmpr}}(n_{seq(y)})=\dfrac{R_{\text{gmt}}(n_{seq(y)})}{R_{\text{gmf}}(G)}\times R_{\text{up\_goal}}(n_{seq(y)})=\dfrac{\sqrt{R_{\max}(n_{seq(y)})\times R_{\min}(n_{seq(y)})}}{\sqrt[|N|]{R_{\max}(G)}\times\sqrt[|N|]{R_{\min}(G)}}\times\sqrt[|N|]{R_{\text{goal}}(G)}$

从而可得每个任务可靠性目标：$R_{\text{goal}}(n_{seq(j)})=R_{\text{goal}}(G)\Big/\left(\prod_{x=1}^{j-1}R(n_{seq(x)},u_{proc(seq(x))})\times\prod_{y=j+1}^{|N|}R_{\text{gmpr}}(n_{seq(y)})\right)$

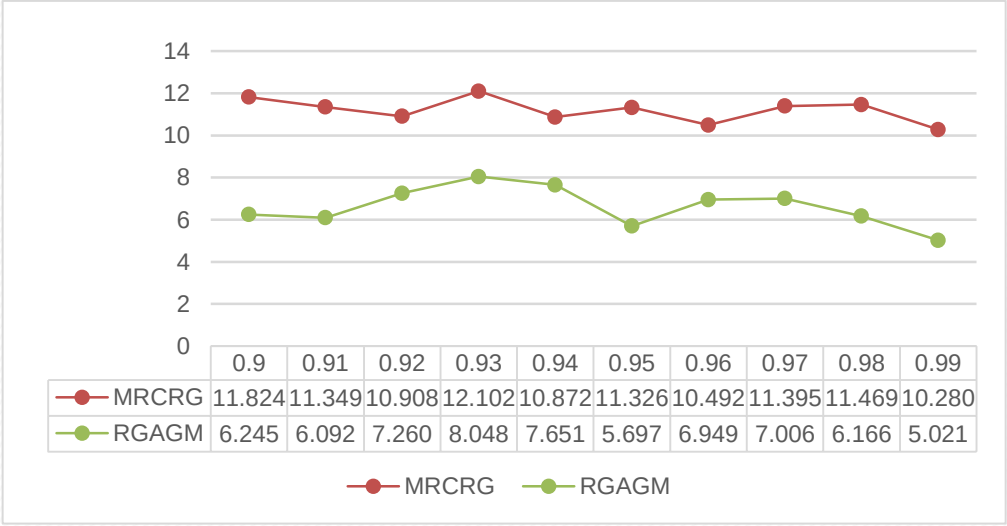
目前研究进度

➢实验结果

- 真实基准汽车



对比不同可靠性目标下的最终资源消耗成本



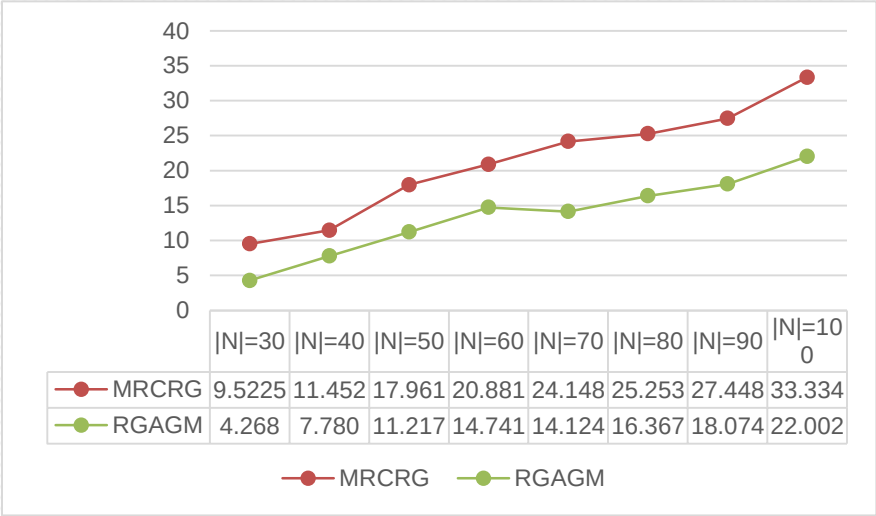
	0.9	0.91	0.92	0.93	0.94	0.95	0.96	0.97	0.98	0.99
MRCRG	11.824	11.349	10.908	12.102	10.872	11.326	10.492	11.395	11.469	10.280
RGAGM	6.245	6.092	7.260	8.048	7.651	5.697	6.949	7.006	6.166	5.021

