考虑传播过程的应急网络控制系统故障恢复

黄雄峰[1], 王 錫[1], 朱严严[2], 黄 双[3], 张宇娇[1†]

(1. 合肥工业大学 电气与自动化工程学院, 安徽 合肥 230009; 2. 中车株洲时代电气股份有限公司, 湖南 株洲 412001;
3. 武汉第二船舶设计研究所, 湖北 武汉 430010)

摘要: 紧急情况下, 应急网络控制系统为人员提供远程控制能力, 但系统仍存在一定故障率, 且故障影响会利用系统灵活传输机制快速扩散, 因此研究如何在故障快速扩散的情况下对系统实施故障控制, 对保证系统安全运行具有重要意义. 本文提出考虑传播过程的应急网络控制系统故障恢复策略. 首先, 基于复杂网络模型建立故障传播模型, 定义传播路径上的故障强度, 将分析故障信息关键传播过程转化为查找系统最大可能传播路径的问题, 进而在连接边的故障传播属性乘积大于终止条件时, 找到最大概率故障传播路径, 有针对地布置故障检测点; 再根据检测到的故障形式及检测点位置生成故障恢复策略库, 结合系统可调度性和故障恢复效果, 确定最优故障恢复策略. 最后, 以舰船应急火炮控制系统构建案例, 验证方法可行性, 并设置多节点故障, 验证算法鲁棒性, 仿真结果表明, 在不同故障情形下均能制定最优故障恢复策略.

关键词: 网络控制系统; 故障传播分析; 恢复; 策略优化

引用格式: 黄雄峰, 王錫, 朱严严, 等. 考虑传播过程的应急网络控制系统故障恢复. 控制理论与应用, 2024, 41(5): 875 – 884

DOI: 10.7641/CTA.2023.20765

Fault recovery of emergency networked control system considering propagation process

HUANG Xiong-feng[1], WANG Yang[1], ZHU Yan-yan[2], HUANG Shuang[3], ZHANG Yu-jiao[1†]

(1. School of Electrical Engineering and Automation, Hefei University of Technology, Hefei Anhui 230009, China;
2. Zhuzhou CRRC Times Electric Co., Ltd, Zhuzhou Hunan 412001, China;
3. Wuhan Second Ship Design and Research Institute, Wuhan Hubei 430010, China)

Abstract: In case of emergency, the emergency network control system provides the remote control ability for the personnel, but the system still has a certain failure rate, and the influence of the failure will spread rapidly by using the flexible transmission mechanism of the system, therefore, it is of great significance to study how to implement fault control under the condition of rapid fault diffusion to ensure the safe operation of the system. In this paper, a fault recovery strategy for emergency networked control systems is proposed, which considers the process of fault propagation. Firstly, a fault propagation model is established based on the complex network model, and the fault intensity on the propagation path is defined, which transforms the analysis of the key propagation process of fault information into the problem of finding the maximum possible propagation path of the system, then, when the product of fault propagation attributes is larger than the termination condition, the most probable fault propagation path is found, and the fault detection points are arranged accordingly. Then, according to the detected fault and the location of the detection point, the fault recovery strategy library is generated, and the optimal fault recovery strategy is determined by combining the schedulability of the system and the effect of fault recovery. Finally, a case is built to verify the feasibility of the method and set up a multi-node fault to verify the robustness of the algorithm, the optimal fault recovery strategy can be formulated under different fault conditions.

Key words: networked control system; fault propagation analysis; recovery; strategy optimization

Citation: HUANG Xiongfeng, WANG Yang, ZHU Yanyan, et al. Fault recovery of emergency networked control system considering propagation process. *Control Theory & Applications*, 2024, 41(5): 875 – 884

收稿日期: 2022−08−29; 录用日期: 2023−04−11.

†通信作者. E-mail: zhangyujiao@hfut.edu.cn; Tel.: +86 13329255852.

本文责任编委: 夏元清.

国家自然科学基金项目(52077048), 中央高校基本科研业务费专项资金项目(JZ2020HGQA0176)资助.

Supported by the National Natural Science Foundation of China (52077048) and the Fundamental Research Funds for the Central Universities (JZ2020HGQA0176).

1 引言

随着通信和控制技术的发展, 网络控制系统被广泛应用于重大公共安全事件、重大自然灾害及军事活动等场所, 为人员提供远程控制能力. 而紧急情景下通信基础设施易遭破坏, 甚至可能没有预先设置, 不利于系统搭建, 故常采用具有高抗毁性、高灵活度的无线自组织网络搭建应急网络控制系统[1]. 如, 在海面上, 舰队利用自组织网络实现舰船编队任务[2]; 在偏远地区, 基于无人机集群建立通信网, 为失踪人员提供通信或地理标记[3]. 这种可快速组建的网络控制系统, 其通信网络中任意两节点可利用多个中间设备的转发实现数据传输, 完成协调控制. 但系统复杂的工作环境及计算、存储资源受限等因素使设备容易故障, 同时, 故障造成的影响会利用系统的高灵活传输特性快速扩散, 最终影响系统决策, 若不及时控制, 可能引发重大安全事故. 这种由微小故障造成控制系统崩溃的案例时有发生[4], 如: 2018年发生的印尼狮航空难事件, 就是由飞机左侧仰角传感器故障使控制系统做出错误控制措施而引发的重大航空安全事件. 因此, 如何在故障快速扩散情况下对系统进行故障恢复, 控制故障传播影响, 对于提高系统可靠性, 拓展应急网络控制系统在关键领域应用具有重要意义[5].

控制系统一般采用冗余故障恢复方法, 包括硬件冗余、软件冗余、时间冗余及信息冗余. 硬件冗余是通过备份多个相同功能的硬件设备, 当主设备故障时, 及时启用备份进行替换[6], 文献[7]通过双重冗余方式提高机载嵌入式系统可靠性, 同时结合交叉通信数据链路使系统满足实时性需求; 软件冗余指通过执行多套相同功能的软件来提高系统可靠性[8–9], 文献[10]利用多核电子控制单元冗余, 通过提供复制线程级的程序设计为汽车控制系统提供容错, 实现错误检测和纠正; 时间冗余用时间换取冗余, 采用指令的重复执行或程序重试来消除暂时性故障影响[11], 文献[12]在实时系统中插入若干个检测点, 通过将任务回卷到距离错误时刻最近检测点重新执行, 提高了系统可靠性; 信息冗余通过增加额外的信息位数来对出错的信息进行检测和纠正, 主要包括在数据传输过程中采用的奇偶校验技术和校验(sum check), 以及具有错误纠正能力的海明码等[13–14].

尽管对于故障恢复方法已有诸多研究, 但这些方法多是考虑当系统节点故障时, 在节点处提供故障恢复手段, 而在应急网络控制系统中, 故障影响会利用系统高灵活传输特性快速扩散到目标节点, 而在不同部位检测到故障所采取的故障恢复措施也是不同的. 因此, 本文提出考虑传播的应急网络控制系统故障恢复, 利用故障传播分析方法分析故障影响扩散过程, 并以此布置故障检测点检测故障, 针对检测到的故障形式, 对策略库中的恢复策略进行比较, 选择最优恢复策略, 保证故障在传播过程中得以恢复, 以保障应急网络控制系统可靠性.

2 应急网络控制系统故障控制架构

2.1 系统结构及特性

应急网络控制系统的应用延长了军事舰艇上设备可用性, 当舰船受到攻击时, 仍可为指挥人员提供应急远程指挥能力. 其系统结构如图1所示.

