基于Copula的ERCS系统软硬件综合可靠性建模与分析

郭荣佐
(四川师范大学计算机科学学院 成都 610068)

摘 要 在现代的电子业、制造业和工业控制等系统中,系统的可靠性越来越重要,而嵌入式实时控制系统(Embedded Real-time Control System,ERCS)大部分是控制系统的核心部分,其系统可靠性尤为重要。首先对嵌入式实时控制系统软硬件进行形式化抽象定义;然后对不可再分的软件模块和IP硬核进行可靠性建模,应用Copula函数对软件子系统和硬件子系统分别进行建模,并建立了ERCS系统的软硬件综合可靠性Copula模型;最后应用建立的模型,对具体的系统进行了软硬件综合可靠性计算。通过实例计算可知,用Copula建立的ERCS软硬件综合可靠性模型考虑了软件各个模块间、硬件各个IP硬核间和软硬件间的相依性,使得ERCS软硬件综合可靠性比独立时有所提高。

关键词 Copula函数,可靠性,建模与分析,嵌入式实时控制系统,软硬件
中图法分类号 TP302.7,TP202+.1 **文献标识码** A

Integrated Reliability Modeling and Analysis of Hardware/Software of ERCS System Based on Copulas

GUO Rong-zuo
(College of Computer Science,Sichuan Normal University,Chengdu 610068,China)

Abstract The reliability of a system employs an increasing important issue in modern day electronic,manufacturing and industrial systems,and most of the control systems are the core part of Embedded Real-time Control System(ERCS),and the system reliability is especially important. At first,formalization of the hardware/software of ERCS was defined. Then,reliability modeling was given for software modules which can not be subdivided and for IP hardcore. The reliability modeling of hardware/software of ERCS was also provided by applying Copula function. The integrated reliability modeling of software and hardware of ERCS was also established by applying Copula function. The reliability of specific system hardware/software was calculated by using the model. The results show that the reliability model established with Copula function takes account of the correlation between software modules,IP hardcore and hardware/software,therefore the integrated reliability of hardware/software of ERCS is improved compared with the independent hardware and software.

Keywords Copula function,Reliability,Modelling and analysis,Embedded real-time control system,Hardware/software

1 引言

嵌入式实时控制系统(Embedded Real-time Control System,ERCS)是以嵌入式系统技术和实时控制技术等为基础、以具体控制为中心的软硬件可裁减的专用实时控制系统。ERCS是包括硬件子系统和软件子系统的综合系统,其功能的实现需通过复杂的硬件和软件协同方能完成,任何软件或硬件的故障、失效和超时,都将导致系统故障。

嵌入式实时控制系统综合可靠性是指系统软件、硬件在规定的条件、规定时间内,完成规定实时控制功能的能力。国内外学者已对软/硬件综合系统可靠性进行了相关研究。杨鹏飞、谭维康[1]对等待系统软/硬件的可靠性进行了建模与分析,给出了该系统的可靠性指标;于敏[2]等从软/硬件综合系统的故障原因、容错技术和失效模式入手,提出了基于Markov过程的软件、硬件相关联的系统可靠性模型,并对系统可靠性进行了分析;吴祥[3]等从软件、硬件特性入手,对计算机系统的可靠性进行了分析,但假定系统由相互独立的软件、硬件串联构成。Michael Allan Friedman[4]等对软/硬件联合系统进行了可靠性研究,系统设计的不同阶段对系统可靠性的影响是不同的,假定各个阶段相互独立,从而研究软/硬件联合系统的可靠性;Kiran Kumar Vemuri[5]等利用故障树对复杂软硬件系统的可靠性进行了分析,但未对硬件、软件之间的依赖关系对系统可靠性的影响进行论述;Xiaolin Teng[6]等将软/硬件系统故障分为硬件故障、软件故障和硬件交互失效,利用Markov过程进行系统可靠性建模并对实际系统进行了可靠性分析。这些研究一般假设软件与硬件相互独立,没有考虑软件与硬件之间的相互依赖、相互联系,未能建立一种能够描述和分析软/硬件综合系统的可靠性模型。

ERCS是软/硬件相互联系、相互依赖的综合性系统,其可靠性除与软件、硬件相关外,还与软/硬件的相互依赖、相互联系相关。Copula理论构造多维联合分布无需对边缘分布作任何假设,即可得到各种不同的多元分布;也可以将边缘分

到稿日期:2013-06-09 返修日期:2013-08-03 本文受四川省教育厅自然科学重点项目:嵌入式实时控制系统可靠性保障技术及策略研究(10ZA008)资助。

