



2009

Progress of Computer Technology
and Application 2009'

计算机技术与应用进展

《计算机技术与应用进展》编委会 编

上册



中国科学技术大学出版社

Progress of Computer Technology and Application in 2009

计算机技术与应用进展

• 2009 •



中国仪器仪表学会



中国系统仿真学会



中国仪器仪表学会
微型计算机应用分会



教育部 安全关键
工业测控技术工程研究中心



合肥工大高科



广西大学

中国科学技术大学出版社

2009 • 合肥

图书在版编目(CIP)数据

计算机技术与应用进展·2009/刘晓平,等主编. —合肥:中国科学技术大学出版社,2009.7
ISBN 978-7-312-02565-5

I. 计… II. ①刘… ②蒋… ③李… III. ①计算机科学—文集 ②计算机应用—文集 IV. TP3-53

中国版本图书馆 CIP 数据核字(2009)第 096170 号

书 名: 计算机技术与应用进展·2009
著作责任者: 刘晓平、蒋建国、李琳
责任编辑: 张善金
出 版 者: 中国科学技术大学出版社
地 址: 合肥市金寨路 96 号 邮编: 230026
网 址: <http://www.press.ustc.edu.cn>
电 话: 发行部 0551-3602905 邮购部 3602906 编辑部 3602910
电 子 信 箱: press@ustc.edu.cn edit@ustc.edu.cn
印 刷 者: 合肥学苑印务有限公司
发 行 者: 中国科学技术大学出版社
经 销 者: 全国新华书店
开 本: 880mm×1230mm 1/16 印张: 72 字数: 2348 千
版 次: 2009 年 7 月第 1 版 2009 年 7 月第 1 次印刷
定 价: 298.00 元

Progress of Computer Technology and Application in 2009

全国第 20 届计算机技术与应用 (CACIS) 学术会议

大会主席: 韩江洪 张协奎

程序委员会主席: 刘晓平 钟 诚

组织委员会主席: 李陶深 张建军

大会程序委员: (排名不分先后)

曹广忠 曹 军 陈家新 陈军宁 陈 明 程 恩 程仁洪 冯冬青
龚 昕 韩江洪 韩晓微 胡成全 纪秀花 贾根莲 简 炜 蒋建国
刘晓平 潘汉达 秦 锋 热合木江 邵晨曦 宋宜斌 宋执环 王 军
王晓峰 王忠群 吴乐南 武 文 徐汀荣 尹建华 郁 滨 余成波
袁 涛 查红彬 张继福 张 琳 钟 诚 梁华国 罗月童 李 琳
郑利平 路 强 徐本柱 石 慧

主编: 刘晓平 蒋建国 李 琳

主审: 韩江洪 吴乐南 钟 诚 邵晨曦 宋执环 王晓峰

前 言

中国仪器仪表学会和中国系统仿真学会长期致力于计算机科学与技术的研究与应用推广工作，CACIS 工作年会已成为全国信息学科相关专业互相渗透和交流的重要平台。全国第 20 届计算机技术与应用学术会议（CACIS·2009）暨全国第 1 届安全关键技术与应用学术会议将于 2009 年 7 月 17-22 日在广西大学举行。本届会议将聚集国内外知名专家学者，交流信息理论与应用的研究成果，探讨计算机技术应用、建模仿真以及安全关键技术中的挑战性问题。

主办单位：中国仪器仪表学会（CIS），中国系统仿真学会（CSSS），中国仪器仪表学会微型计算机应用学会（CACIS），中国系统仿真学会复杂系统建模与仿真计算专业委员会筹备处（CSSC）

承办单位：合肥工业大学、教育部安全关键工业测控技术工程研究中心

协办单位：广西大学计算机与电子信息学院、广西大学科技处、广西玉林师范学院、合肥工大高科信息技术有限责任公司、《仪器仪表学报》、《计算机辅助设计与图形学学报》、《系统仿真学报》、《工程图学学报》

会议地点：广西南宁，广西大学

本次学术会议的重点主题是“安全关键技术及其应用”，尤其是系统安全与工业现场安全的相关问题，会议筹备委员会自 2008 年 12 月发出第一轮征文通知后，共收到学术论文 416 篇，内容涵盖了安全关键技术及其应用、计算机仿真方法与应用、计算机辅助设计与图形学、人工智能与算法、软件工程与软件设计、数据库与信息系统、仪器仪表与检测控制、图像与多媒体技术、网络与通讯等相关主题，具有广泛的代表性，经大会程序委员会通讯评审和集中复审，确定了 217 篇收入由中国科学技术大学出版社正式出版的会议论文集，并初步评选出优秀论文 65 篇，大会宣读后的优秀论文将于会后分别被推荐至《仪器仪表学报》、《计算机辅助设计与图形学学报》、《系统仿真学报》、《工程图学学报》、《合肥工业大学学报》、《广西大学学报》。

特别鸣谢：中国科学院沈绪榜院士、奥地利嵌入式 LINUX 专家 Nicholas Mc Guire 教授、台北教育大学 Timothy K. Shih 教授、工大高科信息技术有限责任公司魏臻总裁。

