“工程问题建模与仿真”之案例2

一个多节点声纳系统中同步时钟机制的可靠性评估和系统优化问题

基本条件和实验要求(V2.7 2018更新)

[1． 词汇表 1](#_Toc464479982)

[2． 符号表 2](#_Toc464479983)

[3． 物理模型 3](#_Toc464479984)

[4． 理论假设、基本参数 4](#_Toc464479985)

[4.1 模型中的元件和部件 4](#_Toc464479986)

[4.2 切换器A的故障类型 4](#_Toc464479987)

[4.3 切换器B的故障类型 5](#_Toc464479988)

[4.4 不可靠元件的使用寿命和各种故障的发生概率 5](#_Toc464479989)

[4.5 其他 5](#_Toc464479990)

[5． 建立理论模型 6](#_Toc464479991)

[5.1 元件的状态 6](#_Toc464479992)

[5.2 节点的状态 6](#_Toc464479993)

[5.3 系统的状态 8](#_Toc464479994)

[6． 仿真实验 10](#_Toc464479995)

[6.1 可靠性指标 10](#_Toc464479996)

[6.2 问题求解 10](#_Toc464479997)

[6.3 本模型下系统失效后“复活”的现象 10](#_Toc464479998)

[6.4 模型漏洞修补：元件特定故障组合令系统“工作寿命无限”的问题 11](#_Toc464479999)

[7． 报告写作 11](#_Toc464480000)

[8． 课题研究报告评判要领 12](#_Toc464480001)

[9． 避免不正当使用他人工作成果 12](#_Toc464480002)

# 词汇表

**元件**

部件的基本构成单位，也是模型中系统的最小组成单位，具有“原子性”，不对其分割研究。

**部件**

系统的构成单元，其本身可以由一个或多个元件构成。

**多状态系统**

具有有限种性能状态等级的系统可称作“多状态系统”。在此有限种性能状态中，可以包括一种“完好”状态（性能完美），一种“完全失效”状态，和其余若干种介于前两者之间的“部分失效”状态（不同程度的性能降级）。

一个只具有“好”（性能完美）和“坏”（完全失效）两种状态的系统，是多状态系统的特例。

组成多状态系统的元件（不可靠元件）和部件也可以是具有多状态的。

**不可靠元件**

在模型中被认为可能出现故障的元件。

**可靠元件**

在模型中被认为不会出现故障的元件。这通常是人为建立的理想化概念，将部分物理元件的故障情况等效为系统中其他元件的故障情况，以便简化模型。

***k-out-of-n:G*系统**

一个系统由*n*个组件（元件或部件）构成，其中若至少有*k*个性能正常，则整体系统能有效工作；换言之，仅当多于(*n*-*k*)个组件同时失效，整体才失效。当*n*大于*k*意味着系统结构有冗余。

**总线阻塞**

当主从系统中的信号总线是各部件间的共享信道时，在同一时刻至多只允许有一个部件占用总线（向总线输出信号）。当出现特定故障时，有部件向占用总线并输出无效信号，或同时有两个及以上部件向总线输出信号，就会造成总线阻塞，导致系统整体失效。

# 符号表

|  |  |
| --- | --- |
|  | 事件*X*的发生概率 |
|  | 事件*X*为真时取1，否则取0 |
| ， | 映射关系 |
| *n* | 声纳系统中节点的总数 |
| *k* | 声纳系统中组成有效主从结构所需的最少节点数 |
|  | 元件*X*使用寿命的概率密度函数 |
|  | 元件*X*的期望寿命 |
|  | 元件发生故障，故障*X*发生的条件概率 |
|  | 时刻*t*元件或系统*X*各可能状态对应的概率， |
| ， | 在时刻*t*节点*i*中切换器A和B的性能状态 |
|  | 在时刻*t*节点*i*的性能状态 |
|  | 在时刻*t*声纳系统整体的性能状态 |
|  | 时刻*t*系统中恰好处于状态的节点总数 |
|  | 系统工作寿命 |
|  | 系统可用性，系统工作寿命超过某一定值*w*的概率 |

# 物理模型

1

2

PLL

本地时钟源

锁相环

时钟信号

检测电路

组合控制

电路

切换器A

切换器B

时钟信号总线

本地工作时钟

往内部其他电路

**节点***i*

**节点1**

**节点2**

**节点***i*

**节点***n*

**……**

**……**

图1 一个多节点声纳系统中的时钟同步机制示意图

如图1所示，某分布式部署的声纳系统共有*n*个独立节点构成。各节点内部均是物理同构的。各节点必须保持严格的时钟信号同步才能有效协同工作，使系统发挥作用。所有节点经由时钟信号总线连接，由其中一个节点担当主节点，它的时钟电路工作于主模式，向总线输出时钟信号；其余节点均应担当从节点，节点内部时钟电路工作于从模式，仅从总线获取信号，不向总线输出信号。