郭荣佐(1973-),男,副教授,硕士生导师,主要研究方向为嵌入式系统、物联网感知技术和可靠性理论与应用等。

布与相关结构拆开分别进行讨论，多元概率分布的研究就变得更为简单。Copula 理论及其应用发展非常迅速，特别是本世纪近 10 年来，Copula 技术在金融、保险、生物和医药等多个领域得到广泛应用[7]。近年来，国内外学者将 Copula 理论应用于系统可靠性方面。文献[8]对具有相依性的 k/n 表决系统的可靠性进行了研究，用 Copula 函数将相依的部件联系起来，建立可靠性模型。文献[9]利用 Copula 的象限相关性对系统可靠性指标的影响，研究了两相依部件并联冗余系统的可靠性，但未对系统可靠性指标的影响程度进行定性或定量分析与计算。文献[10]应用 Gaussian Copula，对输入变量的相互关联方式下的可靠性优化问题进行了研究。Copula 理论用于研究具有相依性的部件，为研究软/硬件综合系统可靠性提供了新的理论基础和方法[11]。这些工作促进了 Copula 理论的完善及其在可靠性方面的应用，但对 Copula 理论在 ERCS 软/硬件可靠性方面的研究还未涉及。因此，本文利用 Copula 函数研究 ERCS 的软/硬件综合可靠性是十分必要的，亦是具有重要意义的。

2 目标 ERCS 定义

ERCS 在设计时，先依据实际需求，对系统进行建模分析和软硬件划分，将系统功能划分为合适的软件、硬件予以实现[12]。硬件由若干功能相关的 IP 硬核构成，每个 IP 硬核由电子元器件(Electronic Components，EC)、电路及其结构(Circuit and its Structure，CiS)、电路板(Circuit Board，CB)和执行装置(Executive Device，ED)等组成[13]。要实现特定 ERCS 的功能，必须在需求分析完成后，对系统功能进行划分，给出各个功能得以实现的硬件基础。

假设 ERCS 的硬件组成及约束为：电子元器件 I_{EC1} 不超过 B_1，可选电路及其结构 I_{CiS2} 不能超过 B_2，…，电路板布线方式 I_{CBn} 不能超过 B_{n-1}，执行装置可选种类或可选装置不超过 B_n；而某种功能的可选硬件有很多种，这些可选的硬件又具有不同的可靠性参数。假设 C_{ESH} 为 ERCS 的硬件 IP 核，则为一个 n 元组，即 $C_{ESH}=(I_{EC1},I_{CiS2},\cdots,I_{CBn-1},I_{EDn})$，其中 I_{EC1}，I_{CiS2}，…，I_{CBn-1}，I_{EDn} 是与组成 IP 核硬件相关的 EC、CiS、CB 和 ED。而 ERCS 的硬件由若干个功能单元构成，即 $E_{ESH}=\{F_1,F_2,\cdots,F_M\}$，每个功能单元对应多个可选的 IP 核集合，即：

$$F_1\rightarrow\{C_{ESH11},C_{ESH12},\cdots,C_{ESH1a}\},$$
$$F_2\rightarrow\{C_{ESH21},C_{ESH22},\cdots,C_{ESH2b}\},$$
$$\cdots\cdots,$$
$$F_M\rightarrow\{C_{ESHm1},C_{ESHm2},\cdots,C_{ESHmn}\},$$

其中 $C_{ESH}=(I_{EC1},I_{CiS2},\cdots,I_{CBn-1},I_{EDn})$；$a,b,\cdots,n$ 是常数，分别表示 $F_1,F_2,\cdots,F_M$ 所对应的可选 IP 核的数目。因此，ERCS 的硬件就是寻求 C_{ESH} 的最优组合，且该组合满足：

$$S_1(I_{EC1i},I_{EC2j},\cdots,I_{ECmk})\leqslant B_1,$$
$$S_2(I_{CiS1i},I_{CiS2j},\cdots,I_{CiSmk})\leqslant B_2,$$
$$\cdots\cdots$$
$$S_n(I_{ED1i},I_{ED2j},\cdots,I_{EDmk})\leqslant B_n;$$

其中 $S_1,S_2,\cdots,S_n$ 分别对应为不同硬件组成部件 I_{EC1}，I_{CiS2}，…，I_{EDn} 和约束 $B_1,B_2,\cdots,B_n$，用来分析和计算由多个 IP 核组成的 ERCS 硬件，它们的计算方法由对应的功能和可靠性指标共同决定。