7 月的广西期待着您的到来！

中国仪器仪表学会微型计算机应用学会理事长

广西大学副校长

2009 年 6 月 11 日

目次

大会报告

Floss Software Architecture for Safety Related Systems	Nicholas Mc Guire (1)
计算机的技术演变	沈绪榜 (6)
Video Forgery	Timothy K. Shih (7)
工业铁路智能调度系统的安全关键技术	魏臻 (8)

上册

安全关键应用

工业控制安全研究综述	韩江洪 刘征宇 刘晓平等 (9)
基于角色的 RBAC 模型在保险中介系统中的研究应用	魏亮 周国祥 (16)
基于 d-Left Counter Bloom Filter 的深度包检测	蒋昱城 周健 (21)
基于 IPSec 的 C/S 安全通信模型设计	蒋昱城 周健 潘亚东 (25)
一种基于角色的学习型工作流访问控制模型	方钰 吴国凤 (30)
多路插值求解 RSA 算子	冯新桓 贾启龙 唐宁九 (36)
AdHoc 网络中基于 AODV 协议的安全路由协议	王娟 周鹏 侯整风 (41)
基于 OMNeT++ 的 P2P 系统模型分析研究	朱晓姝 张颖 谭玻 (45)
基于多路数据传输的一种新型加密技术	许洋 冯新桓 贾启龙等 (50)
无线传感器网络加密协议的分析与仿真	王芳 潘舒 范燕等 (55)
SSL VPN 在煤炭行业安全远程访问中的应用	徐畅 (60)
无线 Mesh 传感器网络中的位置隐私	姚剑波 (64)
一种基于攻击树的网络攻击路径生成方法	刘艳芳 丁帅 李建欣等 (69)
一种基于公钥加密的无线传感器网络安全结构	郑文先 姚剑波 文光俊 (78)
可信 KYLIN 安全审计管理研究	李文庆 魏立峰 杨哲 (82)
基于无线传感器的家庭防盗报警系统	张儒瑞 蒋建国 张银霞 (87)
具有突发错误的多阶光存储信道建模及其应用	吴苏婷 熊剑平 贾惠波 (91)
一种基于角色的自主访问控制策略的设计与实现	孟凯凯 魏立峰 (98)
基于 ZigBee 技术的军事定位系统研究	秦旭东 张全红 郑淑丽 (104)
一种新的 Kerberos 认证系统改进方案	姚传茂 (108)
基于蓝牙单芯片的密码算法实现方案研究	黄一才 郁滨 (112)
基于多参数传感器网络可靠性系数 μ 的研究与仿真	方来宝 王健 (117)
基于网格的远程协同故障诊断资源管理模型研究	张利 徐娟 张建军等 (123)
网络安全在电子商务应用中的对策研究	李磊 (128)
关于网络积极防御安全技术的研究	杨剑 鲁昌华 (132)
浅谈安全科学技术学科体系	祝青 刘昱杰 (136)

网络与通讯

ZigBee 技术在无线点菜系统中的应用	孙建梅	陈秀寓	(141)
基于 ZigBee 无线传感器网络的 IPv6 协议栈	戚剑超	魏 臻	(146)
移动 Ad hoc 网络路由协议研究	乔 璐	魏 臻	(151)
一类新型优化模型在 GridFTP 网络环境的超量数据处理特性	冯新桓	贾启龙	唐宁九 (156)
基于分布式 Agent 的网格任务调度模型研究	杨海明 程 龙	赵佛晓	徐 娟 (163)
基于 Jini 的信息栅格组网	李中林 李 辉	张 军	曾丽君 (168)
透视中国电信“全球眼”业务	汪长峰	鲁昌华	(173)
一种关于网格资源出价优化方法的探讨	唐 果	李 浩	姚绍文 (178)
基于怕累托均衡理论的网格资源分配策略研究	孙昌言	李 浩	姚绍文 (185)
使用链表实现无线传感器网络的省电数据存储策略	陈庆章	蔡绍华	陈晓莹 (191)
基于 Netfilter 防火墙的 Per-IP 限速的研究与实现	周 健	孙海霞	(197)
基于数字证书和 Kerberos 协议的身份认证方案	邓科峰	谭子军	周先奉 (203)
基于 IEEE1394 串行总线的网络接口层的实现	宫纪明	刘俊龙	(208)
校园网网络流量分析与控制	刘 平	王 健	(212)
WSN 中 AODV 路由算法的改进和仿真	蔡瑞瑞	周国祥	(216)
基于 CDMA 3G 网络分组域的 VPDN 业务解决方案	杨 陈		(222)
基于语义的 Web 服务匹配算法研究	彭 勃		(229)