节点可能发生故障。由于应用场合的特殊性，故障一旦发生就无法修复。

* 主模式

节点工作于主模式时如图2所示，内部电路中切换器A的掷刀接合于触点2，切换器B处于接通状态。本地时钟源信号既被用作本节点内部其他电路的工作时钟，又被输出到时钟信号总线上。

* 从模式

图1中所示的节点工作于从模式时所示，内部电路中切换器A的掷刀接合于触点1，切换器B处于断开状态。节点从总线获取时钟信号作为锁相环的参考信号，由锁相环输出与参考信号同频同相信好，作为本节点内部其他电路的工作时钟。

* 节点数目冗余

系统中只要有*k*个节点能在同步时钟下正常工作，系统整体就能发挥正常功能。通常，若*n*大于*k*，则系统中节点可能会有多余，这是为了提高系统生存率或使用寿命而做的冗余设计。

* 节点模式变换和主节点的“重选”

若某节点处于主模式。当它内部的时钟信号检测电路发现总线时钟信号失效，或不同于本地时钟源信号，则会通知控制电路改变切换器A和B的连接，退出主模式转为从模式。

若某节点处于从模式。当它内部的时钟信号检测电路发现总线时钟信号失效，则会通知控制电路。控制电路进入戒备状态，为确认情况，将依据预置算法设定一段随机长度的计时。在计时期间，时钟信号检测电路如果检测到有效的总线时钟信号，则退出戒备，该节点继续工作在从模式；但如果计时结束仍未检测到有效的总线时钟信号，则该节点将主动转入主模式。

所以，尽管从系统总体角度观察，当前主节点发生时钟信号输出故障而退出主模式，其余节点中会重新“选”出一个担当新的主节点，但这一机制实际上是由所有节点各自独立动作而造成的总体效果。

1

2

PLL

本地时钟源

锁相环

时钟信号

检测电路

组合控制

电路

切换器A

切换器B

时钟信号总线

本地工作时钟

往内部其他电路

**节点***i*

图2 工作在主模式的节点

# 理论假设、基本参数

## 模型中的元件和部件

为降低运算复杂度，我们将切换器A和切换器B视作不可靠元件，而将系统中的其余元件均视作不失效的可靠元件，这些元件的失效风险已被等效地折算计入不可靠元件的失效风险中。

切换器可视作一种多状态元件，且彼此特性统计独立。由各元件组成的节点是构成系统的部件，显然其性能表现也是多状态的。声纳系统整体可看作一个多状态系统。

## 切换器A的故障类型

切换器A可能出现3种类型的故障，分别称作A1、A2、A3。

* 故障A1：切换器A不能正常受控，掷刀无法与触点1脱离。如图3（a）所示。
* 故障A2：切换器A不能正常受控，掷刀无法与触点2脱离。如图3（b）所示。
* 故障A3：切换器A不能正常受控，掷刀无法与任何一个触点接合。如图3（c）所示。

1

2

切换器A

(a)故障A1掷刀位置

1

2

切换器A

1

2

切换器A

(b)故障A2掷刀位置

(c)故障A3掷刀位置

图3 切换器A的故障类型

## 切换器B的故障类型

切换器B可能出现2种类型的故障，分别称作B1、B2。

* 故障B1：切换器B不能正常受控，掷刀无法与触点脱离。如图4（a）所示。
* 故障B2：切换器B不能正常受控，掷刀无法与触点接合。如图4（b）所示。

切换器B

(b)故障B2掷刀位置

切换器B

(a)故障B1掷刀位置

图4 切换器B的故障类型

## 不可靠元件的使用寿命和各种故障的发生概率

切换器元件使用寿命的概率密度分布都遵从负指数分布。

* 切换器A的使用寿命的概率密度分布和各种故障概率

 （式1） 其中 

条件概率







* 切换器B的使用寿命的概率密度分布

 （式2） 其中 

条件概率





## 其他

* 不同元件随机状态的统计特性彼此独立。
* 元件一旦发生故障，故障类型即刻确定，且其后不会发生变化。
* 故障均不可修复。
* 本课题中*k*取定值4。

# 建立理论模型

依据前文所列各项假设，经分析可建立以下理论模型。

## 元件的状态

切换器A是一个4状态元件，表示其处于正常工作状态，而、、分别表示处于故障A1、A2、A3状态。任一节点*i*中的切换器A状态

 

在时刻*t*时，各状态对应的出现概率

由（式1）可知

 （式3）

因 ，则

 （式4）

 （式5）

 （式6）

同理，切换器B是一个3状态元件，任一节点*i*中的切换器B状态

 

