DOI: 10.19783/j.cnki.pspc.180979

基于 PAT 包含告警信号的智能变电站保护信息交互建模与验证

王洪彬[1]，张友强[1]，童晓阳[2]，郭 升[2]，袁明旭[3]，黄 敏[4]

(1. 国网重庆市电力公司电力科学研究院，重庆 401123；2. 西南交通大学电气工程学院，四川 成都 610031；
3. 国网四川省电力公司雅安供电公司，四川 雅安 625000；4. 国网重庆市电力公司检修分公司，重庆 400039)

摘要：为了准确评估告警信号产生时智能变电站保护系统的可靠运行情况，研究了一种基于进程仿真工具 PAT 的智能变电站保护信息交互建模与验证方法。分析了多个厂家保护装置的原理，构造了保护系统的告警故障树，给出了各保护子功能的工作条件与告警信号的对应关系。采用进程仿真工具 PAT 的实时系统模块 RTS(Real-Time System Module)，对各 IED 的内部工作、各 IED 之间的交互过程等进行建模，包括工作条件、各进程之间的信息传递与时序等，给出了保护子功能死锁与保护系统运行阶段的断言与验证。多个算例验证了基于 PAT 包含告警信号的智能变电站保护系统交互建模与验证方法的有效性，提高了保护模型的准确性和实用性。

关键词：智能变电站；告警信号；保护系统；PAT；信息交互

PAT based modeling and verification of interaction for protection system in intelligent substation using alarming signals

WANG Hongbin[1], ZHANG Youqiang[1], TONG Xiaoyang[2], GUO Sheng[2], YUAN Mingxu[3], HUANG Min[4]

(1. State Grid Chongqing Electric Power Research Institute, Chongqing 401123, China; 2. School of Electrical Engineering, Southwest Jiaotong University, Chengdu 610031, China; 3. State Grid Sichuan Electric Power Ya'an Power Supply Company, Ya'an 625000, China; 4. State Grid Chongqing Power Maintenance Branch Company, Chongqing 400039, China)

Abstract: In order to accurately assess the reliability of protection system in intelligent substation, a kind of modeling and verification of interaction for protection system in intelligent substation using alarming signals is proposed. The principles of protection devices are analyzed. The fault trees of protections are constructed. The relations between the working conditions and the alarm signals are given. Using the Real-Time System Module (RTS) module of Process Analysis Toolkit (PAT), the working process and the information interaction model of IEDs are set up, including the working conditions, information transmission and time sequences. The assertions of protection deadlock and operation stages are designed for the verification. The examples illustrate the effectiveness of proposed method, the accuracy and practicability of protection system can be improved.

This work is supported by National Natural Science Foundation of China (NSFC) (No. 51377137) and Science and Technology Project of State Grid Corporation of China (No. 52199916024N).

Key words: intelligent substation; alarm signals; protection system; PAT; information interaction

0 引言

近几年基于 IEC 61850 的智能变电站自动化系统得到了大力的发展[1-3]。各厂家遵循协议对 IED (Intelligent Electronic Device)进行标准化建模、设计及测试[4-13]。变电站保护系统的可靠运行很大程度上依赖于 IED 之间的互操作和借助于通信网络的信息交换[14-16]。在 IED 的设计、测试过程中，为了更好地保证 IED 可靠运行，需要对各保护功能在 IED 的内部工作、交互过程及系统行为等进行严格的描述，并加以验证，才能保证各分布式功能的正确性。

基金项目：国家自然科学基金面上项目资助(51377137)；国家电网公司科技项目资助(52199916024N)

因此有必要研究智能变电站 IED 交互行为的形式化建模与验证。

文献[17]为 IED 的交互过程构建了较统一的功能模型，阐述 IED 之间、IED 内部逻辑节点 LN 之间的交互类型，采用扩展协作图和时序图分别刻画分布式保护功能下各 LN 之间的协作和时序关系。文献[18]采用着色 Petri 描述系统的行为，但是对于复杂系统，存在状态空间过大的问题。文献[19]研究基于统一建模语言的 IED 逻辑模型向通信顺序进程 CSP 模型的转化，对 IED 交互行为的描述和验证，但是该方法的转化难度较大。以上 IED 建模成果在设计阶段有助于分析系统的行为和设计的规范化、促进了测试效率的提高。而在 IED 的运维过程中，各设备发出的告警信号反映了设备的正常运行与异常状态，目前，国内外缺乏研究各告警信号作用下保护系统交互过程的分析与验证，利用告警信号的 IED 交互行为的建模与验证研究尚不多见。

本文通过分析变电站配置描述文件(Substation Configuration Description, SCD)，得到各保护装置的告警信号，构造保护失效故障树，反映各保护失效的原因，将来自设备的各告警信号与失效故障树的叶子节点(底层事件)建立联系。运用 PAT 对各保护子功能的进程及其工作条件、IED 之间的交互模型等进行形式化建模。采用 PAT 对各告警信号作用下各保护系统的交互行为进行仿真实验，检验各保护系统的可达性与运行阶段。