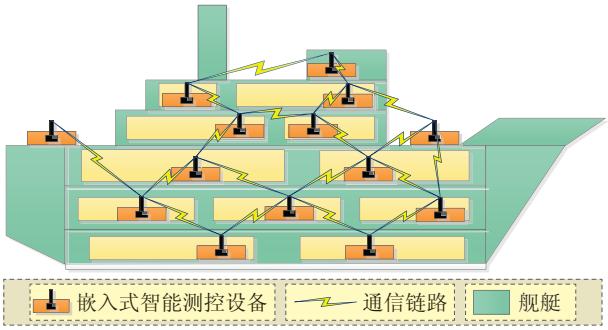


图 1 舰船网络控制系统基本结构

Fig. 1 Basic structure of ship network control system

舰船网络控制系统主要分为无线自组织通信网络和嵌入式智能测控设备, 这使系统具有如下特征: 1) 通信网络自组织特性, 无需基础网络设施, 可随时随地快速搭建通信网络, 完成设备间数据传输; 2) 数据多跳传输, 系统中各节点既是主机又是路由器, 两节点可通过多中间节点转发实现数据传输; 3) 两节点间存在多条路由路径; 4) 设备具有多任务特征, 既要执行本地任务, 又要协同其他设备完成控制任务; 5) 系统实时性要求, 各设备中控制任务输出的正确性与输出数值的正确性及输出产生的时间密不可分; 6) 设备资源受限, 嵌入式设备受能耗、体积、重量等因素限制, 其计算、存储、能量资源受限.

2.2 系统故障分类

系统中常见故障基于时效性分为永久故障和瞬时故障, 永久故障指硬件或软件发生的不能自愈而要人工干预才能恢复功能的故障; 瞬时故障指硬件或软件发生的可恢复性故障, 这种故障在发生后可通过适当的恢复措施实现自恢复. 数据表明控制系统中瞬时故障比永久故障发生的概率要高的多, 且网络控制系统常面临高电磁、高温、高湿等因素的干扰, 这种现象更为明显. 此外, 基于故障产生速度, 又可分为突发性故障和渐进性故障. 突发性故障指故障在产生之前没有任何征兆, 设备在极短时间内突然故障; 渐进性故障指设备工作过程中, 逐渐逼近其使用寿命时渐渐显现出的故障. 本文主要考虑突发性的瞬时故障对系统造成的影响, 进而制定故障恢复策略.

2.3 系统故障控制架构

突发性瞬时故障对系统影响主要表现在对任务输出数据的影响上. 为控制该类故障影响的快速扩散,

提出考虑故障传播的故障恢复策略, 制定及时合理的故障恢复措施. 图2为系统故障控制架构, 分为: 系统故障传播模型建立、故障传播路径分析、故障恢复策略库制定、故障恢复策略优化、故障控制执行.

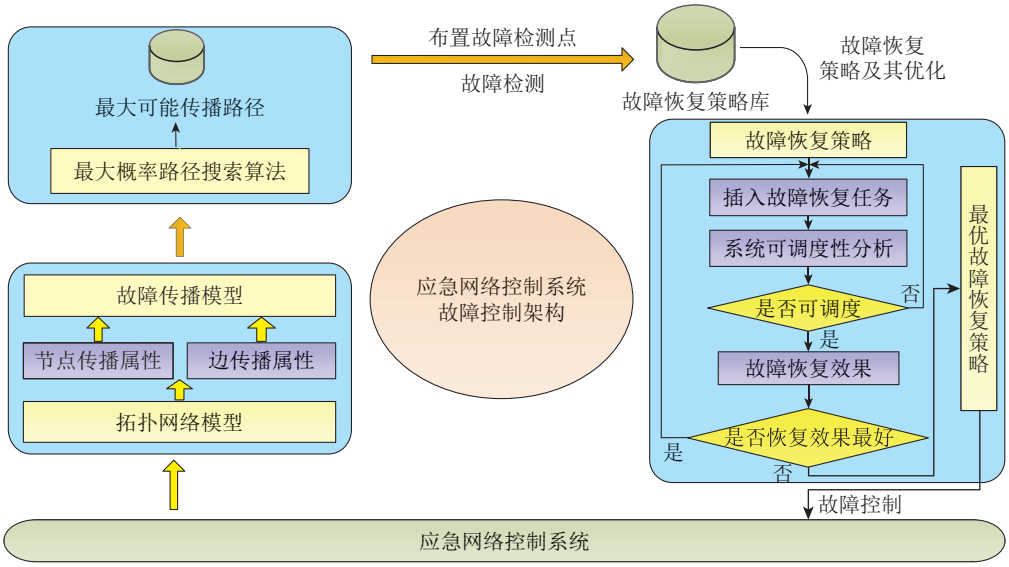


图 2　系统故障控制架构

Fig. 2　Fault control architecture of system

1) 系统故障传播模型建立: 结合系统拓扑网络建立复杂网络模型, 定义节点及连接边的故障传播属性, 得到故障传播模型; 2) 故障传播路径分析: 在每个连接边的故障传播属性乘积大于10^{-8}的终止条件下, 利用最大概率路径搜索算法得到系统两节点间关键传播路径[15]; 3) 故障恢复策略库制定: 针对突发性瞬时故障, 本文基于软件和时间冗余的故障恢复方法, 结合检测点选取恢复点, 制定故障恢复策略; 4) 故障恢复策略优化: 同一种故障情形下可预先制定多个恢复策略, 形成策略库, 结合系统任务可调度性及故障恢复效果, 选出最优策略; 5) 故障控制执行: 将最优策略应用在系统中, 故障发生时, 执行策略, 控制故障影响.

3　应急网络控制系统故障传播及恢复策略

应急网络控制系统控制任务输出的正确性跟计算的数值准确性和控制策略执行的实时性有关. 当对采取故障恢复策略时, 势必增加系统开销, 而不同策略对系统实时性影响不同, 有些可能导致系统任务不可调度. 故为能可靠执行恢复策略, 需建立系统任务调度模型, 研究不同故障恢复策略对系统可调度性的影响, 为选择最优的可行策略奠定基础.

3.1　系统任务调度模型

网络控制系统中, 各实时任务都要求在规定的时间期限内完成. 作为分布式实时系统, 其任务更复杂, 频繁地拥有要在各节点或组件上执行的子任务, 这种需要多个系统节点中的相关子模块, 按照明显的先后顺序协同运行, 并且需要在一个给定开始和结束时间内完成的系统任务, 被称为端到端实时任务, 而这个给定的时间段, 称为端到端任务的截止时间.

系统中存在某一端到端任务T, 其由若干子任务组成, 各子任务依次分布在嵌入式设备序列$\{P_1,\cdots,P_j,\cdots,P_i\}$上, 假设各设备的处理能力相同, 端到端任务与本地任务之间相互独立. 这时若分布在P_1上的子任务为$\{T_{1,1},\cdots,T_{1,h}\}$, P_j上的为$\{T_{j,k},\cdots,T_{j,l}\}$, P_i上的为$\{T_{i,m},\cdots,T_{i,n}\}$. 则整个端到端任务$T$是由$T_{1,1},\cdots,T_{j,k},\cdots,T_{i,n}$组成的, 其中: $i\geqslant j\geqslant 1, n\geqslant m\geqslant l\geqslant k\geqslant h\geqslant 1$.