人工智能与算法

一种基于 Q 学习的任务调度算法的改进研究	杜 琳	石 慧	刘晓平 (236)
汽车损失神经网络评价模型的研究与设计	徐向东	周国祥	(241)
基于本体的语义检索研究	丁政建	张 路	(246)
基于回程的弱多车场车辆路径算法的研究	王世卿	焦佳佳	李忠信 (251)
一种集成粗糙集与 Logistic 回归的分类模型	叶明全	伍长荣	胡学钢 (257)
TSP 问题的一个新算法	陈 华	管乐乐	宗鹏安 等 (264)
基于模糊 Petri 网的语义 Web 服务组合	吴 亮	袁兆山	(268)
基于 Agent 的 P2P 文件共享系统的研究	王 浩	孔凡林	(273)
基于可拓功能模型与功能树的 FFL 模型研究	陈 欣	路 强	唐益明 等 (279)
一种新颖的概念格构造算法			申锦标 (283)
发布订阅系统中匹配算法的研究	王翠茹	高丽鲜	(288)
战时通信装备的优选方法研究			李剑宏 (293)
嵌入式电脑鼠运行算法的研究			张 晋 (297)
单个销售商垄断电子销售市场的动态定价研究	陆 慧	王金田	(302)
基于遗传算法的异构计算环境独立任务调度	姜志阳	冯圣中	(307)
基于改进遗传算法的足球机器人角色分配	左宏涛	卢锦波	冯新桓 (313)
遗传算法的实现及其在生产调度中的应用	彭 军	徐本柱	刘晓平 (318)
用于行为分析反木马的模糊分类算法研究	陈庆章	莫建华	顾雨捷 (323)
一种挖掘大型数据库的关联规则新算法	李志云	周国祥	(329)
Petri 网的改进的可覆盖性树的构造算法	高 茜	周大均	李爱民 (334)
大规模遥感解译本体存储和推理方法研究	贾晓光	林正位	(339)
智能算法平台中设计模式的应用	金 彤	李元香	王 珑 等 (347)

基于领域知识的虚拟导游行为模型研究	罗月童 陈 韬 孙 静 (353)
1998~2004 年间世界恐怖活动的无标度特性分析	许 晴 祖正虎 郑 涛 (358)
求解 TSP 问题的锦标赛选择模拟退火算法	蔡荣英 钟一文 (364)
K-means 算法在散货船代货运系统中的应用	陈 磊 胡佳敏 严 华 (369)
高职学生综合素质的模糊综合评判	徐祖倩 周国祥 (375)
中文情感倾向分析中主观句子抽取方法的研究	林慧恩 林世平 (379)
基于三 I 方法或 CRI 方法的模糊系统及其响应性能	唐益明 路 强 刘晓平 (385)
基于多核处理器的动态负载平衡并行遗传算法	王力生 张 欣 (390)
基于 K-最近邻居图划分的聚类中心初始化算法	吴继兵 李心科 (395)
An Efficient Processor Allocation Scheme for Three-dimensional Mesh-connected Multi-computers	Hong Yue-hua Xu Shuang Wu Hua-jian (399)
基于多链接分析的主题爬虫设计实现	刘 兵 胡学钢 (404)
模糊数学在巢湖水质评价预测中的应用	王 睿 (409)
数据挖掘算法在保险客户分析中的应用	潘国林 杨 帆 (414)
基于本体的语义网技术在信息检索中的研究	李雪竹 周国祥 (419)
聚类分析在网络舆情监测中的应用	朱晓东 杨国俊 (423)
基于双信息源的协同过滤算法研究	董全德 (427)
基于改进的二进制辨识矩阵的属性约简算法	李 菊 王 军 王 兴 (434)
规则化描述方法中的规则化简方法	魏振春 汪国胜 毕 翔 等 (438)
一种基于等积替换的 CAD 模型简化方法	吴 敏 季 浩 金 灿 等 (442)
基于 BBS 挖掘的危机预测算法	杨国俊 朱晓东 (446)
图像与多媒体	
A "Self-Similar background" Image Compression Method	Su Ze-yang Teng Fei (450)
一种用于印刷品防伪的数字水印算法	王嘉璐 王慧琴 (456)
基于颜色图像分割的 RoboCup 中型组机器人目标识别	刘载文 张 弢 连晓峰 (461)
无损压缩编码方法中的关联性研究	魏 歌 (468)
图形显示控制器的设计与实现	谢 军 吴新军 欧阳伟 (472)
一种基于灰度差阈值的快速车牌定位方法	曹陆军 (477)
基于本体和描述逻辑的图像语义识别	张 杨 房 斌 徐传运 (482)
基于 HOUGH 变换的水表子表中心检测方法	王美玲 黎 宁 高元元 (489)
基于水表自动判读系统的半字识别算法	张星星 黎 宁 李文灿 (493)
基于模糊集的图像增强在车牌预处理中的应用	朱 芳 王晓东 (497)
一种鲁棒的 DCT 域图像水印算法	林洪文 杨绍清 (502)
免疫组化显微图像自动分割方法的研究	董吉文 李 静 (506)
基于聚类与 TSVM 融合的图像通用隐写检测算法	方 昕 钟尚平 (511)
基于 Matlab GUI 的 SAR 图像相干斑检测平台设计	武 文 刘 阳 王晓军 (517)
SAR 图像点目标检测 Pd-SNR 曲线性能评估方法	林 芝 武 文 王晓军 等 (522)
一种基于彩色图像的目标定位算法	方宝富 潘启树 洪炳熔 等 (529)
基于视频相关性的人脸识别算法改进	陈 皓 霍 星 (535)
一种像素不扩展的可验证视觉密码方案	付正欣 王益伟 郁 滨 (539)
极化误差对图像分类的影响分析	武 文 李 昊 王晓军 等 (544)

基于单个平行四边形的摄像机标定方法	徐 伟 郑利平 刘晓平	(551)
基于 ITK 的数字重建放射影像重建算法与应用	闫 锋 罗月童 龙鹏程 等	(556)