1　告警信号与保护故障树

1.1 告警信号的分类分析

IEC 61850 将智能变电站保护功能定义为由多个设备配合完成的分布式功能。智能变电站中线路保护功能借助网络由合并单元、保护装置、智能终端等设备配合完成。研究多个厂家保护装置的工作原理及其工作条件，收集各厂家装置的告警信号。对 SCD 文件进行解析，获得各逻辑设备的告警信号，它们反映设备与保护功能的异常情况。

智能变电站各保护功能由多个设备通过通信网络配合完成。某保护功能的失效，是由其组成设备的故障及彼此之间的通信设备与通信链路的故障与失效等造成的。设备的告警信号大致分为装置自检告警、一般运行告警、运行异常告警、通讯管理运行告警等类，告警级别分一般、异常、严重。保护正常动作、对时信号异常等告警信号，不会影响保护的正常工作。其它一般运行告警信号，如内部通信运行异常，属于一般告警，本文不做处理。剩余的几类告警信号反映保护功能受到了影响。图 1 线路差动保护的故障树中叶子节点(底层事件)对应着一个告警信号。针对各保护子功能，对影响其运行的各告警信号进行分类，划归到各装置、各保护功能的各工作条件中，便于检查保护装置或保护功能是否正常运行。

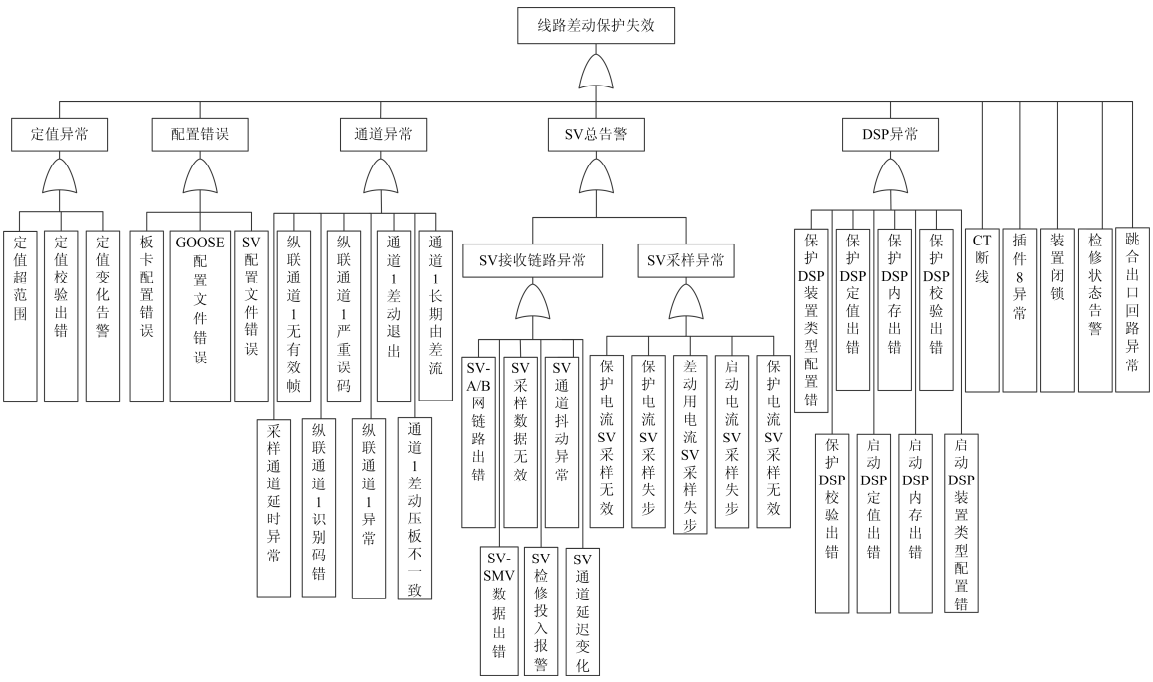

图 1　线路差动保护系统的故障树

Fig. 1 Fault tree of the line protection device

根据来自设备厂家的告警信号，将其分为定值异常、配置错误、通道异常、SV 总告警信号、DSP 异常、硬件异常、其他影响保护功能的异常信号。

1.2 基于告警信号的保护系统故障树建模

各设备在运行过程中发生故障与异常时，通过其自身的站控层和过程层通信接口传递相关 MMS 报文的告警信号。事先解析 SCD 中各 IED 下“S1”访问点下公用 LD0、保护逻辑 PROT 逻辑设备下告警信号数据集(如 dsAlarm、sWarning 等)，得到各 LD 的告警信号，对它们进行分析，只保留对保护功能有影响的告警信号，由此构建基于告警信号的各保护系统故障树。

本文以线路差动保护为例，图 1 中线路差动保护失效原因大体分为上述几类，每类下面有各自的失效子原因，每个子原因是该故障树的叶子节点，对应一个基本事件，一般也对应一个告警信号。

2 PAT 简介

PAT(Process Analysis Toolkit)是由新加坡国立大学开发的模型检测工具，能够对 CSP、实时系统模块(Real-Time System Module, RTS)等模型建模与校验。PAT 提供了进程可视化模拟、可达性分析、死锁检测等功能[20]。PAT 的 RTS 模块支持组成定时过程的实时系统，可捕获定量时序要求，例如延迟、超时、截止时间、定时中断等。