每个子任务$T_{j,k}$需分配合适的相对截止时间$d_{j,k}$, 以及给定每个子任务的释放时间$\phi_{j,k}$, 且$\phi_{j,k}=\phi_{j,k-1}+d_{j,k-1}$. 保证端到端任务可靠执行

$$\sum_{j=1}^{i}\sum_{k=1}^{n}d_{j,k}\leqslant d, \tag{1}$$

其中: $i\geqslant j\geqslant 1, n\geqslant k\geqslant 1$. 采用等分剩余松弛时间法为每个子任务分配相对截止时间[16]. 而子任务序列的总松弛时间

$$s=d-e_{1,1}-\cdots-e_{j,l}-\cdots e_{i,m}-\cdots e_{i,n}. \tag{2}$$

平分到各子任务上的松弛时间$s_{j,k}=s/n$, 则子任务$T_{j,k}$的相对截止时间为$d_{j,k}=e_{j,k}+s_{j,k}$.

3.2　应急网络控制系统故障恢复策略生成

3.2.1　应急网络控制系统故障传播分析

针对突发性瞬时故障, 若在所有节点中部署故障检测任务, 将严重消耗系统资源, 同时会影响各节点中实时任务的执行. 若能找出系统中故障影响的主要传播路径, 就可有针对地部署检测点, 进行故障检测

和恢复, 从而既减小系统资源消耗, 降低对系统任务实时性的影响, 又可有效控制故障影响范围[17].

构建系统网络模型$G(V,E)$, 嵌入式设备抽象为网络节点, 节点组成集合$V=\{v_1,v_2,\cdots,v_n\}$; 设备间的通信链路抽象为连接边, 连接边集合$E=\{(v_i,v_j)\mid v_i\in V,v_j\in V\}$. 假设各节点通信范围相同. 由于各设备都具有中继能力, 故在两节点间的信息传递是双向的, 定义邻接矩阵A为

$$A=\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}. \tag{3}$$

当$a_{i,j}=1$, $e_{i,j}$存在; 否则, 不存在. 为衡量节点以及连接边对故障数据传播起到的促进作用大小, 定义了节点及连接边的传播属性$P(v_i)$, $P(e_{i,j})$, 以反映故障沿节点v_i和连接边$e_{i,j}$进行传播的强度大小.

$$P(v_i)=\exp\frac{d_i}{\sum\limits_{j=1}^{n}d_j}, \tag{4}$$

$$P(e_{ij})=\exp(-\frac{d_{ij}}{r})\times\frac{b_{ij}}{\sum b_{ij}}. \tag{5}$$

其中: d_i为节点v_i的出度, 指从该节点指向其他节点的有向边数目; r为节点通信半径; $d_{i,j}$为节点间欧式距离; $b_{i,j}$为边介数, 在复杂网络理论中表示网络中所有最短路径中经过该边的路径的数目占最短路径总数的比例[18]. 由此结合系统复杂网络模型得到系统故障传播模型, 如图3所示.

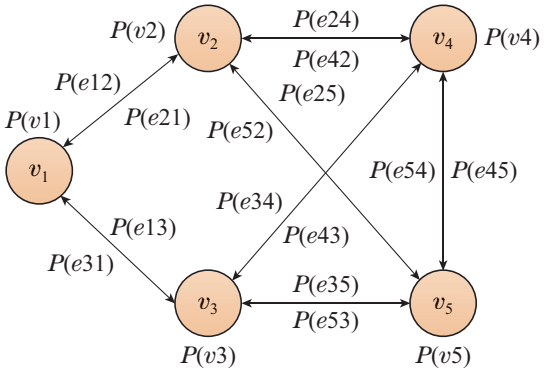


图 3 5节点的系统故障传播模型

Fig. 3 5-node system fault propagation model

故障沿最小代价传播路径到达目标节点, 定义故障在传播路径上的传播强度, 传播强度越大, 代价越小. 若节点v_i和节点v_j存在一条传播路径$I_{i,j}=e_{i,m},\cdots,e_{n,j}$, 则故障在路径上的故障传播强度为

$$I_{ij}=P(v_i)\times P(e_{im})\times\cdots\times P(e_{nj})\times P(v_j). \tag{6}$$

通常两点间路径跳数越少, 故障传播速度越快, 则作为本文重点关注的系统中故障影响从源节点传播至目标节点的主要传播过程, 可转变为找出两点间传播最快的最大概率路径, 即为

$$\begin{cases}\max\{I_{ij}^{k}(1),\cdots,I_{ij}^{k}(m)\},\\ k_{\min},\end{cases}\quad m=1,2,\cdots, \tag{7}$$

式中$I_{i,j}^{k}(m)$代表第m条经过k跳转发使得故障信息从节点v_i到v_j的路径上的故障传播强度. 由此将分析系统中故障信息的关键传播过程转化为了在一定约束条件下查找故障最大可能传播路径的问题, 进而利用最大概率路径搜索算法可得到两节点间的最大可能传播过程, 从而为检测点的部署提供理论依据.

3.2.2 故障恢复策略生成

故障恢复策略的生成指根据检测点检测的故障形式, 选取合适的恢复点并利用已有的故障恢复方法生成若干动作, 以实现故障恢复. 突发性瞬时故障多是使系统的任务输出数据偏离真实值, 从而影响系统的控制效果. 而数据的类型不同所产生的故障形式就不同, 进而所采取的恢复策略也不同, 具体如图4所示.

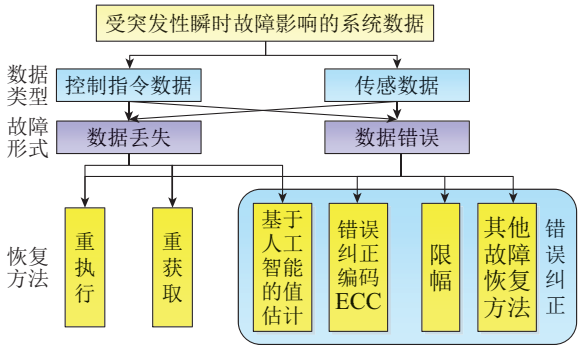


图 4 故障恢复方法

Fig. 4 Fault recovery method

图4中, 重执行指将相关变量保存在所选的故障检测点上, 当一检测点检测到故障发生时, 将任务回滚到上一检测点处, 重新执行相关任务, 进行故障恢复. 数据重获取指当检测点检测到数据信息丢失, 通过“重传”方式重新获得数据信息. 错误纠正是指利用编码算法对传输过程中引起的数据逻辑单元变化造成的错误数据值进行纠正, 或对超出阈值的数据进行限幅, 或利用历史数据基于神经网络等得到该时刻的估计值, 以弥补数据丢失或数据错误等.

3.3 系统故障恢复策略优化算法

针对某一故障情形, 生成了故障恢复策略库, 但实际执行时, 采用一种即可实现故障控制, 故考虑从系统可调度性及故障恢复效果两方面出发, 选择最优故障恢复策略, 实现故障控制. 这里把从故障恢复策略库中选择最优故障恢复策略的过程, 称为策略优化.

3.3.1 故障恢复任务插入模型

故障会影响端到端任务T中某一子任务的执行, 故需要在原子任务序列基础上插入故障恢复任务. 当

任务T中有新任务插入时, 为保证新子任务序列调度, 就需要对剩余子任务重新分配相对截止时间.