在时刻*t*时，各状态对应的出现概率

而  （式7）

 （式8）

 （式9）

## 节点的状态

节点的状态由其内部元件状态的组合来确定，不同的组合也可能对应相同的节点性能状态。

  （式10）

经分析可知，节点性能状态可以归为6种



其中表示节点性能完好，为直观起见，定义别名（意为perfectly functioning）；

表示只能作为从节点，别名（slave only）；

表示或者作为主节点，或者作为不阻塞总线的失效节点，别名（disable / master）；

表示只能作为主节点，否则就会阻塞总线，别名（master only）；

表示成为不阻塞总线的失效节点，别名（disable node）；

表示节点总是阻塞总线，别名（failed bus）；

切换器A和B的所有组合对应的节点状态见表1。

表1 切换器-节点状态映射关系

|  |  |  |  |
| --- | --- | --- | --- |
| 切换器A状态 | 切换器B状态 | 节点状态 | 别名 |
|  |  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |  |
|  |  |  |
|  |  |  |

在时刻*t*，任一节点*i*的性能状态的概率分布可表示为

 其中   （式11）

## 系统的状态

系统的整体工作状态由所有*n*个节点状态的组合来确定

 （式12）

时刻*t*的系统各节点状态组合可以用*n*阶组合空间来表示





不妨定义表示时刻*t*恰好处于状态的节点总数

 （式13）

利用前文对状态定义的别名，也可写作 （式14）

同样，有，，，，，或称，，，，。

从整体性能的角度，可将的状态归为4类，。

* 系统确定不能有效工作的状态

当有以下情形之一，系统就无法有效工作。

* 1. 条件C1：任一节点处于，即
  2. 条件C2：有两个或以上节点处于，即
  3. 条件C3：无法找到适合工作于主模式的节点，即
  4. 条件C4：能构成有效主从系统的节点总数少于k个，即
* 系统确定能有效工作的状态

当满足条件，系统能有效工作。

* 1. 条件C5：无节点处于，即
  2. 条件C6：有且仅有一个节点处于（注：按前文描述的系统工作机制，该节点必然担当主节点，虽然因为随机因素，过程可能曲折），其余可工作于从模式的节点数不少于k-1，即且
  3. 条件C7：无节点处于，至少一个节点处于且该节点担当主节点，其余可工作于从模式的节点数不少于*k*-1，即且且；或者无节点处于和，但至少一个节点处于能担当主节点，其余处于工作于从模式的节点数不少于*k*-1，即且且且。
* 同时满足条件C8和C9，系统恰能有效工作的状态

当同时满足以下条件，系统在一定概率下有效工作。

* 1. 条件C8：无节点处于或，即
  2. 条件C9：处于的节点大于等于1，且处于和的节点总数恰好为*k*-1，另有若干节点处于，即且且

只有当任一个处于的节点恰好被选作主节点时，系统有效节点总数才能达到*k*，恰好可以有效工作，称作状态。

由于主节点选择机制是随机等概的，所以有条件概率

 （式15）

* 同时满足条件C8和C9，系统恰不能有效工作的状态

当同时满足条件C8和C9，而任一个处于的节点被选作主节点时，系统有效节点总数只能达到*k*-1，恰好不能有效工作，称作状态。

与（式15）相对，有条件概率

 （式16）

# 仿真实验

## 可靠性指标

本系统的各类故障均不可修复，所以可重点研究以下可靠性指标。

首次失效时间（time to failure）：又称工作寿命。是系统从初始时间到首次发生失效的时间。在本系统中，就是系统状态首次向或发生转移的时间，但最大值（见6.4的解释）限定为75000 *hour* 。

平均首次失效时间MTTF（mean time to failure）：平均工作寿命，的统计平均。

系统可靠性：系统工作寿命超过某一定值*w*的概率，系统在期间一直有效工作。

 （式17）

## 问题求解

根据前文的理论假设、基本参数和理论模型，确立仿真算法，用蒙特卡洛法模拟*S*套同型系统的运行状况。建议取。

系统可靠性统计式可以取

 （式18）

其中为仿真实验的*S*套声纳系统中第*i*套的有效工作寿命。

1. 通过随机模拟运行实验，求节点总数*n*，使系统可靠性最大，其中
2. 通过随机模拟运行实验，求节点总数*n*，使系统平均工作寿命最大，其中
3. （optional）通过理论计算，解答以上1和/或2的问题，并与1、2中随机模拟运行的各项结果进行对比分析
4. （optional）自行设立感兴趣的其他论题

## 本模型下系统失效后“复活”的现象

在两种特定的情况下，系统会发生先失效而后又恢复功能的现象。

情况一，同时有两个节点，系统失效。假如两个中至少一个节点内部切换器状态组合为（见表1），其后某一时刻切换器A发生A3故障，节点状态转为（）。由于两个节点争抢总线的情况消失，于是系统可能恢复功能。