下 册

计算机辅助设计与图形学

海军合同战术仿真系统中的碰撞检测算法	严宗睿 张为民 孙向军	(561)
协同环境下面向模型信息安全控制的多角度模型	季 浩 吴 敏 石 慧 等	(565)
一种基于特征点的三维网格数字水印算法	万 杰 刘 辉 胡 敏	(570)
基于 MFC 的 Ogre 三维图形编程框架的设计	瞿德清 罗月童 王晓静	(575)
基于 VRML 虚拟相机控制系统	林丽华 唐依珠	(579)
UG 与 ANSYS 模型格式转换方法研究	李 丹 金 灿 刘晓平	(583)
大区域地物场景数据组织管理方法讨论	王林旭 崔雪峰	(587)
B/S 下基于 XML 的线束图纸绘制	李智慧 徐本柱 刘晓平	(593)
建筑物的三维建模技术研究	何国林 王林旭 崔雪峰 等	(597)
基于多分辨率裁剪纹理的体裁剪技术	罗月童 伍国永 龙鹏程 等	(603)
一种基于错切变形的分布式体绘制算法	张 继 何 兵	(607)
基于操作语义的线束工艺设计系统研究	李忠泽 徐本柱 刘晓平	(614)
Web3D 中复杂交互的实现	刘学超	(619)
基于 Virtools 的 Web 虚拟现实系统的设计与实现	王玉培 郑利平 刘晓平	(623)
OpenGL 纹理映射技术在三维图形逼真绘制中的应用研究	何国林 王林旭 崔雪峰 等	(627)
一种基于手绘二维曲线的三维模型自动生成方法	吴 正 李 琳 刘晓平	(631)
一种非结构矢量场的帧间结构动画处理方法	王 博 何 兵	(635)
线束连接图自动布局研究	徐本柱 程光春 李忠泽 等	(642)
Research on Key Technologies of Virtual Tourism teaching System	刘洪利 王琳琳 石海鹏 等	(648)
基于 LiDAR 点云的城市地面提取	朱晓强 李 琳 余 烨 等	(655)
数据融合技术在 DEM 数据修正中的应用	宋国民	(659)
三维地形模拟基本原理与实现	王德才 原 伟 杨 军	(663)
基于动态反馈的集群渲染系统的实现	付鹏斌 张雪峰 杜金莲	(668)
晶源塑业 PPR 管材 CAD 系统设计	李姜昀	(674)

仿真理论及实践

基于状态修正 Jerk 模型的卫星跟踪多步预测	晏 彬	(679)
基于 SysML 建模和基于 agent 建模的比较	赵立军 张晓清	(684)
通信对抗仿真中一种改进的 Lanchester 作战损耗模型	高春蓉 贲可荣	(690)
基于 Sinda/Fluint 的空间目标红外辐射特性分析	王正宇 赵 阳 王 丽	(695)
计算机仿真中配对实验模型的应用	赵丹亚 王 铮 邵 丽 郑小玲	(700)
基于 LS-DYNA 的高强钢结构轴向冲击性能研究	李 楠	(705)
脉冲多普勒雷达恒虚警检测系统仿真	袁兴生 段 红 姚新宇	(709)
生物战剂采样仿真训练系统设计	王德才 吴明飞 邱云波	(714)
蚁群算法在导航卫星载体姿态测量中的应用	夏 娜 熊平闯 李玉海 唐 媚	(720)
徽派建筑群自动生成方法研究	王启骏 钱晶晶 李 琳 等	(725)

数据库与系统

管理信息系统设计模式的研究与应用	魏 亮 周国祥	(729)
指数平滑模型在农产品价格预测中的应用	苗开超 胡学钢 徐建鹏 琚书存	(734)
MyISAM 存储引擎的分析与改进	张 萍	(739)
冶金企业能源管理系统的实现	谈春燕	(744)
城市公交规划信息数据系统建立方法研究	张欣环 晏克非	(750)
基于 GDI+ 的医疗影像管理系统的设计与实现	于志强 康 青	(755)
嵌入式数据库存储管理机制的设计与实现	薛明星 李绪蓉	(760)
基于决策树技术的新农村建设类型划分	王朝勇	(765)
基于 CBR 的车险公估系统的应用研究	汪 淼 周国祥	(771)
空间数据库模式下的 GIS 协同标绘技术的研究	刘海涛 董国庆 冯少艳	(776)
冰箱动态测试系统的设计与应用	王庆友	(782)
高职院校信息管理系统化的研究与实践	宁书林	(787)
事务管理器构架模型及并发控制协议研究	廖正新	(792)
银行业办公自动化系统建设要点及发展策略探讨	徐 懿	(796)
一种嵌入式数据库内存管理设计与实现	宋 双 王立松	(802)
虚拟数据库技术在传输网管中的应用研究	刘高军 姚文猛	(807)
基于分治融合的混合属性数据聚类算法研究	吴继兵 李心科	(812)
Checksum 技术在文件系统中应用的研究	郑 思 杨 尹	(817)
FCD 道路交通信息采集与应用系统设计与实现	叶加圣 胡学钢 陈 锋	(822)
基于 SOA 技术的保险代理信息管理系统的分析与设计	程晓蕾 周国祥	(828)