目前研究进度

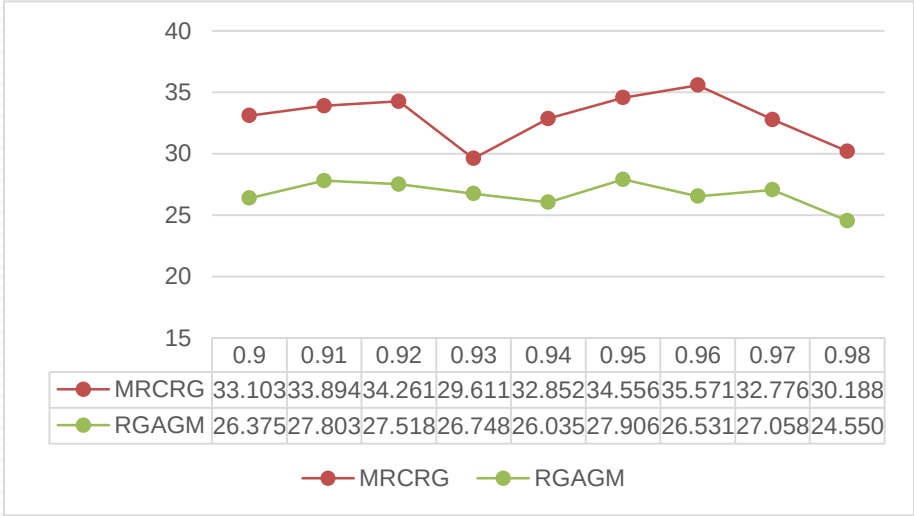
➢实验结果

- 随机生成的分布式汽车功能

不同任务数条件下的最终资源消耗成本



不同可靠性目标下的最终资源消耗成本



目前研究进度

➢小论文

An Effective Reliability Goal Assurance Method using Geometric Mean for Distributed Automotive Functions on Heterogeneous Architectures

Na Yuan[1,2], Renfa Li[1,2,*], and Guoqi Xie[1,2], Xiaoming Chen[1,2]
[1]College of Computer Science and Electronic Engineering, Hunan University, China
[2]Key Laboratory for Embedded and Network Computing of Hunan Province, China
{yuanna0415@hnu.edu.cn, lirenfa@hnu.edu.cn, xgqman@hnu.edu.cn, 260933722@qq.com}
*Corresponding author

***Abstract*—Functional safety is aimed at avoiding unacceptable risks and safety damages due to system functional failures, and it is a critical demand for the automotive embedded systems. The automotive functional safety standard ISO 26262 has clearly stated that it is necessary to take measures to satisfy the designated reliability goals to assure the automotive functional safety. In general, the linchpin of reliability goal assurance method is to transfer the reliability goal of a distributed function to that of each task. This study proposes an effective reliability goal assurance method called RGAGM for automotive functional safety. The core idea of this method is defining two kinds of geometric mean for tasks and function, respectively, and preassigning geometric mean-based reliability values for unassigned tasks, thereby saving more resources for systems. The correctness of the proposed RGAGM method is proved. Experiment results on the real-life automotive function and the randomly generated distributed automotive functions show that the method can effectively ensure the reliability goal and reduce resource consumption cost compared with the existing MRCRG method.**

***Keywords*—automotive embedded systems, functional safety, geometric mean, reliability goal assurance**

I. Introduction

A. Motivation

The automotive electronic system is a typical heterogeneous distributed embedded system. Along with the higher requirements of the safety and comfort for cars, lots of distributed functions have been introduced into the automotive electronic

To ensure the reliability goal of a distributed automotive function, replication-based fault-tolerance is a common used measure. However, resource is limited for automotive embedded systems such that replication is a waste of resource. To assure the reliability goal of a distributed automotive function, the preassignment mechanism of preassigning reliability values for unassigned tasks is a state-of-the-art strategy. The method called minimizing resource consumption cost with reliability goal (MRCRG) concentrates on minimizing resource consumption cost for a reliable function without fault-tolerance [2]. This method can satisfy the reliability goal of function but consumes too much resource due to the pessimistic preassigned values for unassigned tasks. Furthermore, the heuristic method (HRRM) results in excessively high reliability goal of each task when applying it to non-fault-tolerant manner [3]. In summary, existing methods either cannot always satisfy the reliability goal of the distributed automotive function or consume too many resources.

B. Our Contributions

The emphasis of this paper is to present an effective reliability goal assurance method of a distributed automotive function without using fault-tolerance, and take the resource consumption cost as the optimization objective. Our contributions compared with the MRCRG method are summarized as

下阶段研究计划

- 研究容错情况下满足可靠性目标最小化资源冗余，完成实验仿真
- 撰写大论文

THANKS

恳请老师批评指正！

姓名：袁娜
导师：李仁发教授
日期：2017.07.04