PAT 中实时系统模块 RTS 的基本规范式如下：

通过一些基本事件组成一个事件的序列称为一个进程，通常用大写字母表示如规范式中的 *X*、*P*、*Q* 等。

用 *a*、*b*、*c* 等小写字母或自定义字符串作为变量名，表示基本事件，其定义方式如下：

var*a* = 0;

其中 var 是定义变量的关键词，*a* 是变量名。

X=if *b* (*cond*) {*P*};

表示线程 *X* 在条件 *cond* 满足情况下执行线程 *P*。

if (cond1) { *P* } else if (cond2) { *Q* } else { *M* }

表示一个进程内部在不同条件下分支执行子进程，如果满足条件 1(cond1)就执行子进程 *P*，满足条件 2(cond2)就执行子进程 *Q*，否则执行子进程 *M*。

P;*Q*

表示两个进程依次执行，先执行 *P* 再执行 *Q*。

V() = *P*{*m*=1}->*Q*->*V*();

表示一个进程 *V*()由两个事件 *P*、*Q* 组成，从第 1 个事件 *P* 执行到第 2 个事件 *Q*，再递归返回到进程本身。“->”表示指向下一个事件。{}中间是事件中给某变量赋值，如给 *m* 赋值 1。

Wait[10]：

表示延时语句，10 表示延时时间，单位为 ms。

system=*X* || *Z*;

||表示某线程 system 是由线程 *X*、*Z* 并行执行。

#assert*X*deadlockfree;

表示线程 *X* 无死锁的断言语句，用于判断进程 *X* 无死锁(deadlockfree)。如果进程 *X* 顺利执行，则该语句的验证执行结果是“VALID”(合法)，无死锁；否则执行结果为“NOTVALID”(不合法)，表示死锁。

#define WholeProcess*m* == 1;

定义一个宏条件 WholeProcess，表示变量 *m* 等于 1。

#assertsystem reaches WholeProcess;

该断言语句的验证执行结果是“VALID”(合法)，表示进程 system 到达宏变量 WholeProcess，满足了 WholeProcess 定义的条件，即线程 system 满足 *m*=1；执行结果为“NOT VALID”，表示 system 满足 *m*=1。

3 智能变电站保护系统交互的 PAT 建模

根据各装置的工作原理及其工作条件，建立各装置内部的各子进程模型，建立各子进程的执行条件。反映装置异常的各告警信号将会影响这些执行条件，运用 RTS 模块对各保护进程及其判断条件进行形式化建模。根据故障树给出的几类原因及其它影响保护装置正常工作的条件，对各保护功能在保护装置、智能终端、合并单元的内部子进程及设备之间的交互过程进行建模，对各进程设置其工作条件的判断变量。

构造各保护进程死锁的断言、系统到达某个阶段的断言。运用 PAT 的 RTS 模块对这些断言进行校验，检查在各种告警信号作用下各保护子功能的死锁、各保护功能的执行阶段等情况。

3.1 各保护子功能的建模

各保护系统由多个保护子功能(子进程)组成，各子进程有各自的工作条件，需要根据告警信号来检查其工作条件是否满足，并建立 IED 之间的交互进程。

以线路差动保护系统为例，主进程是 P1。若保护装置没有发出异常信号，标记当前阶段为 0，对其循环检查(Pre_read{counter=0}->P1)。若线路发生故障，并且保护装置没有发出异常信号，则通过智能终端向断路器发跳闸信号(子线程为 IT)，再向站控层发送报告(子线程为 ReportStr)。此时保护装置正常工作、GOOSE 网正常，就完成了采样、保护

计算、跳闸，则设置该阶段标记为 1(counter=1)；如果完成了整个流程：采样、保护计算、跳闸，并向站控层发送报告，则设置该阶段标记为 2(counter=2)。

以线路差动保护为例，其功能及其交互建模如下：

```
P1 = ifb(Protection_state==0) {
        if(Protection_state ==0 &&Line_Error==0)
         {Pre_read{ counter=0}-> P1 }}
         else if( Protection_state ==0 &&Line_Error==1)
         {IT; ReportStr; P1};
```

线路差动保护功能 P1 是否正常，需要通过反映 P1 受影响的告警信号来体现。当线路无故障时(Line_Error=0)，通过对反映保护装置受影响的告警信号进行条件检查，若保护装置没有发出异常告警信号，则对它循环检查(Pre_read{counter=0}−>P1)。若线路发生故障，保护装置没有发出异常告警信号，发 GOOSE 跳闸报文给智能终端，后者向断路器发跳闸信号，再向站控层发送保护动作等报告({IT;ReportStr; P1})。此时保护装置正常工作、GOOSE 网正常，完成了采样、保护计算、跳闸。

不同采样跳闸方式下告警信号反映了保护功能受影响的程度。用进程 PreP1 判断各采样跳闸方式受交换机、SV 网、GOOSE 网的影响，从这几个方面检查条件是否满足。