ERCS 软件子系统由板级支持包(Board Support Package，BSP)、嵌入式实时操作系统(Embedded Real-time Operating System，ERTOS)、设备驱动程序(Device Driver Program，DDP)、操作系统抽象程序(Operating System Program，OSAP)、文件系统(Files System，FS)、网络协议(Network Protocol，NP)、图像用户接口(Graphical User Interface，GUI)和实时控制应用程序(Real-time Control Application Program，RCAP)等组成。按照 ERCS 软件子系统的各个组成功能单元的约束条件，采用与其硬件相似的形式化定义，可得到其软件的抽象模型。而软件的各个功能间不是完全独立的，它们之间具有一定的相依性。

综上，可得到 ERCS 的软硬件形式化抽象模型，如图 1 所示。

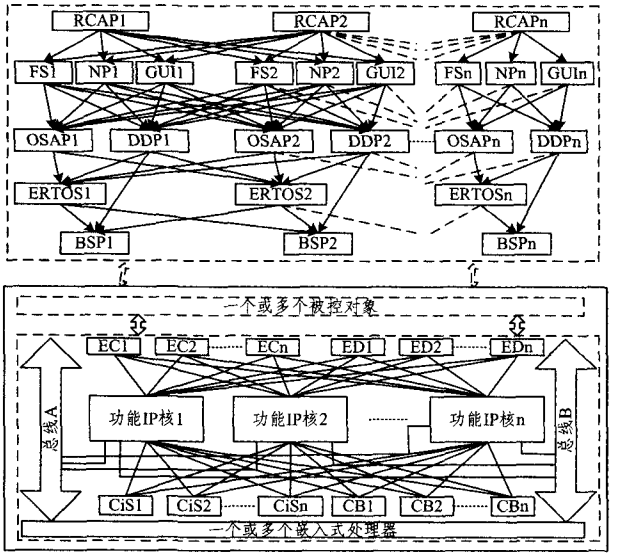

图 1 ERCS 系统软硬件抽象模型

3 ERCS 的 Copula 可靠性模型

3.1 单位块的可靠性模型

ERCS 的软件、硬件都是由一定的单位块组成，硬件的单位块为 IP 硬核，软件的单位块为不可再分的模块，因此，需要分别研究其单位块的可靠性模型。

单个 IP 硬核由 I_{EC1} 个电子元器件、I_{CiS2} 种可选的电路及其结构和 I_{CB3} 种电路板布线方式等构成。而 IP 硬核在设计完成之后，假设使用的元器件或部件的种类为 n，则依据参考文献[13]得到 IP 硬核的 EC 失效率为：

$$\lambda_{IPECi}=\sum_{i=1}^{n}N_i(\lambda_G\pi_Q)_i \tag{1}$$

其中，λ_{Gi} 为第 i 类器件或部件的通用失效率；π_{Qi} 为第 i 类器件或部件的质量系数；N_i 为第 i 类器件或部件的数量；n 为不同器件或部件的种类数。由此得到单个 IP 硬核的可靠度计算模型为：

$$R_{IPi}(t)=e^{-\lambda_{IPi}t} \tag{2}$$

其中 $\lambda_{IPi}=\lambda_{IPECi}+\lambda_{CiSi}+\lambda_{CBi}+\lambda_{EDi}$ 为 IP 硬核失效率。

若 ERCS 的软件模块仅有正常和失效两种状态。模块失效可分为模块内部可改正的错误所致的模块失效、模块内不可改正的错误所致的模块失效和模块正确情况下模块运行产生的硬件故障所致的失效等，不同的失效原因引起的失效，其失效率不相同。依据参考文献[14]有：

$$\lambda_i=abe^{-bt}+e^{-at}+ae^{-at} \tag{3}$$

其中，a 为软件模块被发现的错误的期望；b 为比例常数；c 为

常数；α 为难以确定的因素造成模块失效次数的期望。

ERCS 的软件模块失效为不可维修型，故可用 Markov 理论建立软件模块的状态转移图，如图 2 所示，其中“0”表示模块 j 正常运行、“1”表示模块 j 失效。则可得如下方程：

$$p_j'(t)=A\cdot p_j(t) \tag{4}$$

其中，$A=\begin{bmatrix}-\lambda_j(t) & 0\\ \lambda_j(t) & 0\end{bmatrix}$，初始条件为 $(p_{j0}(0),p_{j1}(0))=(1,0)$。解此微分方程有：

$$\begin{cases}p_{j0}=e^{-\int_0^t\lambda_j(y)dy}\\ p_{j1}=1-p_{j0}\end{cases} \tag{5}$$

