·软件技术与数据库· 文章编号：1000-3428(2016)03-0089-05 文献标识码：A 中图分类号：TP311

馈线自动化算法的形式化建模与验证

唐郑熠，王金水，何栋炜，薛醒思，胡文瑜

（福建工程学院信息科学与工程学院，福州 350118）

摘 要： 分布式馈线自动化系统能否正确运作，目前主要是通过测试与仿真技术来保证，但这 2 类方法都要涉及电气设备的底层细节，会分散计算资源，影响验证效率，且难以覆盖足够的系统路径。针对该问题，提出一种馈线自动化算法的验证方法。通过对电气设备行为与特征的抽象，建立馈线自动化算法的形式化模型，在此基础上，使用自动化模型检测技术验证算法的正确性。测试结果表明，该方法将计算资源集中在动作逻辑验证上，实现了与底层细节的分离，从而能够获得较高的验证效率，完整覆盖系统路径，并有效降低缺陷修正的代价。

关键词： 馈线自动化；形式化模型；自动验证；模型检测；时间自动机

中文引用格式： 唐郑熠，王金水，何栋炜，等. 馈线自动化算法的形式化建模与验证[J]. 计算机工程，2016，42(3)：89-93.

英文引用格式： Tang Zhengyi，Wang Jinshui，He Dongwei，et al. Formal Modeling and Verification of Feeder Automation Algorithm[J]. Computer Engineering，2016，42(3)：89-93.

Formal Modeling and Verification of Feeder Automation Algorithm

TANG Zhengyi，WANG Jinshui，HE Dongwei，XUE Xingsi，HU Wenyu

（College of Information Science and Engineering，Fujian University of Technology，Fuzhou 350118，China）

【Abstract】 Testing and simulation are main technologies used to ensure the proper running of distribution feeder automation system. But they both refer to the low-level details of electrical equipment so that the computing resources are scattered，affecting the verification efficiency and the coverage of system paths. For this problem，a new verification method for distribution feeder automation system is proposed. The formal model of the feeder automation algorithm is built by abstracting the actions and features of electrical equipment. Then，the automatic model checking technology is used to verify the correctness of the algorithm. Test results show that，this verification method focuses computing resources on the verification of action logic of algorithm by separating the low-level details. So it has higher verification efficiency and covers all system paths，and it can also reduce the cost of bug fixing.

【Key words】 feeder automation；formal model；automatic verification；model checking；timed automata

DOI： 10.3969/j.issn.1000-3428.2016.03.016

1 概述

馈线自动化是智能电网系统的核心技术，它是指变电站出线到用户用电设备之间的馈电线路的自动化，其作用包括用户检测、运行优化、故障检测、故障隔离、供电恢复等[1]。馈线自动化系统可分为集中式和分布式 2 类[2-3]：前者是将各个开关上的智能电子设备采集的数据传输到主站，由主站进行故障区域定位，并向相应开关的智能电子设备下达故障处理命令；后者依靠智能开关设备的相互配合，即可实现故障隔离和健全区域恢复供电的功能。分布式的馈线自动化系统又可分为自动化开关配合模式与面保护模式 2 类：前者不需要构建通信系统，较为简单和易于实现，但同集中式馈线自动化系统一样，易发生越级跳闸或多级跳闸现象，造成事故范围的扩大[4-5]；后者通过智能电子设备间的通信，获取和利用系统中多个设备的信息，从而能够更有效地进行故障判定与系统保护。

基于面保护模式的分布式馈线自动化系统，可以视作由一组分布在各开关上的、具有独立处理与运算单元，并能够进行信息交换的智能电子设备构成的分布式并行系统[6]。从宏观上看，该类系统的

基金项目： 国家自然科学基金资助项目(61402108)；福建省自然科学基金资助项目(2012J01245)；福建省中青年教师教育科研基金资助项目(JA14221，JB14068，JB14069)；福建工程学院科研启动基金资助项目(GY-Z13112，GY-Z13113)。