软件工程

对象之间连接器的设计与实现	肖 颖 蒋建民 朱恒亮	(833)
军事后勤战时配送式保障系统研究	田 甜 叶雪梅 范青刚	(839)
轻量级嵌入式 TCP/IP 协议栈的设计与实现	张亚魁 魏 臻 刘征宇	(845)
基于 Linux 平台的智能卡通用驱动模型	朱国正 侯整风	(851)
面向方面程序设计的缺陷分析	劳阳辉 施 霖	(856)
RDDM: 一种新的分布式数据挖掘系统	马泽波 蔡 群 张 培	(862)
QoS 驱动的事务性 WEB 服务组合	袁兆山 吴 亮	(867)
一种基于模块化的前端快速开发模式	余镜周 周晓光 苏志远 等	(872)
基于运行时验证的 AOP 程序检测框架	梁 睿 刘林霞 张自强	(877)
Windows Vista 内存保护机制及分析	江 荣 魏立峰 赵 栋 等	(882)
SOA 在应急数据交换、共享平台中的实践研究	武兴悦 石丽梅 王 钢	(889)
基于 SOA 方法的企业服务架构研究	雷傲雄 谢旭升 邓华锋	(894)
基于有限自动机的列车交接系统研究	闫继钢 武文忠 李汉文 等	(899)
Web 服务互操作标准符合性测试框架设计与实现	房友园 齐 璇	(905)
中文文档与源代码间关联关系提取方法的研究	韩晓东 王晓博 刘 超	(912)
一种基于注释的监控编程语言设计与实现	王 涛 郭长国 邹 鹏 等	(917)
三种开源工作流系统中的基本控制流模式的比较研究	王 虎 薛 峰	(924)
数字课程教材教与学服务系统版权管理设计	覃文圣 李 林	(929)
行业细分下的工作室教学研究	胡国雄 黄 莉	(934)

基于 DSC 的工作流模式描述研究	陈娇娇 薛 岗 何象林 等 (938)
初探苹果机下的数据恢复技术	罗 竞 卢 泉 (946)
基于 Microsoft Agent 开发人机交互程序	王德才 原 伟 孙 牧 (950)
Web 服务在电子政务中的应用研究	牛瑞贤 赵 艳 熊 进 (955)
一种动态内存泄露检测方法	许宝喜 王林章 (960)
多需求驱动的测试用例集约简方法	孙富强 王林章 (967)
基于着色 Petri 网的工作流模型的研究与应用	高德平 周国祥 (973)
Scrum 方法的研究与分析	张智海 周国祥 (978)
基于 Ajax 技术 B/S 体系架构系统的研究与设计	郭 元 周国祥 (983)
面向 XML 结构查询的标签位图过滤加速技术	李志云 周国祥 (988)

仪器仪表

电脑织袜机伺服控制系统研究	刘长柱 (994)
一种基于光纤的 USB 转接器	马海燕 韩存武 (999)
一种基于磁阻传感器的无线车辆信息检测系统	姜胜山 李宗伯 肖灿文 等 (1003)
基于冗余容错技术的轨道运输监控终端的设计	史久根 徐 杨 张 超 等 (1009)
基于 MF-RC530 的 IC 射频卡读卡器的设计与实现	余 望 赵云志 (1013)
EBPSK 调制信号的特殊滤波响应	高 鹏 冯 慢 吴乐南 (1018)
一种新型的低电压低功耗 CMOS 电流传输器设计	程 勇 潘 敏 杨依忠 (1025)
天气雷达数据浏览器的设计	范 晖 曹俊武 (1028)
基于正向体效应技术的低压低功耗 CMOS 放大器设计	李建峰 窦建华 潘 敏 等 (1032)
SCCPM 系统迭代检测方法的改进	赵武生 吴克启 韩志学 (1035)
基于 Labview 的虚拟示波器设计及应用	韦 巍 韦 仲 (1040)
系留气球尾翼变形检测方法的研究与应用	谭剑波 郭立俊 (1045)
基于 FPGA 的 EBPSK 调制系统实现	葛玉明 吴乐南 (1049)
基于小波变换的一种 QRS 波检测方法	李 芳 胡志忠 (1053)
基于超声波定位的机车监控与导航系统	张银霞 魏振春 张儒瑞 等 (1057)
ADS1274 及在新型数字三分量检波器中的应用研究	王怀秀 朱国维 (1061)
GPS 导航定位中时效性优化的卫星选择算法	唐 媚 夏 娜 李玉海 (1066)
管道缺陷参数与漏磁场的关系	范 伟 何辅云 陈文明 (1071)
管道磁化方法的研究	何辅云 范 伟 (1076)
CPCI 外设板卡通用设计方法	段玲琳 段晓超 叶明傲 (1081)
基于 GPRS 的 ARM 嵌入式气象监测系统的设计	黄新林 李绍甫 (1085)
基于自适应体偏压技术的低功耗研究	黄新林 窦建华 (1090)
应急指挥车的电磁兼容性分析与设计	陶照清 李绍甫 窦新华 (1094)
基于 Labwindows/CVI 的离网型风力机性能测试系统的改造与应用	韩晓亮 汪建文 (1098)
基于 INTERBUS 总线的兆瓦级风电控制系统设计	王晓华 张 兴 (1102)
基于 PCI 运动控制卡的玻璃切割机控制系统设计	马 瑞 (1107)
电机反时限过流保护模型的分析与改进	史久根 王 磊 洪 杰 等 (1112)
基于多传感器数据融合的机械振动研究	金未平 刘征宇 张 利 (1116)

Floss Software Architecture for Safety Related Systems

Nicholas Mc Guire

Distributed and Embedded Systems Lab, Lanzhou University

Abstract: The utilization of COTS/FLOSS in the context of safety related systems is of interest for technical as well as economical reasons and there are on-going efforts in industry to find solutions to the challenging question of how to utilize FLOSS in safety applications. Substantial research efforts have reached positive conclusions about utilizing COTS, albeit with restrictions^{[2],[5],[4]}.