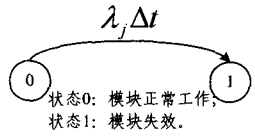

图 2　模块状态转移图

而 ERCS 的软件具有很强的实时性要求，即所有软件模块必须在规定时间 t_0 内完成，若时间超出 t_0，则视为模块失效。软件模块 i 由状态 0 转移到状态 1，访问状态 0 的次数 V_{i0} 为：

$$V_{i0}=1+\sum V_{i1}\cdot(1-p_{i0}) \tag{6}$$

其中，V_{i0} 表示访问状态 0 的次数；p_{i01} 表示由状态 0 到状态 1 的转移概率。假设每次访问状态 0 的时间为 t_i，则可用 $V_{i0}t_i$ 表示模块运行时在状态 0 上需要的平均时间，模块 i 运行所需的时间为：

$$\bar{t}_i=\frac{1}{n}\sum_{i=1}^{n}V_{i0}t_i \tag{7}$$

若 ERCS 软件模块 i 的可靠度表示该模块正常运行的概率，则可用 $R_{SWi}(t)$ 来描述模块在规定时间 t 内的正常运行概率，则可定义 $R_{SWi}(t)$ 为：

$$R_{SWi}(t)=e^{-\int_0^{\bar{t}_i}\lambda_i(t)dt} \tag{8}$$

其中，R_i 表示模块 i 的可靠度；$\lambda_i(t)$ 表示模块 i 的失效密度函数；$\bar{t}_i$ 表示访问模块 i 的平均时间。

由此，可得到模块 i 的可靠度为：

$$R_{SWi}(t)=e^{-\int_0^{\bar{t}_i}\lambda_i(t)dt}=\exp(-\varphi(t)) \tag{9}$$

其中：

$$\varphi(t)=\int_0^{\sum_{i=1}^{n}(\sum V_{i1}\cdot p_{i1}+1)t_i}\lambda_i(y)dy$$

$$\lambda_i(y)=(abe^{-by}+e^{-cy}+\alpha e^{-cy})y$$

3.2　Copula 可靠性模型

完整的 ERCS 由 3 个部分组成，即嵌入式硬件系统、嵌入式软件系统和控制执行机构。在此假设控制执行机构可靠度为常数，且等于 1，则 ERCS 的可靠性就由嵌入式硬件和软件两部分决定。

3.2.1　软件可靠性模型

ERCS 的软件系统由 BSP、ERTOS、DDP、OSAP、FS、NP、GUI 和 RCAP 等模块组成，每个模块又由若干个子模块构成，在此假设 BSP 的子模块数不超过 N_1，RTOS 的子模块数不超过 N_2，…，RCAP 的子模块数不超过 N_n，则可对 ERCS 的软件系统进行抽象，得到如图 3 所示的层次结构和抽象图[15]。

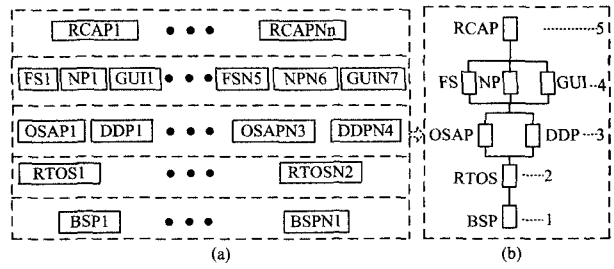

图 3　ERCS 软件体系结构及其抽象

由文献[16]可知软件模块的可靠度为：

$$R_{mc}(t)=\sum \mathrm{sgn}(F)C^n(F) \tag{10}$$

其中，$F=(F_1,F_2,\cdots,F_n)$，$F_i=F_i(t_i)(i=1,2,\cdots,n)$ 或 1，因 $F_i(\infty)=1$，$\mathrm{sgn}(F)=\begin{cases}1, & \text{有偶数个子模块 } F_i=F_i(t)\\ -1, & \text{有奇数个子模块 } F_i=F_i(t)\end{cases}$。

从而得到 OSAP 与 DDP 并联的可靠度为：

$$\begin{aligned}R_3(t)&=P\{\max(X_{OSAP},X_{DDP})\}\\&=1-P\{\max(X_{OSAP},X_{DDP})\leqslant t\}\\&=1-C^2(1-R_{OSAP}(t),1-R_{DDP}(t))\end{aligned} \tag{11}$$