PreP1 为不同采样跳闸模式下的保护装置工作条件检查进程：

```
PreP1=ifb(Protection_state==1)
{if(Line_Error==0 )
{Pre_read{ counter=−1}->Stop}
else if( Line_Error==1 &&SV_state==0 &&
GOOSE_state==0&&Caiyangtiaozhafangshi==1)
{Pre_read{ counter=−1}->IT;ReportStr;Stop }
else if( Line_Error==1 &&jiangejiaohuanji==0
&&zhongxinjiaohuanji==0 &&SV_state==0 &&
GOOSE_state==0&&Caiyangtiaozhafangshi==2)
{Pre_read{ counter=−1}->IT;ReportStr;Stop}
else if( Line_Error==1 &&jiangejiaohuanji==0
&&zhongxinjiaohuanji==0 &&SV_state==0 &&
GOOSE_state==0&&Caiyangtiaozhafangshi==3)
{Pre_read{ counter=−1}->IT;ReportStr;Stop}
else
{Pre_read{ counter=−1}->ReportStr;Stop}};
```

其中，Caiyangtiaozhafangshi==1 表示直采直跳、Caiyangtiaozhafangshi==2 表示直采网跳、Caiyangtiaozhafangshi==3 表示网采网跳。3 种采样跳闸方式下参与的设备各不同，直采直跳方式下不需要交换机参与，因此交换机故障告警信号对该采样跳闸模式下的保护功能没有影响。“直采网跳”和“网采网跳”模式下均有间隔交换机和中心交换机参与，因此交换机故障告警信号会影响这两种模式下的保护功能。

TCTR 表示采样环节，主要受到 SV 网的采样链路与 SV 接收链路的影响，从这两个方面检查条件是否满足，如果它们正常则给 SV 网状态 SV_state 赋值 0。

```
TCTR = ifb(SVcaiyang==0 &&SVjieshoulianlu==0 )
    {TCTR_ready{SV_state=0} -> TCTR};
```

IT 表示跳闸环节，主要受到保护装置和 GOOSE 网状态的影响，从这两个方面检查条件是否满足。

```
IT=ifb(Protection_state==0&&GOOSE_state==0)
    {Protection_state==0, str_to_IT{counter=1}->
Wait[0] };
```

ReportStr 表示向站控层发送报告，其正常运行受保护装置和站控层通信的影响，需要对这两个条件进行检查。如果各条件都满足，依次延时后向站控层发送报告 strop1、strop2，此时设置阶段标记为 2 (counter=2)，即完成整个过程：采样、保护计算、跳闸、向站控层发报告的完整过程。

```
ReportStr=ifb(Protection_state==0&&
            tongxin_to_Zhankong==0)
    {report_strop1{counter=2}->Wait[10];
report_strop2->Wait[1000] };
```

线路差动保护功能 LP1_System 是由多个进程并行完成。

```
LP1_System=PreDingZhi1 || PreDingZhi2||PrePeiZhi1
    ||PrePeiZhi2 || PreTongDao1 || PreTongDao2
    ||PreSVjianshoulianlu1||PreSVjianshoulianlu2
    || PreSVcaiyang1 || PreSVcaiyang2
    || PreGOOSE_state1 || PreGOOSE_state2
    || PreDSP_state1 ||PreDSP_state2
    || PreYingJian_state1 || PreYingJian_state2
    ||PreProtection_state1 || PreProtection_state2
    || TCTR_P1_Protocol || IT ||ReportStr;
```

PreDingZhi 进程为定值告警信号集合校验、PrePeiZhi 进程为配置告警信号集合校验、PreTongDao 进程为通道告警信号集合校验、PreSVjianshoulianlu 进程为 SV 网接收链路告警信号集合校验、PreSVcaiyang 进程为 SV 网采样告警信号集合校验、PreGOOSE_state 进程为 GOOSE 网告

警信号集合校验、PreDSP_state 进程为 DSP 告警信号集合校验、PreYingJian_state 进程为硬件告警信号集合校验、PreProtection_state 进程为保护装置告警信号集合校验。

3.2 各保护子功能工作条件的建模

根据告警信号的分类集合，将故障树中叶子节点对应的告警信号转化为各保护子系统的工作条件检查。对每个保护的告警信号进行定义，例如定值相关信号中的定值超范围转化为 PAT 语言，定义为 vardingzhichaofanwei=0(0 表示正常，1 表示异常)。

用两个进程表示某定值状态的正常与异常状态，每个进程判断完后继续指向该进程本身，实现对告警的实时检验。保护装置定值正常进程 PreDingZhi1、保护装置定值异常进程 PreDingZhi2 如下：

```
PreDingZhi1=ifb(dingzhichaofanwei==0
    &&dingzhijiaoyanchucuo==0
    &&dingzhibianhuagaojing==0)
    {Pre_read{DingZhi=0}-> PreDingZhi1
```

如果保护装置定值状态的 3 个条件(定值超范围、定值校验出错、定值变化告警)正常，则设置定值状态变量 DingZhi 为 0，然后返回进程自身。

```
PreDingZhi2=ifb(dingzhichaofanwei==1
    || dingzhijiaoyanchucuo==1
    ||dingzhibianhuagaojing==1)
    {Pre_read{DingZhi=1}-> PreDingZhi2
```