While building on high-complexity software is in principle contended in much of the safety community, we believe that the vast resource of FLOSS components is of such great utility that it is mandatory to investigate there usage in safety related systems and find answers to the open questions.

Safety critical system design been focused on minimizing complexity of the system most notably of software components which is also suggested by key standards [61508-37.4.2.6]. Here we will argue that while there are grounds to claim that GNU/Linux is conservative with respect to design and technology, it is obviously large and complex, never the less usable if an appropriate solution at the architectural level is designed. These solutions need to address a deeper problem of the safety community, with respect to software: how can we address high software complexity - it is not going to g down in the future and answers need to be found based on sound technical reasoning.

1. Introduction

Utilization of COTS/FLOSS in the context of safety related systems is of interest for technical and also economical reasons. While it is highly contended to utilize high complexity software for safety related systems all together. There have been successful demonstrations of such use at the highest safety integrity level (i.e. SICAS [3], EN 50128, based on diversity).

We believe that the vast resource of FLOSS components is of such great utility that it is mandatory to investigate there usage in safety related systems. Aside from the economical aspects, security aspects, long term stability and reliability play a decisive role why industry is looking into the use of COTS/FLOSS based systems for safety applications.

While space limitations prohibit an extensive design discussion, we outline a possible basic software architecture, allowing to utilize FLOSS for safety related systems.

2. FLOSS for safety related systems

Safety critical systems have traditionally been focused on minimizing complexity of the system - most notably of software components. This is not only due to the exponential efforts of assessment and validation but also firmly rooted in the guiding standards [61508-3 7.4.2.6]. This seems to almost preclude the usage of FLOSS components

in safety related systems (FLOSS being one form of COTS software [prEN 50128 3.18]). Generally 61508 and its derived standards reiterate frequently that

- size
- complexity
- novelty of design
- novelty of technology

are considered critical factors to consider when selecting technical solutions. In this presentation we will argue that while there are grounds to claim that GNU/Linux is conservative with respect to design and technology, it is obviously large and complex, never the less usable if an appropriate solution at the architectural level is designed. These solutions need to address a deeper problem of the safety community, with respect to software: how can we manage the very high complexity of FLOSS based systems ?

Why COTS for safety related systems ?

Before looking at how COTS/FLOSS could be utilized we should look at why this is being discussed in the first place. Taking clause 7.4.2.6 of IEC 61508 which is echoed in many of its derived application specific standards, one might reject the concept of FLOSS for safety related systems in principle - some reasons why we think it is worth looking at:

- recent safety standards are amended with stringent security requirements – one area where FLOSS has proven its capabilities and many bespoke safety critical operating systems have deficits.
- Flexibility of design, most notably of the non-safety related components in the system used for monitoring, remote maintenance or auxiliary services packed on the same hardware simply because the platforms are becoming more and more potent.
- The plethora of available components in the FLOSS community is large and rapidly growing, mandating that an answer in the context of safety related systems for this economically attractive pool of technology be found.
- Stability of COTS/FLOSS systems - though this might well be contended, the stability (reliability, availability) of COTS/FLOSS based systems has proven to be high - most notably in high-complexity systems - it is not a coincidence that quite a few of the top 500 clusters are based on GNU/Linux (notably the current Nr1:Roadrunner)
- Industry is trying to consolidate its OS usage, with GNU/Linux being used widely in embedded industrial applications, extending its use into the high-cost area of safety related systems seems economically sensible.
- Portability properties of FLOSS components
- Maintainability issues, notably personnel availability and long term stability of interfaces (i.e. POSIX, Single UNIX Specifications [?]).

This list of arguments is by no means complete and it is not claiming that usage of opensource in safety related systems is the solution to all safety problems, but it is worth looking into FLOSS as an enhancement of options, with some technical and economic properties that are not found in commercial competitors.

In our research work at DSLab we have identified 6 general approaches to utilizing FLOSS for safety related systems [6], we are not able to outline all of them here, but will focus on one of them - Application level safety.

3. A sample FLOSS safety architecture for application level safety

Traditional approaches of KISS assume that the role of software can be reduced to a minimum, that we can actually know each detail, know the behavior of the system based on rigorous design methodologies, given a specific input data set and a well defined environment. But with large open-source components the picture changes,

we no longer are able to constraint the usage to a well known set of meticulously designed functions, nor do we know the details of how the system will behave on particular inputs - what we do have on the other hand is a level of information on field service that clearly exceeds the information typically available for bespoke software components.

One approach that might come to mind now would be to focus on proven-in-use arguments. While this might be a suitable strategy for some systems, notably those in the SIL1/2 range, we don't see proven-in-use as a sufficient argument on its own – even with extensive, and high-quality bug-tracking available for key GNU/Linux components.