其中，$R_{OSAP}(t)$，$R_{DDP}(t)$ 服从式(10)。可得到 FS、NP 和 GUI 组成的三模块并联相关结构的可靠度为：

$$R_4(t)=1-C^3(1-R_{FS}(t),1-R_{NP}(t),1-R_{GUI}(t)) \tag{12}$$

其中，$R_{FS}(t)$，$R_{NP}(t)$，$R_{GUI}(t)$ 服从式(10)。

由此可得到 ERCS 系统的软件 Copula 模型为：

$$\begin{aligned}R_{SWr}(t)=1-&\sum_{i=1}^{5}(1-R_i(t))+\sum_{1\leqslant i<j\leqslant 5}C^2(1-R_i(t),1-R_j(t))-\sum_{1\leqslant i<j<k\leqslant 5}C^3(1-R_i(t),1-R_j(t),1-R_k(t))+\sum_{1\leqslant i<j<k<m\leqslant 5}C^4(1-R_i(t),1-R_j(t),\\&1-R_k(t),1-R_m(t))-C^5(1-R_1(t),1-R_2(t),1-R_3(t),1-R_4(t),1-R_5(t))\end{aligned} \tag{13}$$

其中，R_1，R_2，R_5 分别表示模块 BSP、RTOS、RCAP 的可靠度，由式(10)描述；R_4，R_5 分别由式(11)、式(12)给定。

3.2.2　硬件可靠性模型

对硬件进行可靠性建模时，需对图 1 的硬件抽象模型进行实例化描述。每个 IP 硬核执行或完成一定的功能，为单一或多功能的硬件模块，若干 IP 硬核按照具体应用进行特定的裁减或组合，成为专门用途的嵌入式系统。图 4 为图 1 的实例化描述图，图中将 IP 硬核对应为实例化的功能模块，而现场的各种模块仅控制使用的嵌入式系统才具有，故在图中使用虚线进行描述。

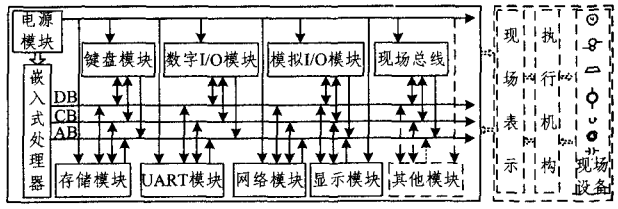

图 4　嵌入式系统硬件实例化描述图

由图 4 可知，电源模块的可靠性直接影响整个嵌入式系统的可靠性，更会影响系统各个模块的可靠性，因此，电源模块与嵌入式处理器和各种模块间构成串联相依关系。而作为一个完整的嵌入式系统硬件平台，其存储器也是至关重要的，所有的设备驱动、RTOS 和组件、构件、应用程序等都存储在存储器中，由此使嵌入式处理器与存储器间构成串联相依关系。各种应用接口模块的启动、运行都与存储器有关，即都是从存储器读取程序运行而操作各种接口，实现数据的输入输

出，故存储器与各种接口间构成串联相依关系。信号输入模块采集信号，输入到嵌入式处理器和存储器，进行处理后，输出到显示模块、现场总线、网络模块或其他模块；信号输入模块包括 UART 模块、网络模块、键盘模块、现场总线和模拟/数字出入等。由此使信号输入模块、嵌入式处理器、存储器和输出模块间构成串联相依关系。各信号输入模块、输出模块为并联相依关系。综上，电源模块与嵌入式处理器、存储器串联相依，作为一个整体与各种接口模块又构成串联相依关系而成为一个系统，故可得嵌入式系统硬件的相依性抽象图，如图 5 所示。

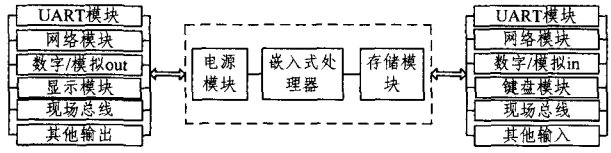

图 5　嵌入式系统硬件模块间相依关系抽象图

硬件子系统各个组成部分任意一个硬件功能模块失效都可能引起系统局部或全局失效，从而导致不能实现规定的功能，因此，可用并串联混合相依特性来表示各个功能 IP 硬核的关系。

而每个功能 IP 硬核正常运行的概率由式(2)予以确定，由上述分析和 Copula 理论，可得系统硬件可靠度为：

$$R_{HWr}(t)=1-(1-R_{MinS}(t))-(1-R_{intM}(t)+C^2(1-R_{MinS}(t),1-R_{intM}(t)) \tag{14}$$