由第3.1节可知, 假设在子任务$T_{j,k}$后插入故障恢复任务$T'_{j,k}$, 则剩余子任务序列变为$T'_{j,k}, \cdots, T_{j,l}, \cdots, T_{i,m}, \cdots, T_{i,n}$, 此时剩余端到端截止时间也发生变化, 变为

$$d' = d - d_{1,1} - \cdots - d_{1,h} - \cdots - d_{j,k}, \tag{8}$$

剩余子任务序列的总松弛时间l'为

$$l' = d' - e'_{j,k} - \cdots - e_{j,l} - \cdots - e_{i,n}, \tag{9}$$

平分到剩余子任务$T_{j,l}$上的松弛时间为

$$l'_{j,l} = \frac{l'}{n-k+1} = \frac{d' - e'_{j,k} - \cdots - e_{i,m} - \cdots - e_{i,n}}{n-k+1}, \tag{10}$$

则剩余各子任务的相对截止时间发生变化, 如: 子任务$T_{j,l}$的相对截止期变为$d'_{j,l} = e_{j,l} + l'_{j,l}$.

3.3.2　故障恢复策略优化算法实现

端到端任务T的各子任务分布在不同嵌入式设备中, 且和设备中其他任务按可抢占最早截止期限优先(earliest deadline first, EDF)调度算法完成独立调度, 所以只要保证插入故障恢复任务后, 各设备中实时任务仍可调度, 整个系统就是可调度的.

文献[19]给出了不同截止期的任务基于可抢占的EDF调度的可调度性分析指标, 但不适用于各子任务截止时间都小于任务周期且同一端到端任务中的多个子任务可能分布在同一设备上的应急网络控制系统. 文献[20]给出了一种基于EDF调度策略的端到端实时系统可调度性分析算法, 其算法流程如图5.

嵌入式设备中包括各端到端任务的子任务及其本地任务, 其中, 本地任务可作为单独的端到端任务, 即该端到端任务的目标节点与源节点相同且只有一个子任务. 则可以用上述算法对系统进行可调度分析.

同一故障情形存在多种恢复策略, 若其中有多个策略都满足系统可调度条件, 这时可进一步对比故障恢复效果. 即将控制任务的理想输出同故障恢复之后的实际输出之间的差值error, 作为进一步的优化评估指标, 而差值最小的策略为最优恢复策略, 如下式:

$$\mathrm{Error}(\tau)_{\min} = \left|\mathrm{Output}_{\mathrm{g}} - \mathrm{Output}_{\tau\mathrm{r}}\right|_{\min}. \tag{11}$$

经两步优化选出最优的故障恢复策略, 既保证了恢复策略的可实施性, 又保证了恢复策略的恢复效果, 算法流程如图6.

4　案例分析

4.1　系统建模

舰载火炮控制系统是舰船的重要组成部分, 在战场上舰船可能受到敌方攻击导致原通信设施损坏, 紧急情况下, 可利用船上执行特定功能的嵌入式设备组成临时通信网络, 雷达设备可通过此无线多跳网络将测得的目标方位角信息传输到火炮控制台, 火炮控制台解算出目标方位角数据后, 控制火炮跟踪目标.

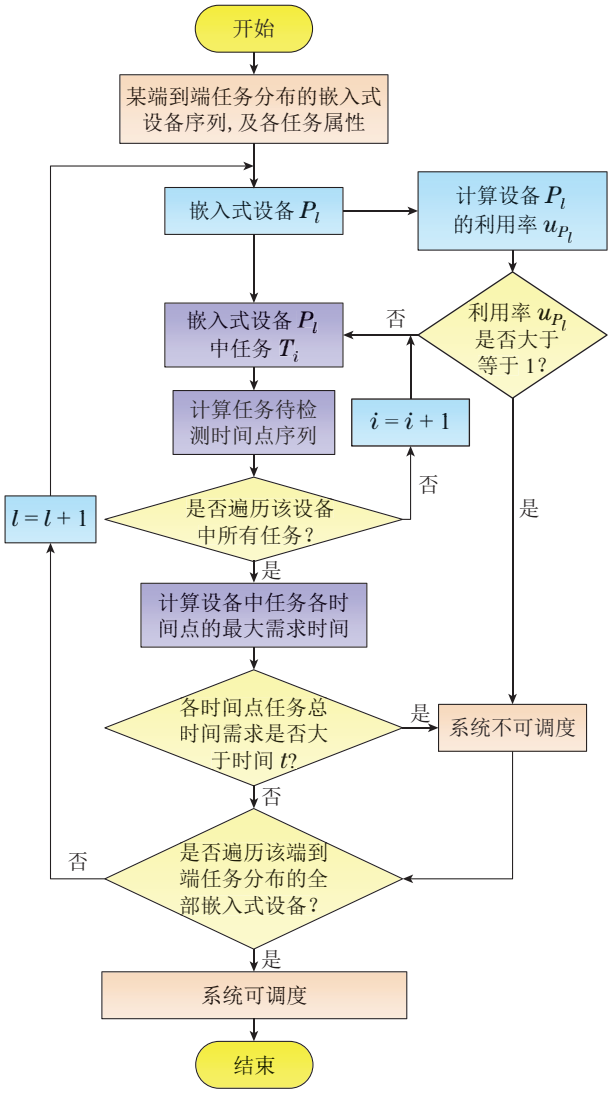


图 5　系统可调度性分析算法流程

Fig. 5　Flow chart of schedulability analysis algorithm

图7为系统网络拓扑图, 设备1为雷达设备, 设备14为火炮控制台, 设备1采集到的方位角数据通过多跳网络传输到设备14, 设备14解算出方位角后控制火炮瞄准. 系统中每台嵌入式测控设备的通信半径均为$r = 60$ m, 表1为存在通信链路的两节点间的欧式距离(m). 设备14处随动控制系统的状态空间方程为

$$\begin{cases} \dot{x} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -364.5 & -200 & -45 \end{bmatrix} x + \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} u, \\ y = [364.5 \ \ 0 \ \ 0] x. \end{cases} \tag{12}$$

系统中各嵌入式设备的任务可分为: 传感任务τ_{s}、执行任务τ_{a}、接收任务τ_{g}、本地数据传输任务τ_{t}、转发任务τ_{z}、安全检测任务τ_{m}和时钟任务τ_{n}. 各实时任务

按可抢占式EDF调度算法进行调度. 其中, 传感任务、执行任务、安全检测任务和时钟任务都为周期性任务.

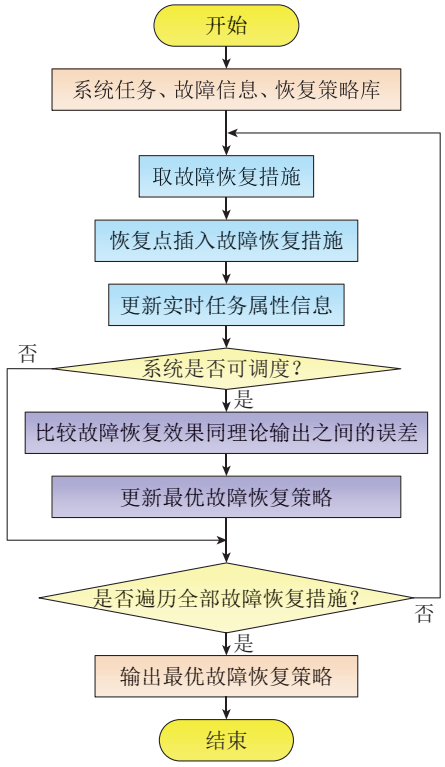


图 6 故障恢复策略优化算法流程

Fig. 6 Fault recovery strategy optimization algorithm flow

4.2 故障设置及故障恢复策略的制定

根据系统拓扑结构, 由故障传播分析可知, 若采集的方位角数据若受到故障影响, 故障数据最可能沿着设备4、设备9、设备8传播至设备14(火炮控制设备)处, 其中, 数据源为设备1(雷达设备), 故在这几个设备中部署故障检测点. 此时, 传播路径上各节点中的实时任务集和任务属性如表2所示.