作者简介： 唐郑熠(1984－)，男，讲师、博士，主研方向为软件测试、软件工程；王金水、何栋炜、薛醒思，讲师、博士；胡文瑜，教授、博士。

收稿日期： 2015-06-23 **修回日期：** 2015-08-10 **E-mail：** tangzy84@126.com

行为显得杂乱无章,为其设计正确有效的算法与程序是一项十分困难的工作。而对该类算法与程序的正确性验证,也还处于比较原始的状态,依赖于实际的系统运行与调试。

目前用于验证馈线自动化系统正确性的方法,主要包括测试[7-8]与仿真[9-11]。测试方法需要以实际完成的系统或系统单元作为对象,通过大量的用例测试系统在不同情况下的运行状况。其缺点主要有:发现系统缺陷的时间较迟;修正缺陷所需要的代价较为高昂;无法覆盖系统所有的运行路径;效率较低。仿真方法是指使用电力系统仿真软件搭建虚拟的配电网,并在其上构建馈线自动化系统,从而能够在虚拟环境中,以较低的代价完成测试。但是这类方法依然不能避免测试方法的非完全路径覆盖与低效的缺陷。同时,在搭建虚拟环境时,无法屏蔽底层的细节,往往需要进行复杂的参数设置。但是对于馈线自动化系统而言,其算法策略所控制开关的动作逻辑才是验证的对象,过多的底层细节不仅无助于提高验证工作的准确性,反而会导致验证工作变得更加复杂。

UPPAAL[12]以扩展的时间自动机为建模语言,以 TCTL 逻辑为性质描述语言,适合于对能够被划分为多个并行子结构的实时系统进行建模和验证,并且在状态空间约减和搜索速度上具有显著的优势。为此,本文提出一种新的自动化方法对分布式馈线自动化算法进行验证,即基于时间自动机的模型检测方法,并以 UPPAAL 模型检测器作为实现工具。

2 分布式馈线自动化算法

文献[13]提出针对开环配电网的分布式馈线自动化算法,能够实现故障段的自动定位与隔离,简述如下:

(1)故障段定位机制

若一个智能电子设备检测到其控制的开关流过了故障电流,则向相邻的智能电子设备发送报告。若一个配电段内有且只有一个智能电子设备报告流过了故障电流,则故障发生在该配电段内部;否则,故障就没有发生在该配电段内部。

(2)故障段隔离机制

若与某一个开关相关联的所有配电段内部都没有发生故障,则即使该开关流过了故障电流也没有必要跳闸来隔离故障区域。只有当与某一个开关相关联的一个配电段内部发生故障时,该开关才需要跳闸来隔离该故障配电段。

因为故障电流报告的交换需要消耗一定的时间,该算法还规定在检测到或接到故障电流信息后,智能电子设备应在一定的延时后再进行故障判定,从而避免对故障段的误判。

由于开环运行的配电网在联络开关的一侧都只有单个电源,并且在不考虑健全区域恢复机制的情况下,联络开关不需要执行任何动作,因此可以将其视为末梢节点,并以其为分界点,将开环配电网划分为 2 个配电区。例如文献[13]中的开环配电网,可以划分为如图 1 所示的 2 个配电区(方形图标表示出线开关节点,圆形图标表示分段开关节点)。

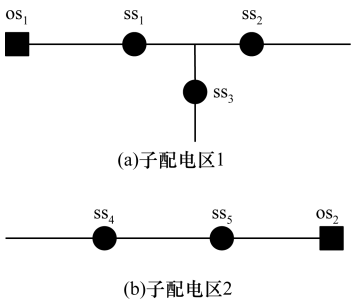

图 1 配电区的划分

3 形式化模型

由于上述算法所执行的操作与配电区中开关的分布有关,因此首先定义配电区的结构图,然后从中定义配电段与故障链,最后建立配电区中各开关单元的时间自动机模型。

3.1 配电区结构

配电区中包含大量的节点,使其呈现为一个复杂的网状结构。但在上述算法中,只有其中的馈线开关及安装在其上的智能电子设备(称为开关单元)对算法才有作用,因此,在进行算法验证时,只有这些开关单元才需要被描述。据此,可以把配电区的结构描述为一种受限的连通图。