While this data can provide valuable input for selecting components and will impact the ease of certification we propose to investigate architectural options to ensure the required level of safety integrity. Building on diversity i.e. as IEC 61508-6 Appendix E suggests, is one option to utilize COTS software components in safety critical systems, here we would like to introduce an alternative approach based on placing the COTS hardware and software components into a "gray-channel" arguing the SIL at the application level only.

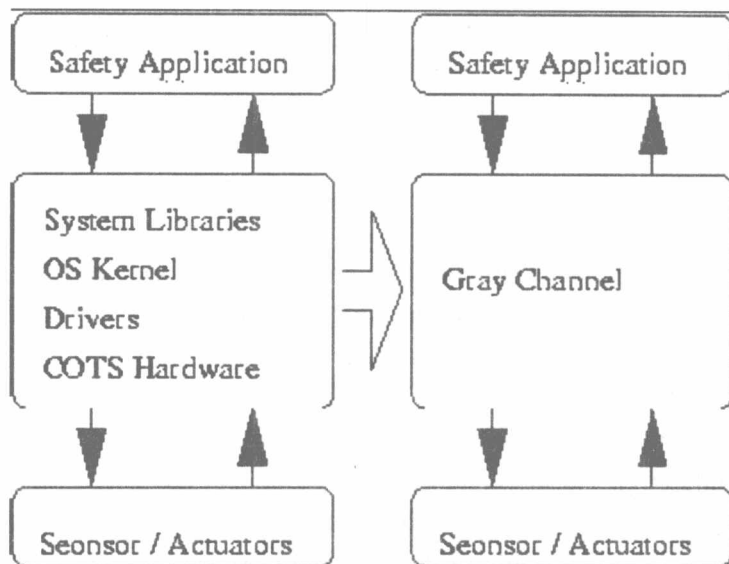


Figure1: Gray Channel for COTS/FLOSS

The application model is a general "control-loop" of read data, process data, write data with the data coming from the sensors and results going to the actuators. This model is not concerned with the correctness of the bespoke algorithm nor with the implementation of the same. The safety application is assumed to be a bespoke software components, achieving its safety integrity by a suitable process - it is assumed to be suitable for the SIL in question. The Sensor/Actuator is considered to be safe appropriate to the required SIL and also no considered, further, and this is still a limitation of this model, we are assuming that there is no direct feedback possibility, at the software level, from the gray-channel to the sensor/actuator other than the data channels (i.e. via Ethernets).

4. Fault Class Mapping

Instead of a traditional FMEA type mapping we approach the problem slightly differently- we look at general fault classes and which of them could lead to detection problem and thus impact the safety properties of the safety application.

To argue such a container of "unknown software", potentially allowing to utilize COTS components of arbitrary

complexity we use a generic fault model.

- Random Faults that impact the properties of the gray-channel
- Systematic Faults that impact the properties of the gray-channel
- Random Faults in the gray-channel that "feed-back" to the safety application
- Systematic Faults in the gray-channel that "feed-back" to the safety application

If all four can be shown to lead to no undetected fault at the safety application, we believe this is a potentially suitable architecture to utilize COTS components of high-complexity - i.e. GNU/Linux.

4.1. Faults within the gray-channel

For data traversing the gray-channel EN 50159 has suitable methods available, some of the needs resulting are

- appropriate checksums on data objects - detection of random and systematic modification in the data channels.
- sequence numbers on data objects being transmitted, ensuring the detection of retransmission of old data or missing of a data object.
- timeout response on failure to receive data at the receiving side, ensuring that a fail-silent application does not go undetected.

The problems of random and systematic faults within a communication channel, which is a full featured FLOSS OS in this case, can be considered resolved.

4.2. fault feed-back to the safety application

The more problematic realm is the faults introduced by unintended feedback from the gray-channel to the safety related software. This can be split into the two broad categories of random and systematic faults.

4.2.1. Random faults

To address random faults, the simplest option is to provide redundancy at the application level, note that we are assuming replication of the identical application, with the constraint that there are no functionally shared components at the application level. The constraints introduced are that the sensor/actuator must be able to handle multiplexing demultiplexing and voting of data received from the duplicated (but independent) applications, and thus random faults impacting the functionality of the application or the data are mitigated at the sensor/actuator level.

4.2.2. Systematic Faults

The big problem are the systematic faults that the components in the gray-channel may inflict on the safety application, OS and hardware have the quite obvious potential to directly impact any application level flow of control or data objects. To mitigate systematic faults we distinguish between text segment (code) manipulation and data segment manipulation.

Text segment modification:

Text segment modification can be detected by traditional means of running CRC checks on the text-segments, this could be run at application level on a per-request basis preceding any calculation, to ensure that the check itself is not disabled by faults in the text-segment, qualification of the test-results are left to the actuator, thus the property of text-segment correctness is diversely represented and manipulation can be detected again at the (external) actuator level.

Data modifications:

Systematic data modification are problematic because they constitute single points of failure, a single instruction i.e. adding two values modified to subtract the same two values by sign inversion of one of the values (a single bit

is flipped) would not alter the flow of execution nor would it necessarily break the algorithmic logic - thus stay undetected.

A systematic fault has the property of introducing a unintended state transition in a system when a particular context is given - every time this context is presented to the system. Thus one defense would be diversity at the application level. Coded monoproducts have been proposed to mitigate these faults, explicit N-version programming (with all its known problems) has been in discussion, and forms of automated or inherent diversity also look like an option to be looked into.