其中，$R_{MinS}(t)$表示图 5 虚线框内各部件的相依可靠度；$R_{intM}(t)$表示各种接口模块间的相依可靠度。

又电源模块为单一硬件模块，其可靠度由式(2)予以确定；存储器模块一般由 Nand Flash、Nor Flash 或 EEPROM 等组成，其构成相依关系为 Nand Flash、Nor Flash 并联后与 RAM 串联，由此得到 R_{MinS} 为：

$$R_{MinS}(t)=1-\sum_{i=1}^{3}(1-R_{HWi}(t))+\sum_{1\leqslant i<j\leqslant 3}C^2(1-R_{HWi}(t),1-R_{HWj}(t))-C^3(1-R_{HW1}(t),1-R_{HW2}(t),1-R_{HW3}(t)) \tag{15}$$

其中，$R_{HW1}(t)$、$R_{HW2}(t)$、$R_{HW3}(t)$分别表示电源模块、微处理器和存储模块的可靠度，且 $R_{HW3}(t)$的计算表达式为：

$$R_{HW3}(t)=1-(1-R_{RAM}(t))-C^2(1-R_{Nor}(t),1-R_{Nand}(t))+C^2(C^2(1-R_{Nor}(t),1-R_{Nand}(t)),1-R_{RAM}(t)) \tag{16}$$

其中，$R_{RAM}(t)$、$R_{Nor}(t)$、$R_{Nand}(t)$分别表示 RAM、Nor Flash 和 Nand Flash 模块的可靠度函数。各种外围接口为并联相依关系，而接口数量依据具体应用有所差异，在此假设接口模块数为 n，则可得到 $R_{intM}(t)$为：

$$R_{intM}(t)=1-C^n(F_{hw1}(t),F_{hw2}(t),\cdots,F_{hwn}(t)) \tag{17}$$

其中，$F_{hwi}(t)$表示接口 i 的分布函数。

因此，系统硬件的可靠度的 Copula 模型由式(14)予以描述，其各个分项由式(16)和式(17)确定。

3.2.3　软硬件综合可靠性模型

由图 1 可知，ERCS 由软件和硬件两个部分协调实现实时控制功能，从而完成给定的任务。其软件和硬件不是单一的两个部分，软件子系统的运行需要硬件子系统提供物质平台，而硬件子系统又是在软件操作和指挥下实现实时控制，因此，ERCS 是由软件子系统和硬件子系统构成的串联相依系统。

由 Copula 函数和式(16)、式(17)，可得到 ERCS 系统的软硬件综合可靠性 Copula 模型为：

$$R_{SYS}(t)=1-(1-R_{SWr}(t))(1-R_{HWr}(t))+C^2(1-R_{SWr}(t),1-R_{HWr}(t)) \tag{18}$$

其中，$R_{SWr}(t)$，$R_{HWr}(t)$分别由式(13)、式(14)予以确定；C^2 为二维 Copula 函数，且具有唯一存在性。

在建立了式(18)的模型后，要选择合适的 Copula 来描述；因 Copula 的类型比较多，如椭球 Copula、阿基米德 Copula 和 FGM 族 Copula 等，不同的 Copula 具有不同的应用，所以依据参考文献[16]，选用 FGM 族 Copula 对式(18)进行分析。

由前面分析可知，ERCS 的硬件系统为串并联相关混合系统，其软件也是串并联相关混合系统，故整个 ERCS 为串并联相依系统。因此，由 FGM 族 Copula 理论[9,16]可得：

$$C^2(1-R_i(t),1-R_j(t))\cong C_m(1,1,\cdots,1-R_{i\atop i}(t),\cdots,1-R_{j\atop j}(t),1,\cdots,1)$$

$$C^3(1-R_i(t),1-R_j(t),1-R_k(t))\cong C_m(1,\cdots,1,1-R_{i\atop i}(t),\cdots,1-R_{j\atop j}(t),\cdots,1-R_{k\atop k}(t),1,\cdots,1)$$

$$\vdots$$

$$C^{m-1}(1-R_1(t),1-R_2(t),\cdots,1-R_x(t))\cong C_m(1-R_{1\atop 1}(t),\cdots,1-R_{2\atop 2}(t),\cdots,1-R_{x\atop x}(t),1,\cdots,1)$$

即利用 FGM 族 Copula 理论，将前面的模型中使用到的 Copula 函数，无论是二维、三维，还是 n 维的，都统一使用 m 元 Copula 函数予以描述。

由可靠度函数，可方便得到 ERCS 系统的软硬件综合可靠性的其他指标。因此，对给定的具体 ERCS 系统，利用式(18)可得到瞬态可靠度，进而得到系统的其他可靠性指标。