定义 1(配电区结构图) 一个配电区结构图 DNS = (N,E),其中,N 为开关单元节点集合,包含一个唯一的出线开关单元节点 os、分段开关单元节点集合 SSN、分支节点集合 FN、末梢节点集合 EN,即 $N = \{os\} \cup SSN \cup FN \cup EN$;E 为节点连接关系集合,即 $E = \{\{m,n\} \mid m,n \in N\}$。E 满足以下约束:

(1)出线开关单元节点有且只有一条边,即存在唯一的 $\{os,n\} \in E, n \in N$。

(2)任意分段开关单元节点有且只有 2 条边,即 $\forall ss \in SSN: \exists \{os,n\}, \{os,m\} \in E, n,m \in N \wedge m \neq n$。

(3)任意末梢节点有且只有一条边,即 $\forall e \in EN$:存在唯一的 $\{e,n\} \in E, n \in N$。

在配电区结构图中,除馈线开关外的其他设备都被隐藏到边中,末梢节点和分支节点是为了使其符合图的定义而增加的虚拟节点。如图 2 所示,开

关单元结点中的数字为该开关单元的编号;虚线圈出的部分为随后定义的配电段,旁边的数字为该配电段的编号,这些编号会在后面的建模中使用到。

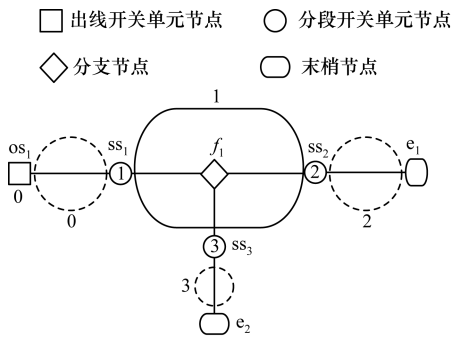

图 2　配电区结构

定义 2(配电段)　在配电区结构中,2 个属于 $\{os\}\cup SSN$的节点 rn,rn′称为同段节点,当且仅当:$\exists <rn,n_1,n_2,\cdots,rn'> \wedge \forall n_i: n_i \in \{os\}\cup FN$。由同段节点构成一个配电段,记为 pdr(RN),RN 为该配电段所有同段节点的集合。

如图 2 的配电区结构图,有 4 个配电段:$pdr(os_1,ss_1)$,$pdr(ss_1,ss_2,ss_3)$,$pdr(ss_2,e_1)$,$pdr(ss_3,e_2)$。

3.2　故障链

当一个配电段中的馈线发生故障时,故障电流会传导到多个配电段,并被这些配电段中的某些同段节点上的智能电子设备检测到,因此,可以用这些同段节点描述一条故障链。

定义 3(故障链)　故障链 $FC(pdr(RN)) = <sn_1,sn_2,\cdots,sn_m>$,其中,pdr(RN)是一个配电段;$sn_i$ 是某个配电段的同段节点,且 sn_i 上的智能电子设备能够监测到配电段 pdr(RN)所传导的故障电流,sn_i 按照故障电流流经的先后顺序排列。

由于每个配电区只有一个电源点,当某个馈线段出现故障时,故障电流会沿原路径流回电源点,即出线开关单元节点,因此可以使用深度优先搜索策略,计算每个配电区的故障链。以下为具体的算法描述:

算法　CFC(Comput Fault Chain)
输入　A power distribution area(Graph) G
输出　A set of fault chain FC

```
Set chain as a stack;
Set seq as a sequence;
Set visited as a set;
Get os from G;
searchFaultChain(os);
searchFaultChain(n) {
    if(n ∈G. SSN ∪{os}) then {
        chain. push(n);
    // reverse 函数将 chain 中结点的顺序逆转
        FC: = FC ∪{reverse(chain)};
    }
    visited: = visited ∪{n};
    while(∃{n,n′}∈G. E ∧n′∉visited) {
        searchFaultChain(n′);
    }
    if(n ∈G. SSN ∪{os}) then chain. pop();
    return;
}
```