设置保护装置定值状态为 1(异常)，返回。

保护功能由采样、计算、跳闸、向站控层发报告等环节配合完成，因此必须要对与保护功能相关的各个环节正常工作的条件进行校验。

首先需要检查保护装置的状态是否正常，本文根据反映保护功能异常的保护装置告警信号集合，从定值告警、配置告警、通道告警、SV 采样告警、SV 接受链路告警、DSP 告警、硬件告警等方面对保护装置是否正常工作进行检查，具体建模如下：

```
PreProtection_state1= ifb(DingZhi==0 &&PeiZhi==0
    &&TongDao==0 &&SVjieshoulianlu==0
    &&SVcaiyang==0 &&DSP_state==0
    &&YingJian_state==0 )
    {Pre_read{Protection_state=0}->
    PreProtection_state1
```

进程PreProtection_state1表示保护装置状态正常。

```
PreProtection_state2=ifb(DingZhi==1||PeiZhi==1
    || TongDao==1 || SVjieshoulianlu==1
    || SVcaiyang==1 ||
    DSP_state==1||YingJian_state==1)
    {Pre_read{Protecton_state=1}->PreProtecton_state2
```

进程PreProtection_state2表示保护装置状态异常。

当采用网采方式时，本文根据反映采样受影响的告警信号，从SV采样告警、SV接受链路告警等方面对采样环节是否正常进行检查，具体建模如下：

```
TCTR = ifb(SVcaiyang==0 &&SVjieshoulianlu==0 )
    {TCTR_ready{SV_state=0} -> TCTR};
```

采样环节成功采样与否，需要检查采样信息向保护装置的传输环节是否正常。本文根据反映采样信息向保护装置传输环节受影响的告警信号，从检修压板告警、软压板告警、SV告警等方面，检查采样信息向保护装置传输环节是否正常，建模如下：

```
TCTR_P1 = ifb(jianxiuyaban==0 &&ruanyanban==0
    &&SV_state==0)
    {TCTR_ready{counter=0}->P1};
```

保护装置在完成采样、保护计算后向智能终端发跳闸命令，需要保护装置状态正常、GOOSE网正常。从保护装置告警与GOOSE网告警两个方面进行检查，具体建模如下：

```
IT= ifb(Protection_state ==0 &&GOOSE_state==0 )
    {str_to_IT{counter=1}->Wait[0]};
```

3.3 保护子功能死锁和保护系统运行阶段检查的建模

利用 RTS 完成基于告警信号的保护功能建模后，在线收集来自各设备的告警信号，对各保护功能进程的工作条件进行检查，对各保护系统各阶段完成情况加以标记，反映各保护系统的完成阶段。运用 PAT 的 RTS，构造各保护子功能进程无死锁(deadlockfree)的断言(#assert)，通过 PAT 的校验(verification)功能进行验证，可得到哪个保护子功能出现问题。对各保护系统的不同运行阶段设置标记，构造各保护系统到达(reaches)不同阶段的断言，验证各保护系统执行到哪个阶段。

以线路差动保护系统的建模为例进行说明：

```
#assertPreProtection_state1 deadlockfree;
```

该语句用于校验保护装置状态是否正常，若正常则输出结果为“VALID”，不正常则为“NOT VALID”。

```
#assert TCTR deadlockfree;
```

该语句用于校验采样环节是否正常，若正常则输出结果为“VALID”，不正常则为“NOT VALID”。

```
#assert IT deadlockfree;
```

该语句用于校验跳闸环节是否正常。

```
#assertReportStrdeadlockfree;
```

该语句用于校验向站控层发报告环节是否正常。

```
#assert TCTR_P1deadlockfree;
```

该语句校验从采样到保护计算环节是否正常。

#define ProtectionError counter == −1;

#assert PreP1 reaches ProtectionError;

以上两个语句用于校验保护装置的出错，先执行进程 PreP1，如果装置异常，即满足宏条件 ProtectionError，则输出结果为“VALID”，表示保护装置出错(阶段标记 counter =−1)，若保护装置正常，则输出结果为“NOT VALID”。

#define PartProcess_TCTR_P1_IT counter == 1;

#assert TCTR_P1_Protocol reaches PartProcess_TCTR_P1_IT;

以上两个语句用于校验保护功能是否达到阶段 1(完成采样、保护计算及跳闸)，先执行进程 TCTR_P1_Protocol，若达到阶段 1，则输出结果为“VALID”，否则为“NOT VALID”。

#define WholeProcess counter== 2;

#assert TCTR_P1_Protocol reaches WholeProcess;

以上两个语句用于校验该保护系统是否达到阶段 2(完成采样、保护计算、跳闸、向站控层发送报告)，若达到阶段 2，则该断言校验的输出结果为“VALID”，否则为“NOT VALID”。

4　算例

基于告警信号运用 PAT 的保护系统交互模型验证的工作流程为首先收集告警信号，然后根据告警信号设置对应条件变量的值，再运用 PAT 的 RTS 模型的校验功能，对基于告警信号与保护工作条件的各保护进程的死锁断言、到达某阶段的断言进行校验，检查各保护子进程是否闭锁，检查线路保护系统的执行阶段。