4　算例

文献[17]设计了嵌入式车站信号联锁控制器，从软硬件两方面进行了设计与分析，并对控制器的可靠性进行了定量计算，得到控制器可靠度为 0.9999768。因其可靠性分析与计算是采用 Markov 理论和方法进行的，现利用本文所建立的 ERCS 软/硬件综合可靠性模型，对其系统可靠性进行重新分析与计算。

控制器软件结构服从图 3 所示的体系结构。依据铁路站场信号联锁控制工艺特点和列车运行速度信号系统反应时间的要求，控制器必须在规定时间 $t_{STTG}=60$ms 内完成控制功能。控制器完成控制功能与软件、硬件都相关，即软件完成控制功能的规定时间为 t_{SWTG}，硬件完成控制功能的规定 t_{HWTG} 满足：

$$t_{SWTG}+t_{HWTG}\leqslant t_{STTG} \tag{19}$$

而控制器的控制功能需要许多软件模块和多个硬件功能块相互协调才能实现，则式(19)可表述为：

$$\sum_{i=1}^{n}t_{SWi}+\sum_{j=1}^{m}t_{HWj}\leqslant t_{SWTG}+t_{HWTG}\leqslant t_{STTG} \tag{20}$$

其中，n 表示软件模块的个数，m 表示硬件功能块的个数。

还需估算各个软件模块在最坏情况下的执行时间(the Worst Cases of the Execution Time，WCET)上限[23]，与各个模块的规定时间 t_{SWTGi} 进行比较，若所估算得到的 WCET 大于 t_{SWTGi}，则需进行重新设计和估算。控制器软件须在规定时间 $t_{SWTG}=40$ms 内执行完，进而实现系统的控制功能。控制器处理器主频为 206MHz，通过实验和计算得到如表 1 所列的数据，从而得到 $\sum t_{SWi}=16.9$ms，满足式(20)的要求。

表1 各模块预计和规定执行时间表(单位:μs)

模块	BSP	ERTOS	OSAP	DDP	FS	NP	GUI	RCAP
t_{SWi}	100	4000	100	100	100	2000	500	10000
WCET	25	500	100	50	50	250	250	500

若控制器的软件模块为同型模块,且服从式(9)的可靠度模型,则由式(9)计算得到软件模块(此处软件模块为不可再分的子模块)的可靠度为0.9999999;控制器软件的每个模块由多个子模块通过相依关系构成,因此可得到各个软件模块的相依可靠度,如表2所列。

表2 模块内子模块独立、相依可靠度表

功能模块	子模块数	可靠度	
		独立	相依
BSP	3	0.9999875	0.9999993
ERTOS	20	0.99985760	0.9998898
OSAP	2	0.99998578	0.9999998
DDP	9	0.99991457	0.9999984
FS	3	0.99997	0.9999988
NP	20	0.9998845	0.9998893
GUI	5	0.9999554	0.9999876
RCAP	40	0.9996049	0.9996478

将表2与式(13)结合进行计算,得到R_{SWr}和控制器软件运行10000小时的平均无故障时间(Mean Time To Failures, MTTF)分别为:

$$R_{SWr}(10000)=0.9999965$$

$$MTTF_{SWr}=\int_0^{3.6\times10^7} R_{SWr}(t)\mathrm{d}t=3.5999874\times10^7\,(\mathrm{s})$$

若控制器软件模块相互独立,则可计算得到$R_{SWrDULI}$和10000小时的$MTTF_{SWrDULI}$分别为:

$$R_{SWrDULI}(10000)=0.99935$$

$$MTTF_{SWrDULI}=3.59766\times10^7\,(\mathrm{s})$$

依据参考文献[13]和前面计算公式可得到控制器各个IP硬核运行10000小时的可靠度,如表3所列。

表3 控制器各IP硬核运行10000小时的可靠度

编号	IP硬核名称	可靠度	编号	IP硬核名称	可靠度
1	信号采集	0.99988	8	输出模块	0.99936
2	MCU控制	0.99987	9	比较模块	0.99888
3	时钟模块	0.99868	10	输入隔离模块	0.99975
4	存储模块	0.99864	11	输出隔离模块	0.99964
5	LED模块	0.99688	12	CAN总线控制	0.99754
6	电源模块	0.99836	13	CAN总线收发	0.99644
7	中断模块	0.99989	14	通信模块	0.99854