使用该算法对图 2 所示的配电区进行计算,依次得到故障链:$<os_1>$,$<ss_1,os_1>$,$<ss_3,ss_1,os_1>$,$<ss_2,ss_1,os_1>$。

每个故障链第一个节点逆向的配电段对应该故障链,即:$FC(pdr(os_1,ss_1)) = <os_1>$,$FC(pdr(ss_1,ss_2,ss_3)) = <ss_1,os_1>$,$FC(pdr(ss_2,e_1)) = <ss_2,ss_1,os_1>$,$FC(pdr(ss_3,e_2)) = <ss_3,ss_1,os_1>$。

3.3　开关单元的时间自动机模型

每个开关单元可能处于 4 种不同的状态:闭闸(Close),故障报告(Report),故障定位(Detection),开闸(Cutoff)。这 4 种状态之间存在 5 类迁移,迁移发生的条件与效果如表 1 所示。表 2 是描述迁移的过程中所使用的各种数据。

表 1　开关单元的迁移

迁移	条件	效果
Colse →Report	检测到故障电流	–
Report →Detection	–	向全部同段开关发出故障报告
Colse →Detection	接收到同段开关单元的故障报告	–
Detection →Close	故障不处在其所连接的配电段	–
Detection →Cutoff	故障处在其所连接的配电段	–

表 2　数据定义

数据定义	说明
broadcast chan cirFault[4]	用于引发配电段故障
broadcast chan reptFault[4]	用于引发故障报告
int[0,1],faultAlarm[4]	标识对应编号的开关单元是否发出故障报告(1 为是,0 为否)
bool faultFlag[4]	标识对应编号的配电段是否发生了故障(1 为是,0 为否)

下面解释如何用 UPPAAL 的建模语言描述表 1 中的迁移:

(1)检测故障电流

广播通道能让一个发射迁移(!)引发多个接收迁移(?),因此,当 cirFault[i]! 发生时,若配电段 i 的故障链中包含开关单元 j,则开关单元 j 存在从 Colse 到 Report 的,以 cirFault[i]? 为条件的迁移。

显然,Colse →Report 的迁移可能有多个。

(2)发送与接收故障报告

当开关单元 i 发送故障报告时,与其处于同一个配电段的所有开关单元都要从 Colse 状态进入 Detection 状态。因此,开关单元 i 存在从 Report 到 Detection 的,以 reptFault[i]! 为效果的迁移,同时为了故障定位的需要应将 faultAlarm[i]的值置为 1,而其同段的开关单元则存在从 Colse 到 Detection 的,以 reptFault[i]? 为条件的迁移。因为发送故障报告不能延迟,所以可以将 Report 状态设为紧急(Urgent)状态,该状态不允许发生延时。

(3)故障定位

开关单元 i 在发送故障报告时,会将faultAlarm[i]的值置为 1,因此,开关单元判定其连接的配电段是否发生故障时,只需判定 faultAlarm[n_1] + faultAlarm[n_2] + … + faultAlarm[n_k] (n_1 ~ n_k 为同段开关的编号)的值是否为 1 即可。需要注意的是,在进入 Detection 状态后,不能立即进行故障定位,应有一定的延时(例如 15 ms)。UPPAAL 支持函数(语法类似 C 函数),因此,可通过定义函数来进行故障定位,例如可以定义函数 isFaultSeg1( ) 判定 1 号配电段是否出现故障。

```
bool isFaultSeg1( ) {
    if( faultAlarm[1] + faultAlarm[2] + faultAlarm[3] == 1)
        return true;
    return false;
}
```