情况二，系统处于状态，节点未能成为主节点，有效节点少于*k*个，系统失效。若节点的切换器状态组合为，其后某一时刻切换器B发生B1故障，节点状态转为（），于是必然成为主节点，使系统内有效节点增加1个，系统功能得以恢复；或者还有，主节点发生故障进入状态，一个节点成为主节点，使系统内有效节点增加1个，系统功能得以恢复。

在实际工程系统中，这类因两个故障效果叠加产生的“负负得正”现象确会发生。比如曾有过报道，某航天器上系统失灵后一段时日又戏剧性恢复功能，就被认为是后一个故障戏剧性地“修复”了前一个故障引发的症状。

在本案例中，对随机试验中出现“复活”现象的样本，根据可靠性的定义，不应归入可靠样本计数。

## 模型漏洞修补：元件特定故障组合令系统“工作寿命无限”的问题

考虑这样的情况：如果系统中一个节点的切换器A、B都已损坏，并处在Master Only的状态，而其余的节点的切换器A、B也均损坏，且处在Slave Only的状态。

由于假定了元件损坏后状态不再改变，则处于上述情况的系统将一直保持在工作状态，工作寿命将“无限长”。这种情况，一方面与工程常识不尽相符；另一方面，在进行可靠性指标统计时，通过加和平均运算求取首次失效时间，则上述微小概率事件会直接导致运算结果为无穷大，这无疑是一个模型漏洞。

综合考虑，决定作补充限定：当出现上述情况时，定义其工作寿命为一个足够大的有限值，在前文中已给出此数值。

# 报告写作

将课题研究的结果编写成报告，又称小论文，既是学生课程学习成果的总结，也是本课程评分的主要项目。

报告写作应尽量做好 “言之成理，言之有据”。

提交报告时，应附有用于计算机辅助求解的程序代码。

其他具体要求如下。

* 文章主题目（不是指电子文件名称）指定为“一个多节点声纳系统中同步时钟机制的可靠性评估和系统优化问题”；
* 正式稿无须详细介绍课题背景，可假定读者已阅读过《基本条件和实验要求》（即本文），将本文列为关联文档加以引述，适当减少图文重复，把主要篇幅用作描述自行完成的工作；
* 如果有自主选做的拓展研究话题，请在正文中设立醒目的“一级标题”，并将相应内容置于该标题之下；
* 不包含自主拓展问题讨论的报告，正文篇幅限定不得超过6页（不计正文前的“摘要”、“名词定义和说明”等，正文5号字体，A4纸张，允许双列排版，标题格式自拟）；包含自主拓展问题的报告，篇幅可放宽到最多不超过8页；
* 因内容或篇幅不宜编入正文的部分，允许作为文章附录，但正文应能脱离附录独立成篇；
* 使用本课程提供的小论文模板。

# 课题研究报告评判要领

表2 实验报告评判要领

|  |  |  |
| --- | --- | --- |
| 评判项目 | 要领 | 备注 |
| 数学模型合理性 | 数学逻辑自洽，前提假设合理 | —— |
| 算法说明合理性 | 算法流程清晰 | —— |
| 实验结果合理性 | 与物理实际相一致 | —— |
| 结果分析合理性 | 从实验数据和现象中得到合理和有实用意义的分析结果 | —— |
| 报告整体完整度 | 标题、摘要、引言、正文、附录等 | —— |
| 格式规范程度 | 排版、图表、公式等 | —— |
| 学术规范程度 | 引文注解，禁止抄袭 | 实质性抄袭可能直接导致不及格！ |
| 独立性 | 观点、方法的独特性，对研究内容的自主拓展等 | —— |
| 总评 | —— | 设等级A+, A, A-, B++, B+, B, B-, B, C+, C, C-, D, F  F对应不及格 |

# 避免不正当使用他人工作成果

科学研究中，经常有必要借鉴和学习一点他人的工作和成果，可以获得更高的工作起点，可以少走弯路。但是，我们在发表自己的工作成果时，必须遵循学术规范和惯例做法，把自己的工作中哪些地方是引用或参考他人的工作，哪些地方是本人的独立原创工作，加以明确表述，尽量避免引起读者误解，防止构成事实上的不正当使用他人成果。

在本课程中，如果你借鉴了同届或往届同学的工作，比如往届作业报告中的文字段落或图表，再比如他人的计算机程序代码等，都必须在写作课题研究报告时明确标注、表述或申明。

严格按照学术规范要求来引用和借鉴他人的报告、代码等，是完全正当的。然而，报告中任何未加引用注释或明确表述的非原创内容，都可能引起评判老师误解为作者原创，导致评分时出现误判。此类不遵守规范的情况一经发现，将给予重罚。

同样，报告中引用本课程的讲义或教学材料的内容时，请添加引文注解，或者在表述时插入“据本课程规定”等字样。