远程数据传输任务T由子任务序列$\{\tau_{s,1}, \tau_{j,1}, \tau_{t,1}, \tau_{g,4}, \tau_{j,2}, \tau_{z,4}, \tau_{g,9}, \tau_{j,3}, \tau_{z,9}, \tau_{g,8}, \tau_{j,4}, \tau_{z,8}, \tau_{g,5}\}$组成. 整个端到端任务周期为0.2 s, 各节点中任务的属性用$\tau(e,p,d)$来描述, 其中: e为任务最大执行时间; p为任务周期; d为相对截止时间, 时间单位均为ms, 初始时均可正常调度.

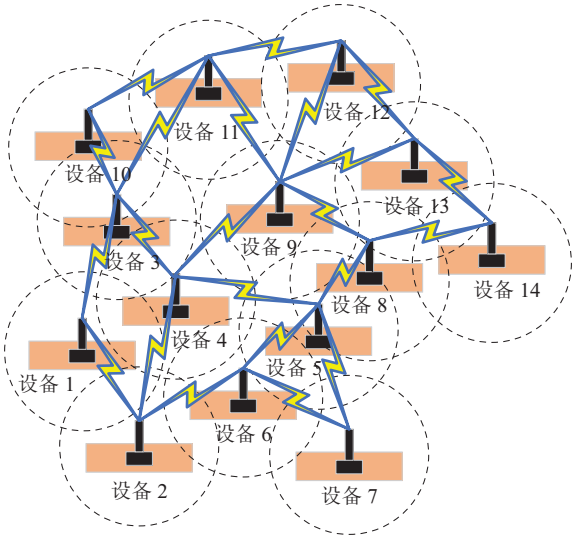


图 7 火炮控制系统网络拓扑图

Fig. 7 Network topology of artillery control system

表 1 两节点间欧式距离

Table 1 Euclidean distance between two nodes

链路	欧氏距离	链路	欧氏距离	链路	欧氏距离
(1,2)	54	(4,9)	58	(8,14)	56
(1,3)	57	(5,6)	30	(9,11)	57
(1,4)	58	(5,8)	57	(9,12)	55
(2,4)	55	(5,9)	31	(9,13)	57
(2,6)	50	(6,7)	57	(10,11)	57
(3,4)	45	(7,8)	50	(11,12)	50
(3,10)	59	(8,9)	59	(12,13)	40
(3,11)	57	(8,13)	55	(13,14)	52
(4,5)	55	–	–	–	–

4.2.1 雷达设备传感模块故障

若雷达设备传感器模块发生突发性瞬时故障, 导致得到的目标方位角数据错误, 即设备1中传感任务输出数据偏离真实数据. 如果故障数据不及时恢复而直接作用于火炮控制器, 则系统控制输出如图8所示.

表 2 各设备中任务集以及任务属性描述

Table 2 Task set and task attribute description in each device

	设备1	设备4	设备9	设备8	设备14
传感任务	$\tau_{s1}(4,200,12)$	$\tau_{s4}(8,150,19)$	$\tau_{s9}(7,100,20)$	$\tau_{s8}(3,100,11)$	$\tau_{s14}(5,200,25)$
执行任务	$\tau_{a1}(10,100,100)$	$\tau_{a4}(5,50,50)$	$\tau_{a9}(10,150,150)$	$\tau_{a8}(10,100,100)$	$\tau_{a14}(15,100,100)$
接收任务	$\tau_{g1}(7,100,16)$	$\tau_{g4}(9,200,17)$	$\tau_{g9}(9,200,17)$	$\tau_{g8}(9,200,17)$	$\tau_{g14}(9,200,17)$
故障检测任务	$\tau_{j1}(5,200,13)$	$\tau_{j4}(5,200,13)$	$\tau_{j9}(5,200,13)$	$\tau_{j8}(5,200,13)$	–
转发任务	$\tau_{z1}(7,100,16)$	$\tau_{z4}(9,200,17)$	$\tau_{z9}(9,200,17)$	$\tau_{z8}(9,200,17)$	–
传输任务	$\tau_{t1}(9,200,17)$	$\tau_{t4}(10,150,21)$	$\tau_{t9}(12,100,25)$	$\tau_{t8}(5,100,13)$	$\tau_{t14}(10,200,30)$
安全监测任务	$\tau_{m1}(10,200,200)$	$\tau_{m4}(10,150,150)$	$\tau_{m9}(10,170,170)$	$\tau_{m8}(10,200,200)$	$\tau_{m14}(10,200,200)$
时钟任务	$\tau_{n1}(5,100,100)$	$\tau_{n4}(5,150,150)$	$\tau_{n9}(5,80,80)$	$\tau_{n8}(5,100,100)$	$\tau_{n14}(5,100,100)$

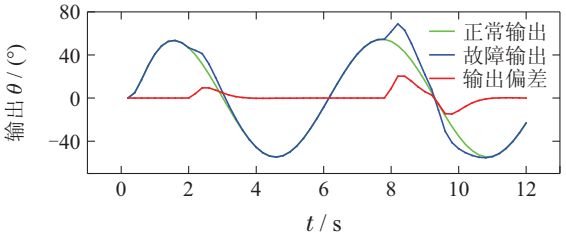


图 8　故障作用下系统输出及偏差

Fig. 8　System output and deviation under the action of fault

为此, 这里可以考虑采用以下3种故障恢复策略:

策略 1　从设备1传感任务重执行, 记作τ_{h1}.

策略 2　在设备1或后续设备中利用历史数据的值估计方法, 得到故障时间内方位角估计值, 记作τ_{h2}, 此任务执行时间为10 ms.

策略 3　在设备1或后续设备中利用限幅的方法, 当检数据异常时, 大于零, 限幅为45, 小于零, 限幅为−45, 以抑制故障影响, 记作τ_{h3}, 此任务执行时间为4 ms.

方位角数据传输为周期任务, 只须确保在任务截止时间之前执行完恢复任务即可, 故本文只将可调度性及故障恢复效果作为故障恢复策略评价标准, 保证恢复任务可在周期时间内完成即可.

策略1在设备1中插入故障恢复任务τ_{h1}, 策略2采用Elman神经网络基于历史数据对时间序列进行预测, 得到错误数据估计值, 即在设备1中故障检测任务后插入故障恢复任务τ_{h2}, 策略3在设备1 利用限幅的方法进行故障恢复, 需在设备1中插入故障任务τ_{h3}.

下面分析不同恢复策略对系统可调度性的影响.

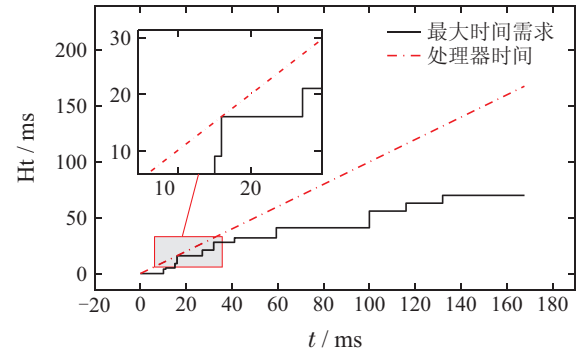
由图9可知, 在所提出的3种恢复策略中, 采用策略1和策略3后各设备中任务调度最大时间需求Ht仍小于系统时间, 系统可调度; 而采用策略2后设备1中任务调度最大时间需求存在大于系统时间的情况, 系统不可调度. 故策略1和策略3可行, 策略2不可行.