开关单元 ss_1 的时间自动机模型如图 3 所示。

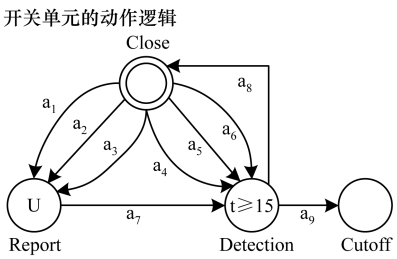

图 3 开关单元 ss_1 的时间自动机模型

图 3 中的迁移标号解释如下:

(1)a_1:cirFault[1]?;

(2)a_2:cirFault[2]?;

(3)a_3:cirFault[3]?;

(4)a_4:reptFault[0]?,t:=0;

(5)a_5:reptFault[2]?,t:=0;

(6)a_6:reptFault[3]?,t:=0;

(7)a_7:reptFault[1]!,faultAlarm[1]:=1,t:=0;

(8)a_8:t>=15 &&! isFaultSeg0( ) &&! isFaultSeg1( );

(9)a_9:t>=15 &&(isFaultSeg0( ) || isFaultSeg1( ))。

4 系统性质与验证结果

4.1 自动机测试

测试自动机的作用是从所有配电段中任意选择一个,并将其设为故障,即一个以 cirFault[i]! 和 faultFlag[i]:= true 为效果的迁移,如图 4 所示。

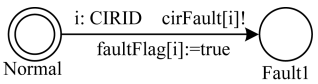

图 4 测试自动机

CIRID 是一个自定义类型,其取值范围为[0,3];表达式"i: CIRID"是指从 CIRID 的取值范围中任取一个值赋给 i。

4.2 系统性质

故障段定位与隔离算法的正确性可由以下 2 个系统性质保证:

(1)当配电段 i 发生故障时,配电段 i 的所有同段开关单元最终都能到达 Cutoff 状态。

(2)在所有情况下,若与某个开关单元相连的所有配电段都没有发生故障,则该开关单元都不能到达 Cutoff 状态。

性质(1)用于保证在发生故障的情况下,算法能够正确地定位出故障位置并进行隔离操作;性质(2)用于保证在没有发生故障的情况下,算法不会产生断闸的误操作。

以配电段 pdr(ss_1, ss_2, ss_3)为例,性质(1)用 UPPAAL 的性质描述语言描述为:

faultFlag[1]-> (SS1. Cutoff && SS2. Cutoff && SS3. Cutoff)

以开关单元 ss_1 为例,性质(2)用 UPPAAL 的性质描述语言描述为:

A[ ](! faultFlag[0] && ! faultFlag[1]) imply not SS1. Cutoff

4.3 验证结果

在只有一个配电段发生故障的情况下,所有的性质都验证通过,证明该算法能够在单个配电段故障的情况下正确运行。

下面考虑另外一种情况:2 个配电段同时或在较短的时间间隔内发生故障。在这种情况下,UPPAAL 验证出上述性质(1)不成立。通过生成反例,可以很清楚地发现问题所在,如图 5 所示,箭头表示信号传递方向。