将表3数据与式(17)结合进行计算,可得到硬件IP硬核相依时的硬件可靠度R_{HWr}为:

$$R_{HWr}(10000)=0.9999241$$

同时可得到硬件相依时,10000小时的MTTF为:

$$MTTF_{HWr}=3.59972676\times10^7\,(\mathrm{s})$$

用式(18)的软硬件综合可靠性Copula模型对控制器软件、硬件可靠度$R_{SWr}(t)$和$R_{HWr}(t)$进行计算,即可得到在软硬件相依情况下的系统可靠度和运行10000小时的MTTF分别为:

$$R_{SYS}(10000)=0.9999973$$

$$MTTF_{SYS}=3.59999028\times10^7\,(\mathrm{s})$$

若控制器的软硬件相互独立,则可计算得到可靠度和MTTF分别为:

$$R_{SYSDULI}=0.9999768$$

$$MTTF_{SYSDULI}=3.59991648\times10^7\,(\mathrm{s})$$

通过计算控制器软硬件相依和独立的可靠度和MTTF可知,用Copula函数建立的可靠性模型能有效分析和计算ERCS系统的软硬件综合可靠性指标,且考虑ERCS软硬件相依性后,能更为有效地表征系统的可靠性。

结束语 主要论述了嵌入式实时控制系统的软硬件综合可靠性的Copula函数建模与分析,首先对ERCS目标系统进行抽象定义,然后对软件子模块的可靠度和硬件IP硬核的可靠度计算模型建立软件模块相依的Copula模型和硬件IP硬核的相依Copula模型,同时建立了软硬件相依的Copula模型;最后利用所建立的模型,对具体的ERCS系统进行可靠性指标的计算与分析。通过分析、计算结果可知,本文所建立的模型综合考虑了ERCS软硬件的相依性,对分析和计算ERCS的可靠性具有一定的实用价值。

参考文献

[1] 杨鹏飞,谭维康.等待系统软件/硬件可靠性模型[J].计算机学报,1989(7):516-524

[2] 于敏,何正友,钱清泉.基于Markov过程的硬/软件综合系统可靠性分析[J].电子学报,2010,38(2):473-479

[3] 吴祥,张靖,等.基于软硬件特性的计算机系统的可靠性分析[J].中国民航飞行学院学报,2006,17(1):33-36

[4] Friedman M A, Tran P P. Reliability Techniques for Combined Hardware/Software Systems[C]// Proc, IEEE RAMS' 1992 Reliability and Maintainability Symposium. 1992:290-293

[5] Vemuri K K, Dugan J B. Reliability Analysis of Complex Hardware-Software Systems[C]// Proc, IEEE RAMS' 1999 Reliability and Maintainability Symposium. 1999:178-182

[6] Teng Xiao-lin, Pham H, et al. Reliability Modeling of Hardware and Software Interactions, and Its Applications[J]. IEEE Transactions on Reliability, 2006, 55(4):571-577

[7] 吴娟. Copula理论与相关性分析[D].武汉:华中科技大学,2009:2-66

[8] 易文德,卫贵武.基于Copula函数的相依部件表决系统的可靠性研究[J].西南师范大学学报:自然科学版,2007,32(6):52-55

[9] Kotz S, Lai C D, Xie M. On the effect of redundancy for systems with dependent components[J]. IIE Transactions, 2003, 35(12):1103-1110

[10] Noh Y, Choi K K, Du Liu. Reliability-based design optimization of problems with correlated input variables using a Gaussian Copula[J]. Struct Multidisc Optim, 2009, 38:1-16

[11] Nelsem R B. An introduction to Copulas [M]. New York: Springer Press, 2005

[12] 郭荣佐,黄君,王霖.基于π网的嵌入式系统软硬件划分方法[J].计算机应用,2012,32(3):855-860

[13] 郭荣佐,黄君.嵌入式实时控制系统硬件可靠性及应用研究[J].电子技术应用,2012,38(5):11-15

[14] 胡仁胜.实时控制软件系统的可靠性分析[J].华南师范大学学报:自然科学版,2001(1):103-107

[15] 郭荣佐,黄君.嵌入式实时控制系统软件可靠性建模与应用[J].计算机应用,2013,33(2):575-578

[16] 钟波,孙永波.基于Copula的部件相依并联系统可靠性分析[J].数理统计与管理,2011,30(2):363-369

[17] 刘丽萍,郭荣佐,王霖.嵌入式车站信号联锁控制器设计[J].计算机仿真,2010,27(6):314-317

[18] 吴国伟,姚琳.一种嵌入式软件WCET估计新方法[J].大连理工大学学报,2004,44(6):912-915