可考虑在设备4处利用值估计方法进行故障恢复. 在设备4中插入恢复任务τ_{h2}后进行可调度性分析.

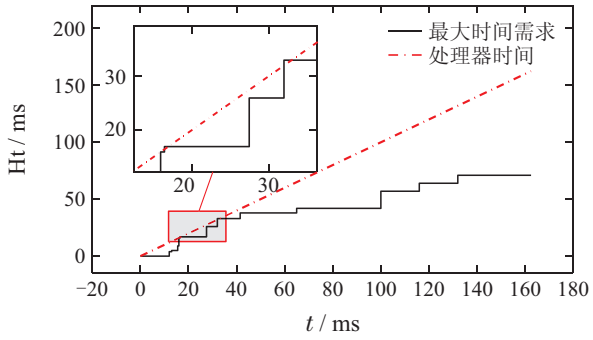
由图10可知, 设备4中各实时任务仍可以正常调度, 同样由可调度分析算法可得其他几个设备中任务也可正常调度, 即在设备4处进行值估计是可行的.

3种恢复策略修正的方位角数据传输到火炮随动系统中, 最后得到的控制效果如图11所示. 可调度分析和故障恢复效果都表示3种策略是可行的, 生成的策略库有效. 但3种故障恢复策略修正后的数据作用于火炮控制器得到的控制效果是不同的.

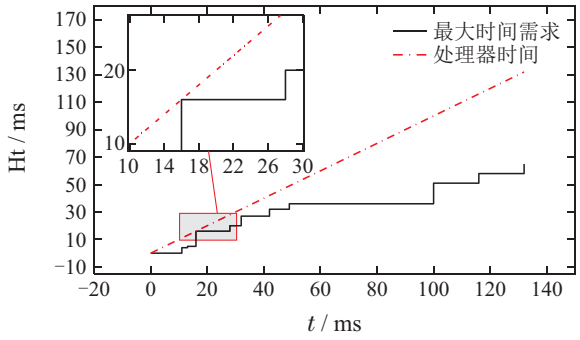
图11(b)显示不同故障恢复策略执行后控制系统的输出偏差, 策略1可重新获得该时刻的真实数据, 该故障恢复策略执行之后, 火炮控制系统的控制输出避免了受到突发性瞬时故障的影响, 系统输出偏差始终为最小. 故所提出的3种故障恢复策略中, 在设备1中重执行传感任务的方法控制故障影响是最优的.



(a) 策略1



(b) 策略2



(c) 策略3

图 9　插入故障恢复任务后设备1中任务最大时间需求

Fig. 9　Task time requirement in device 1 after fault recovery task is inserted

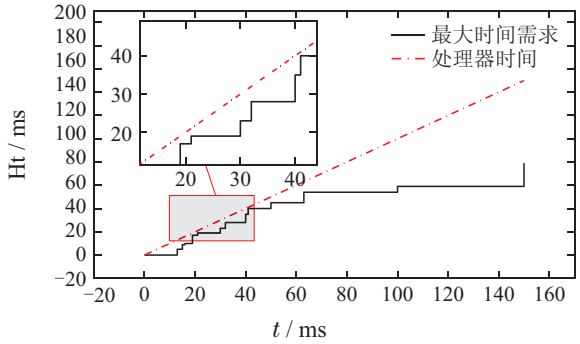
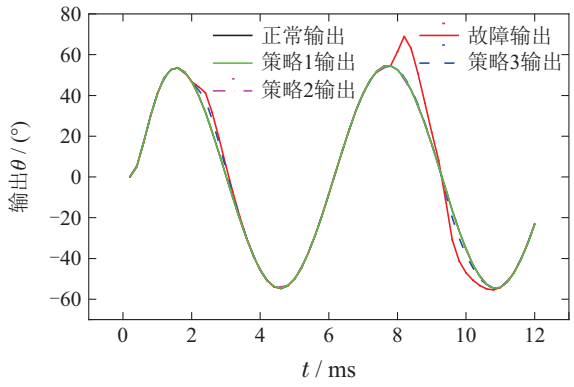
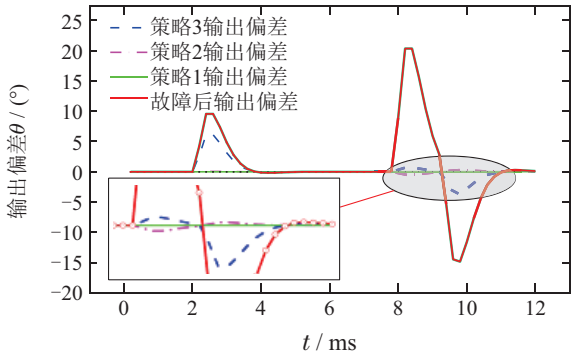


图 10　插入τ_{h2}后设备4中任务最大时间需求

Fig. 10　Task time requirement in device 4 after τ_{h2} is inserted



(a) 故障恢复后系统输出



(b) 输出偏差

图 11 不同故障恢复策略故障恢复后系统输出及偏差

Fig. 11 System output after fault recovery with different fault recovery strategies and deviation

4.2.2 雷达设备故障及中继节点通信模块故障

单个故障状态下的故障恢复只体现了方法的可行性, 通过多故障同时发生时的故障恢复策略可验证方法的鲁棒性. 如, 当雷达设备传感模块及中继节点设备通信模块同时发生突发性瞬时故障, 导致转发的目标方位角数据错误, 即设备1中传感任务输出数据及设备4中转发任务输出数据偏离真实数据. 如果故障数据不及时恢复而直接作用于火炮控制器, 则系统控制输出如图12所示.

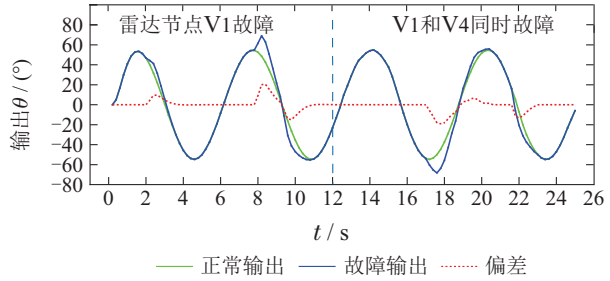


图 12 故障作用下系统输出及偏差

Fig. 12 System output and deviation under the action of fault

设备1与设备4的故障检测点检测出故障数据, 针对两个设备分别生成策略库, 已知在设备1处采用重执行方法, 设备4接受收和转发设备1的数据, 故设备4的恢复策略需考虑设备1处恢复策略的影响.

为此, 在设备4处采用以下3种故障恢复策略:

策略 1 从设备4数据转发任务重执行, 记作τ_{h4}.

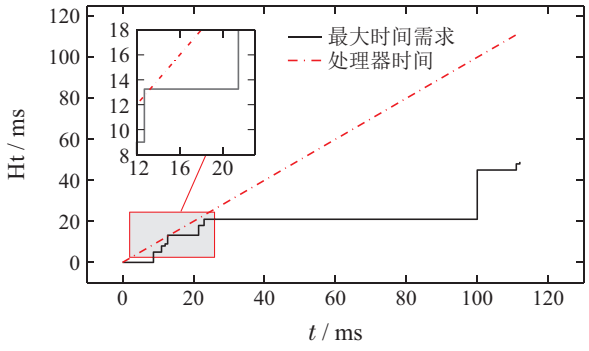
策略 2 在设备9或后续设备中利用历史数据的值估计方法, 得到故障时间内方位角估计值, 记作τ_{h5}, 此任务执行时间为10 ms.