当保护装置告警信号发出时，将模型中预定义的相应告警信号值设置为“1”，此时利用已建好的模型来检验哪些进程阻塞了，各保护系统执行到哪个阶段。

后面各表中的名称解释如下：

PreSVcaiyang1：表示 SV 网采样状态；TCTR：表示采样环节；IT：表示跳闸环节。Protection：表示保护装置；ReportStr：表示向站控层发送报告。

TCTR_P*i*：表示采样与各保护装置的联合环节。

P*i*(*i*=1、2、3、4)：P1 差动保护、P2 零序保护、P3 距离保护、P4 重合闸。

PreP*i* reaches ProtectionError：保护功能 P*i* 出错的断言；TCTR_P*i*_Protocol reaches PartProcess_TCTR_P*i*_IT：完成保护功能 P*i* 完成采样、保护计算及跳闸操作的断言。LP_System reaches PartProcess_ TCTR_P*i*_IT：表示线路保护中保护功能 P*i* 正常工作的断言。

LP_System reaches WholeProcess：表示线路保护系统完成保护的整个过程的断言。

算例 1：当线路出现故障时，线路保护装置没有发出异常告警信号，则保护装置能够正常切除故障，此时模型中各进程的校验结果如表 1 所示。

表 1　算例 1 的模型校验结果

Table 1 Results of model verification of case 1

目标名称	状态数	耗时/s	校验结果
TCTR	2	0.001 500 5	VALID
Protecton	14	0.000 874	VALID
IT	4	0.001 005 8	VALID
ReportStr	6	0.001 755 9	VALID
TCTR_P*i*(*i*=1,2,3)	16	0.000 900 3	VALID
PreP*i* reaches ProtectionError (*i*=1,2,3,4)	1	0.001 690 2	NOT VALID
TCTR_P*i*_Protocolreaches PartProcess_TCTR_P*i*_IT (*i*=1,2,3,4)	67	0.023 791 1	VALID
LP_System reaches PartProcess_TCTR_P*i*_IT (*i*=1,2,3,4)	71	0.018 324 3	VALID
LP_System reachesWholeProcess	71	0.015 908 6	VALID

从表 1 可看出当故障发生时各保护进程正常执行，校验结果为合法，即检查保护装置自身状态正常，接收故障采样信号、保护计算、向 IT 发出跳闸指令，发送保护动作、跳闸等报告到站控层设备，线路保护系统线程 LP_System 满足条件 WholeProcess=2，断言 LP_System reaches WholeProcess 的检测结果是合法，说明了线路保护装置完成了整个过程。

算例 2：当线路出现故障时，保护装置发出 CT 断线告警时，此时线路保护电流采样异常。各进程校验结果如表 2 所示。

从表 2 可看出，线路保护的某相电流采样异常只影响与电流相关的保护，如差动保护 P1、零序保护 P2、距离保护 P3 等，当 CT 断线时，距离 II 段和 III 段只有 CT 断线那一相无法工作，其它没有断线的两相电流对应的距离保护 II 段和 III 段仍然可正常工作，因此距离保护 P3 可看作正常。针对纵联差动保护，“CT 断线闭锁差动保护控制字”退出时，只闭锁零序差动保护、分相差动保护不闭锁(只是将断线相定值自动抬高，增加 150 ms 延时出口)，因此差动保护正常工作。

表 2 算例 2 的模型校验结果

Table 2 Results of model verification of case 2

目标名称	状态数	耗时/s	校验结果
PreSVcaiyang1	2	0.000 834 2	NOT VALID
TCTR_P1	16	0.000 743 5	VALID
TCTR_P2	1	0.001 743 5	NOT VALID
TCTR_P3	1	0.001 743 5	VALID
PreP1 reaches ProtectionError	5	0.006 431 6	NOT VALID
PreP2 reaches ProtectionError	1	0.001 690 2	VALID
PreP3 reaches ProtectionError	1	0.001 690 2	NOT VALID
PreP4 reaches ProtectionError	5	0.006 431 6	NOT VALID
TCTR_P1_Protocolreaches PartProcess_TCTR_P1_IT	2 586	0.018 324 3	VALID
TCTR_P2_Protocolreaches PartProcess_TCTR_P2_IT	2 586	0.336 092 4	NOT VALID
TCTR_P3_Protocolreaches PartProcess_TCTR_P3_IT	2 586	0.336 092 4	VALID
LP_System reaches PartProcess_P1	1	0.018 324 3	VALID
LP_System reaches PartProcess_P2	1	0.018 324 3	NOT VALID
LP_System reaches PartProcess_P3	1	0.018 324 3	VALID
LP_System reaches PartProcess_P4	1	0.018 324 3	VALID
LP_System reaches WholeProcess	1	0.015 908 6	VALID