With these constraint in mind we arrive at a possible architecture allowing to build on complex COTS software components that looks like this:

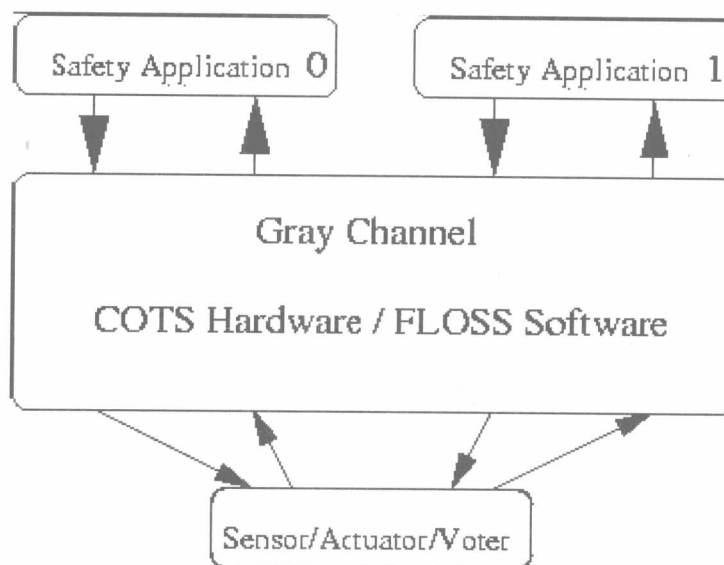


Figure2: Application Level Safety

5. Conclusion

With appropriate software architecture utilization of COTS/FLOSS for safety critical application is feasible. We believe that for technical and economical reasons the option to utilize FLOSS in this challenging domain is worth the effort of resolving open issues with integration of unsafe software components of high complexity for systems of even the highest safety integrity levels. Safety standards have been moving forward on the issue of FLOSS usage (notably prEN 50128) and we expect more functional safety standards to address the open-issues in the future. Usage of FLOSS is not the answer to all safety problems, and such a paradigm change, in it self, exhibits a potential to introduce hazards, thus it needs to be done carefully and based on an open discussion in the safety community. We hope that we can contribute to igniting this discussion.

计算机的技术演变

沈绪榜

中国航天电子基础技术研究院研究员

“每一次长周期的技术大革命的爆发和大规模扩散都要引发整个经济社会的结构性转变。”上世纪美国最后一位诺贝尔奖获得者发明的集成电路，促进了硅芯片的长周期的技术大革命，特别是微处理器的发明，实现了计算机的廉价制造和批量生产。促进了计算机产业与电信产业的发展，使 9 亿人口进入了知识社会。技术可以造就许多种未来，我们真正得到的未来取决于技术和其它因素的相互作用。这些因素包括法律、规章、文化，特别是人。“谁能适应不断加快的技术变革，谁就能生存下去。”计算机的技术演变包括设计、应用和制造三个方面。

研究表明：由于日益增长的晶体管数量和越来越快的晶体管开关速度，集成电路的能力正以每年 74% 的速度增长。而常规体系结构的处理器尽管采用了深度流水线技术，试图支持每个周期能执行一条指令，但预计计算机的性能每年只有 19% 的增长速度。这些数字差别表明，计算机的设计具有极大的发展机会，它的设计技术演变包括算法、模式与结构的演变。

计算机应用的技术演变是以芯片的技术演变为基础的，有高性能计算，网络计算，嵌入式计算，以及飞天梦想与人工智能。计算技术的太空应用是因为“将地球、空气和重力抛在身后，是人类自古以来的梦想（2003 年 2 月“哥伦比亚”号 7 人遇难）”。人工智能（Artificial intelligence）一词是在 1956 年 Dartmouth 学会上提出的，其目的就是要让机器人能够像人一样思考。

现代计算机实现技术进步的基础，是贝尔实验室的固体物理学家肖克莱（W.Shockley,1910-1989）和巴丁（J.Bardeen,1908-1991）以及布莱顿（W.H.Brattain,1902-1987），于 1947 年 12 月 23 日发明的晶体管，1956 年获得诺贝尔物理学奖，晶体管使计算机的体积、功能、速度、价格与可靠性等方面取得了划时代的进步。1958 年杰尔·基尔比（Kilby）研制成功了世界上的第一块晶体管集成电路（IC, Integrated Circuit），又叫做芯片（Chip, die）。相隔 42 年之后的 2000 年，基尔比获得了诺贝尔物理学奖，人们肯定了芯片在信息社会发展中的基础作用。硅基芯片是按照摩尔预言的速度演变的。

上世纪 50 年代 IBM 曾完成过一次市场调研，此调研预言全世界只需要 6 台计算机；1978 年 IBM 的数字设备公司的执行总裁 Ken OLSON 说，他不能够想象为什么每一个人需要一台计算机；20 世纪 80 年代中期，Biu Gates 说，没有人需要大于 640K 内存的计算机 这些非常不准确的预测表明，计算机应用在技术方面所积累的量变，最终会导致质的改变，正像摩尔定律所预言的那样。目前的问题不是技术演变的路标，而是芯片制造的产业现实，如今开工一家新的工厂需要投入 30 亿美元。真正的突破并非是技术演示，而是制成人们可以使用的系统。

2009 年 6 月