策略 3 在设备9或后续设备中利用限幅的方法, 当数据异常时, 大于零, 限幅为45, 小于零, 限幅为−45, 以期抑制故障影响, 记作τ_{h6}, 此任务执行时间为4 ms.

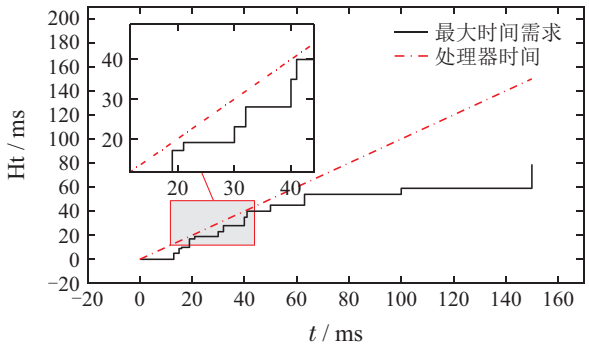
由图13可知, 在所提出的3种故障恢复策略中, 策略1在插入了故障恢复任务τ_{h4}后, 受设备1故障恢复策略影响, 设备8中实时任务的最大需求时钟存在超过系统时间的情况, 即在节点设备8中任务不可调度, 故策略1不可采用. 策略2和策略3在设备9中插入故障恢复任务后系统中任务执行时间虽然受到了影响, 但仍可调度, 故策略2和策略3是可行的.

恢复策略修正的方位角数据传输到火炮随动系统中, 最后得到的控制效果如图14所示.

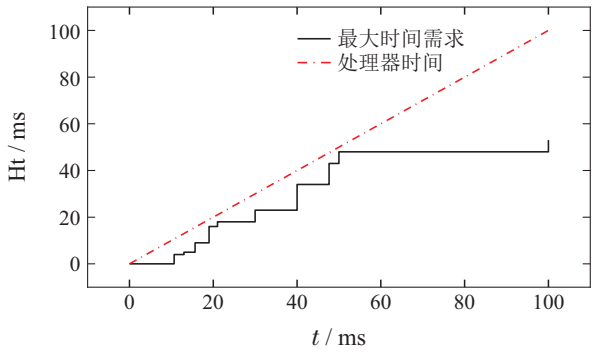
图14显示, 受设备1故障恢复的影响, 设备 4 的重执行故障恢复方法无法实现. 图15显示不同故障恢复策略执行后控制系统的输出偏差, 可知, 策略2在节点设备9处采用基于历史数据的值估计方法进行故障恢复, 其恢复动作执行后, 控制系统输出的偏差最小, 更加接近正常数据的控制效果. 故由此可得到所提出的两种故障恢复策略中, 在设备9中利用历史数据的值估计方法控制故障影响是最优的.



(a) 策略1



(b) 策略2



(c) 策略3

图 13　插入故障恢复任务后各设备中任务最大时间需求

Fig. 13　Task time requirement in device after fault recovery task is inserted

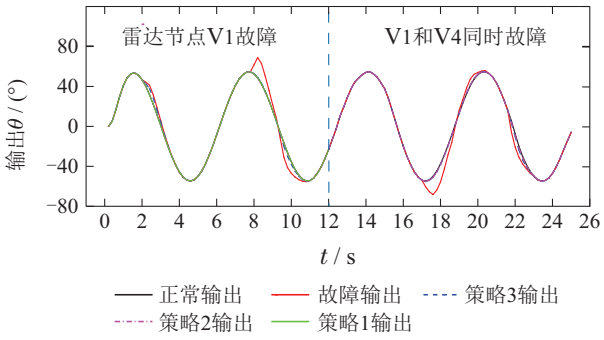


图 14　不同策略的恢复效果

Fig. 14　Recovery effects of different strategies

4.3　最优故障恢复策略

上节对雷达设备传感模块发生突发性瞬时故障影响采集方位信号数据的情形, 提出了多个故障恢复策略, 形成策略库, 利用插入故障恢复任务后系统的可调度性, 以及不同故障恢复策略的恢复效果, 找出了其中的最优故障恢复策略. 同时还考虑雷达设备和中继设备同时故障时, 前一个故障恢复策略对后一个故障恢复的影响, 验证了方法的鲁棒性. 同样还对不同模块故障时对方位角数据的影响, 提出不同的故障恢复策略, 并找出其中的最优策略, 如表3所示. 由表3可以看出, 控制网络中传输的数据受到突发性瞬时故障影响的起始位置不同, 可以采取的最优故障恢复策略可能也不同. 同时发现故障恢复任务的执行时间越短, 即越轻量级的故障恢复方法, 作为故障恢复任务插入系统中, 对系统实时任务调度的影响越小, 但是往往轻量级的故障恢复方法恢复效果不如采用复杂算法的故障恢复方法, 所以后续可以查找或者研究更多更加轻量级且具有更优良恢复效果的故障恢复方法来丰富故障恢复策略库, 从而更好的实现故障控制.

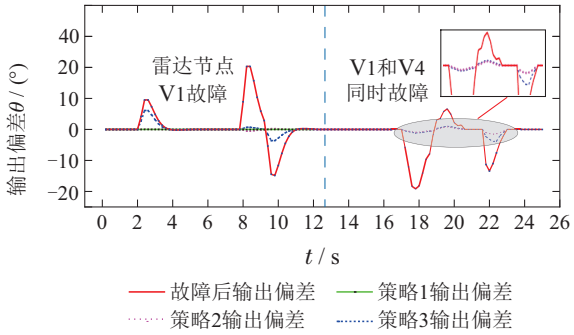


图 15　各恢复策略执行后系统输出偏差对比

Fig. 15　System output deviation after different fault recovery strategies are implemented

表 3　针对故障影响制定的最优故障恢复策略

Table 3　Optimal fault recovery strategy for fault impact

故障位置	故障对数据的影响	提出的故障恢复策略	最优故障回复策略
雷达设备中传感模块执行方位角信号传感任务时突发性瞬时故障	方位角数据错误	1. 从设备1中的传感任务开始重新执行, 以实现数据的重新获取; 2. 在设备1或者后续设备中利用历史数据的值估计故障恢复方法; 3. 在设备1或者后续设备利用限幅的故障恢复方法;	从设备1中的传感任务开始重新执行, 以实现数据的重新获取;
雷达设备通信模块执行传输任务时发生突发性瞬时故障	方位角数据错误	1. 从设备1中的数据传输任务开始重新执行; 2. 在设备4或者后续设备中利用历史数据的值估计故障恢复方法; 3. 在设备4或其后续设备利用限幅的故障恢复方法;	在设备4中利用历史数据的值估计故障恢复方法;
中继转发设备9的通信模块运行转发任务时发生突发性瞬时故障	方位角数据错误	1. 从设备9中的数据转发任务开始重新执行; 2. 在设备8中利用基于历史数据的值估计故障恢复方法; 3. 在设备8中利用限幅的故障恢复方法;	在设备8中利用限幅的故障恢复方法;

5　结论

应急网络控制系统由于工作环境复杂、节点资源受限等特点, 导致在实际应用中容易发生故障, 同时系统高灵活传输机制为系统故障影响的快速扩散提供了可能, 本文为及时控制系统中故障影响范围, 提出了基于故障传播分析的应急网络控制系统故障恢复策略. 主要从故障类型划分、故障传播分析、故障恢复策略制定等多个方面进行了研究, 给出了系统故障

传播分析方法, 帮助找到系统中的关键环节, 为布置故障检测点提供了理论依据; 同时, 介绍了故障恢复策略生成方法, 提出了策略优化算法, 以帮助找到最优故障恢复策略, 最后通过案例分析验证了方法的可行性, 并结合多故障, 验证了方法的鲁棒性. 通过案例分析可以看出, 越轻量级的故障恢复方法, 作为故障恢复任务插入到系统中, 对系统实时任务调度的影响越小, 但是往往轻量级的故障恢复方法可能故障恢复效果不如采用复杂算法的故障恢复方法, 所以后续可以查找或者研究更多更加轻量级且具有更优良恢复效果的故障恢复方法来丰富故障恢复策略库, 从而更好地实现故障控制.