合并单元无法将采样值传递给线路零序保护 P2，因此进程 TCTR_P2 的验证结果为“NOT VALID”(死锁)，断言 PreP1 reaches ProtectionError、PreP3 reaches ProtectionError 的验证结果为“NOT VALID”，断言 PreP2 reaches ProtectionError 的验证结果为“VALID”，即线路差动保护 P1、距离保护 P3 正常工作，零序保护 P2 不能正常工作。断言 LP_Systemreaches PartProcess_P1、LP_System reaches PartProcess_P3 的验证结果为“VALID”、LP_System reaches PartProcess_P2 的验证结果为“NOT VALID”。LP_System reaches WholeProcess 的校验结果为“VALID”，表明线路保护系统完整地完成从接收到故障信号到保护跳闸的整个过程，但是有部分保护子功能未能正常工作。

算例 3：当线路发生故障时，保护装置发出 PT 断线告警，此时线路保护电压采样异常。各进程的校验结果如表 3 所示。

从表 3 可看出，PT 断线告警反映保护装置异常，保护装置的校验结果为部分出错，即断言 PreP1reaches ProtectionError 校验结果为“NOT VALID”，表示保护 P1 仍正常工作，同理断言 PreP4 reaches ProtectionError。PT 断线导致线路保护电压采样异常，电压采样异常只影响与电压相关的保护，如线路零序保护 P2、距离保护 P3 等，断言 PreP2 reaches ProtectionError 、PreP3 reaches ProtectionError 的校验结果为“VALID”，表明保护 P2、P3 不能正常工作，P2、P3 无法发出跳闸命令到智能终端 IT，即断言 TCTR_P2_Protocol reaches PartProcess_TCTR_P2_IT 、TCTR_P3_Protocol reaches PartProcess_TCTR_P3_IT 的校验结果为“NOT VALID”，说明线路保护系统没有执行到 P2、P3。

表 3 算例 3 的模型校验结果

Table 3 Results of model verification of case 3

目标名称	状态数	耗时/s	校验结果
ReportStr	6	0.002 989 1	VALID
TCTR_P1	16	0.000 743 5	VALID
TCTR_P2	1	0.001 743 5	NOT VALID
TCTR_P3	1	0.001 743 5	NOT VALID
PreP1 reaches ProtectionError	5	0.006 431 6	NOT VALID
PreP2 reaches ProtectionError	1	0.001 690 2	VALID
PreP3 reaches ProtectionError	1	0.001 690 2	VALID
PreP4 reaches ProtectionError	5	0.006 431 6	NOT VALID
TCTR_P1_Protocolreaches PartProcess_TCTR_P1_IT	71	0.018 324 3	VALID
TCTR_P2_Protocolreaches PartProcess_TCTR_P2_IT	2 586	0.336 092 4	NOT VALID
TCTR_P3_Protocolreaches PartProcess_TCTR_P3_IT	2 586	0.336 092 4	NOT VALID
LP_System reaches PartProcess_P1	71	0.020 324 3	VALID
LP_System reaches PartProcess_P2	1	0.018 324 3	NOT VALID
LP_System reaches PartProcess_P3	1	0.018 324 3	NOT VALID
LP_System reaches PartProcess_P4	71	0.020 324 3	VALID
LP_System reaches WholeProcess	71	0.025 908 6	VALID

线路保护系统完成各保护子功能的断言 LP_System reaches PartProcess_P1 、LP_System reaches PartProcess_P4 的校验结果为“VALID”(合法)，说明线路保护系统执行到 P1、P4。

整个线路保护系统完整执行的断言 LP_System reaches WholeProcess 的校验结果为“VALID”，表明整个线路保护系统仍然完整地执行了从接收故障信号到保护跳闸的整个过程，尽管有部分保护子功能失效。

从 3 个算例可看到，与文献[17-19]的建模工作相比，本文建立的各保护子功能的子进程模型更为严谨，为它们增加了工作条件及其检查，并与告警

信号进行挂钩，还增加了各保护系统执行阶段的检查，能够验证各失效因素作用下各保护系统的完成度、可达性。

5　结论

本文研究了一种基于 PAT 包含告警信号的智能变电站保护信息交互建模与验证方法。利用进程仿真工具包 PAT 建立了各保护系统的各子功能进程，将保护功能故障树中叶子节点对应的告警信号与各进程的工作条件建立关联；建立了保护装置、合并单元、智能终端等之间交互模型，构造了各保护子功能进程死锁与保护系统运行阶段的断言，对各告警信号下的保护系统执行情况进行校验。多个仿真算例验证了本文方法的有效性。本文的工作为在线获得智能变电站各保护的可靠运行情况提供了有力的技术支持，具有一定的工程借鉴和实用性。

参考文献

[1] IEC. IEC 61850[S]. 2004.

[2] 韩小涛, 聂一雄, 尹项根. 基于 OPNET 的变电站二次回路通信系统仿真研究[J]. 电网技术, 2005, 29(6): 67-71.
HAN Xiaotao, NIE Yixiong, YIN Xianggen. Research on substation secondary circuit communication system using OPNET simulator[J]. Power System Technology, 2005, 29(6): 67-71.

[3] 曹海欧, 严国平, 徐宁, 等. 数字化变电站 GOOSE 组网方案[J]. 电力自动化设备, 2011, 31(4): 143-150.
CAO Haiou, YAN Ouping, XU Ning, et al. GOOSE network scheme for digital substation[J]. Electric Power Automation Equipment, 2011, 31(4):143-150.