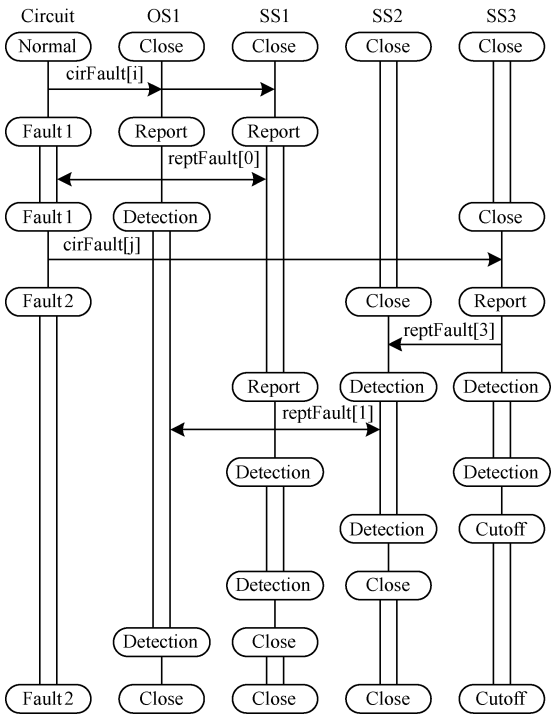

图 5　UPPAAL 生成的反例

在该反例中,1 号配电段与 3 号配电段在故障检测延时内(15 ms)相继发生故障,这导致开关单元 os_1,ss_1,ss_3 都检测到了故障电流,并发出了故障报告。由于 ss_1 和 ss_3 都发出了故障报告,这导致 ss_1,ss_2 和 ss_3 发生误判,认为 1 号配电段没有发生故障,因此 ss_1 和 ss_2 没有执行断闸保护动作。显然,当在较短的时间间隔内出现 2 个或 2 个以上的配电段连续发生故障时,该算法可能对故障配电段产生误判。

5　结束语

模型检测方法已被成功地运用在计算机系统的分析与设计中,成为一种保障系统安全性与正确性的重要而有效的方法。智能电网系统尽管与计算机系统相比存在较大的不同,但如果屏蔽底层细节,抽象出系统的行为及其所产生的效果,那么模型检测方法完全可以对其进行有效验证。本文所提出的验证方法屏蔽了与馈线自动化算法无关电气设备的底层细节,只对算法所控制的系统单元进行描述,并关注算法能否在不同情况下都执行预期的行为。验证结果表明,该方法能够发现算法中的隐藏漏洞,提高系统设计的质量、减少系统测试与错误修正的代价。

参考文献

[1] 赵拥华,方永毅,王　娜,等. 逆变型分布式电源接入配电网对馈线自动化的影响研究[J]. 电力系统保护与控制,2013,41(24):117-122.

[2] Yao Chonggu, Teng Huan. The Research of Feeder Automation Based on IEC61850[C]//Proceedings of International Conference on Electricity Distribution. Washington D. C.,USA:IEEE Press,2012:1-4.

[3] 刘　健,赵树仁,贠保记,等. 分布智能型馈线自动化系统快速自愈技术及可靠性保障措施[J]. 电力系统自动化,2011,35(17):67-71.

[4] 郭谋发,郑新桃,杨耿杰,等. 利用暂态波形伸缩变换的谐振接地系统故障选线方法[J]. 电力自动化设备,2014,34(9):33-40.

[5] 邹贵彬,高厚磊,许春华,等. 馈线自动化自适应快速保护控制方案[J]. 电网技术,2013,37(10):2920-2925.

[6] Waye A,Gilani A,Flemming S,et al. Feeder Automation in Advanced Distribution Systems [C]//Proceedings of International Conference on Electrical and Computer Engineering. Washington D. C.,USA:IEEE Press,2014:1-6.

[7] 李　林,郭晋楠,张少雷,等. 配电自动化分布式 FA 联动测试系统的研究[J]. 电测与仪表,2013,50(5):123-128.

[8] 刘　健,张小庆,赵树仁,等. 配电自动化故障处理性能主站注入测试法[J]. 电力系统自动化,2012,36(18):67-71.

[9] Liu Jinsong, Liu Dong, Ling Wangshui, et al. Study on Simulation and Testing of FLISR[C]//Proceedings of International Conference on Electricity Distribution. Washington D. C.,USA:IEEE Press,2010:1-7.

[10] 翁之浩,刘　东,柳劲松,等. 基于并行计算的馈线自动化仿真测试环境[J]. 电力系统自动化,2009,33(7):43-46.

[11] 吴俊华,温彦君,赵　月,等. 配电网自动化在线仿真系统技术论述[J]. 电力自动化设备,2006,26(4):50-52.

[12] David A, Larsen K G, Legay A, et al. UPPAAL SMC Tutorial[J]. International Journal on Software Tools for Technology Transfer,2015,17(4):397-415.

[13] 刘　健,贠保记,崔　琪,等. 一种快速自愈的分布智能馈线自动化系统[J]. 电力系统自动化,2010,34(10):62-66.

编辑　刘　冰