参考文献:

[1] SEBA A, NOUALI-TABOUDJEMAT N, BADACHE N, et al. A review on security challenges of wireless communications in disaster emergency response and crisis management situations. *Journal of Network and Computer Applications*, 2019, 126: 150 – 161.

[2] WANG Hongmin, TIAN Jiaqiang, WEI Lingyun, et al. Multi-unmanned aerial vehicles cooperative searching and tracking strategy for multiple moving targets. *Control Theory & Applications*, 2021, 38(7): 971 – 978.
(王洪民, 田家强, 韦凌云, 等. 多运动目标的多无人机协同搜索追踪策略. 控制理论与应用, 2021, 38(7): 971 – 978.)

[3] CAMBRA C, SENDRA S, LLORET J, et al. Ad hoc network for emergency rescue system based on unmanned aerial vehicles. *Network Protocols and Algorithms*, 2015, 7(4): 72 – 89.

[4] DOU Liqian, JI Chunhui, ZHANG Xiuyun, et al. Closed-loop active fault detection of deep space exploration spacecraft with minor faults. *Control Theory & Applications*, 2019, 36(12): 2085 – 2092.
(窦立谦, 季春惠, 张秀云, 等. 微小故障下的深空探测航天器闭环主动故障检测. 控制理论与应用, 2019, 36(12): 2085 – 2092.)

[5] YIN Xunhe, WANG Xin. Review, analysis and prospect of self-healing control system. *Control Theory & Applications*, 2021, 38(8): 1145 – 1158.
(尹逊和, 王忻. 自愈控制系统研究的综述、分析与展望. 控制理论与应用, 2021, 38(8): 1145 – 1158.)

[6] STÓJ J. Cost-effective hot-standby redundancy with synchronization using EtherCAT and real-time ethernet protocols. *IEEE Transactions on Automation Science and Engineering*, 2020, 18(4): 2035 – 2047.

[7] ZHANG Yani. Fault-tolerant design of dual hot-standby embeded system. *Journal of Northwestern Polytechnical University*, 2017, 35(SI): 120 – 123.
(张雅妮. 基于热备份的双余度嵌入式系统的容错设计. 西北工业大学学报, 2017, 35(SI): 120 – 123.)

[8] SUBASI N, GUNER U, USTOGLU I. N-version programming approach with implicit safety guarantee for complex dynamic system stabilization applications. *Measurement and Control*, 2021, 54(3/4): 269 – 278.

[9] WU H, GUO R, HU Y. FERNANDO: A software transient fault tolerance approach for embedded systems based on redundant multi-threading. *IEEE Access*, 2021, 9: 67154 – 67166.

[10] MUNIR A, KOUSHANFAR F. Design and analysis of secure and dependable automotive CPS: A steer-by-wire case study. *IEEE Transactions on Dependable and Secure Computing*, 2018, 17(4): 813 – 827.

[11] MANSOURI H, PATHAN A S K. A Review of checkpointing and rollback recovery protocols for mobile distributed computing systems. SHAHRESTANI S. *Internet of Things and Secure Smart Environments*. Berlin Germany: Springer International Publishing, 2020: 111 – 146.

[12] GUO Ruifeng, LIU Xian, DING Wanfu, et al. Schedulability analysis for fault-tolerant real-time system under rollback recovery model. *Journal of Chinese Computer Systems*, 2013, 34(6): 1334 – 1338.
(郭锐锋, 刘娴, 丁万夫, 等. 回卷恢复模型下容错实时系统的可调度性分析. 小型微型计算机系统, 2013, 34(6): 1334 – 1338.)

[13] LIU Shunlan, WANG Yan. A low-complexity decoding algorithm based on parity-check-concatenated polar codes. *Journal of Electronics & Information Technology*, 2022, 44(2): 637 – 645.
(刘顺兰, 王燕. 一种基于奇偶校验码级联极化码的低复杂度译码算法. 电子与信息学报, 2022, 44(2): 637 – 645.)

[14] BASKAR S, DHULIPALA V R. Biomedical rehabilitation: Data error detection and correction using two dimensional linear feedback shift register based cyclic redundancy check. *Journal of Medical Imaging and Health Informatics*, 2018, 8(4): 805 – 808.

[15] WANG Y, LI M, SHI H. A method of searching fault propagation paths in mechatronic systems based on MPPS model. *Journal of Central South University*, 2018, 25(9): 2199 – 2218.

[16] KAO H, GARCIA-MOLINA H. Deadline assignment in a distributed soft real-time system. *The 13th International Conference on Distributed Computing Systems*. Pittsburgh, PA, USA: IEEE, 1993, 8: 428 – 437.

[17] ZHOU C, HUANG X, NAIXUE X, et al. A class of general transient faults propagation analysis for networked control systems. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2015, 45(4): 647 – 661.

[18] XIONG Jinshi, LI Jianhua, SHEN Di, et al. Evaluation method for node importance of information system networks based on edge-betweenness. *Science & Technology Review*, 2013, 31(14): 53 – 55.
(熊金石, 李建华, 沈迪, 等. 基于边介数的信息系统网络节点重要性评估方法. 科技导报, 2013, 31(14): 53 – 55.)

[19] LIU C L, LAYLAND J W. Scheduling algorithms for multiprogramming in a hard-real-time environment. *Journal of the ACM*, 1973, 20(1): 46 – 61.

[20] SHEN Zhuowei, WANG Yun. Schedulability analysis algorithm for EDF-based end-to-end real-time systems. *Journal of Computer Research and Development*, 2006, 43(5): 813 – 820.
(沈卓炜, 汪芸. 基于EDF调度策略的端到端实时系统可调度性分析算法. 计算机研究与发展, 2006, 43(5): 813 – 820.)

作者简介:

黄雄峰 博士, 副教授, 硕士生导师, 目前研究方向为网络控制理论与应用、网络控制系统故障恢复与安全控制, E-mail: hfut_huangxf@hfut.edu.cn;

王 錫 硕士研究生, 目前研究方向为智能控制、网络化控制系统理论与应用, E-mail: 2021110419@mail.hfut.edu.cn;

朱严严 硕士研究生, 目前研究方向为网络控制系统故障恢复与安全控制, E-mail: zhuyy@csrzic.com;

黄 双 博士, 高级工程师, 目前研究方向为舰船信息化, E-mail: huangshuang0709@126.com;

张宇娇 博士, 教授, 博士生导师, 目前研究方向为电力设备故障诊断与健康寿命预测、超/特高压输电线路先进设计、施工及智能运维, E-mail: zhangyujiao@hfut.edu.cn.