[4] 高磊, 卜强生, 袁宇波, 等. 基于二次回路比对的智能变电站调试及安全措施[J]. 电力系统自动化, 2015, 39(20): 130-134.
GAO Lei, BU Qiangsheng, YUAN Yubo, et al. Smart substation commissioning and safety measures based on secondary circuit comparison[J]. Automation of Electric Power Systems, 2015, 39(20): 130-134.

[5] 刘昊昱, 左群业, 张保善. 智能变电站过程层网络性能测试与分析[J]. 电力系统保护与控制, 2012, 40(18): 112-116.
LIU Haoyu, ZUO Qunye, ZHANG Baoshan. Process level network performance testing and analysis in smart substation[J]. Power System Protection and Control, 2012, 40(18): 112-116.

[6] 方晓洁, 季夏秩, 卢志刚. 基于 OPNET 的数字化变电站继电保护通信网络仿真研究[J]. 电力系统保护与控制, 2010, 38(23): 137-140.
FANG Xiaojie, JI Xiayi, LU Zhigang. Study on relaying protection communication network in digital substation using OPNET simulation[J]. Power System Protection and Control, 2010, 38(23): 137-140.

[7] 张巧霞, 贾华伟, 叶海明, 等. 智能变电站虚拟二次回路监视方案设计及应用[J]. 电力系统保护与控制, 2015, 43(10): 123-128.
ZHANG Qiaoxia, JIA Huawei, YE Haiming, et al. Design and application of virtual secondary circuit monitoring in smart substation[J]. Power System Protection and Control, 2015, 43(10): 123-128.

[8] 李忠安, 王娇, 张惠刚, 等. IEC 61850 过程层网络通信分析诊断工具设计[J]. 电力系统保护与控制, 2015, 43(1): 93-97.
LI Zhongan, WANG Jiao, ZHANG Huigang, et al. Design of process layer network communication fault diagnosis and analysis tool based on IEC 61850[J]. Power System Protection and Control, 2015, 43(1): 93-97.

[9] 彭少博, 郑永康, 周波, 等. 220 kV 智能变电站检修二次安措优化研究[J]. 电力系统保护与控制, 2014, 42(23): 143-148.
PENG Shaobo, ZHENG Yongkang, ZHOU Bo, et al. Study of optimization of secondary safety measures of 220 kV smart substation maintenance[J]. Power System Protection and Control, 2014, 42(23): 143-148.

[10] 李鹏, 卫星, 郭利军, 等. 智能变电站继电保护运维防误技术研究及应用[J]. 电力系统保护与控制, 2017, 45(19): 123-129.
LI Peng, WEI Xing, GUO Lijun, et al. Study and application of relay protection maintenance anti-misoperation technology in smart substation[J]. Power System Protection and Control, 2017, 45(19): 123-129.

[11] HUANG H, KIRCHNER H. Formal specification and verification of modular security policy based on colored Petri nets[J]. IEEE Trans. on Dependable and Secure Computing, 2011, 8(6): 852-865.

[12] LEI H, SINGH C, SPRINTSON A. Reliability modeling and analysis of IEC 61850 based substation protection systems[J]. IEEE Transactions on Smart Grid, 2014, 5(5): 2194-2202.

[13] 耿治, 张建忠, 陈昊. 智能变电站保护装置自动测试

系统分析与设计[J]. 电力系统保护与控制, 2017, 45(11): 121-125.
GENG Zhi, ZHANG Jianzhong, CHEN Hao. Research and design of automatic test system for protection device in intelligent substation[J]. Power System Protection and Control, 2017, 45(11): 121-125.

[14] 高翔, 杨漪俊, 姜健宁, 等. 基于 SCD 的二次回路监测主要技术方案介绍与分析[J]. 电力系统保护与控制, 2014, 42(15): 149-154.
GAO Xiang, YANG Yijun, JIANG Jianning, et al. Analysis of secondary circuit monitoring methods based on SCD[J]. Power System Protection and Control, 2014, 42(15): 149-154.

[15] 韩小涛, 尹项根, 张哲. 故障树分析法在变电站通信系统可靠性分析中的应用[J]. 电网技术, 2004, 28(1): 56-59.
HAN Xiaotao, YIN Xianggen, ZHANG Zhe. Application of fault tree analysis method in reliability analysis of substation communication system[J]. Power System Technology, 2004, 28(1): 56-59.

[16] 许宗光, 文继锋, 李彦, 等. 一种基于数据冗余校验的数字化变电站继电保护装置防误方法[J]. 电力系统保护与控制, 2018, 46(5): 166-170.
XU Zongguang, WEN Jifeng, LI Yan, et al. An anti-maloperation method based on redundancy data check for relay protection devices in digital substations[J]. Power System Protection and Control, 2018, 46(5): 166-170.

[17] 童晓阳, 李映川, 章力, 等. 基于 IEC 61850 的保护功能交互模型[J]. 电力系统自动化, 2008, 32(21): 41-45.
TONG Xiaoyang, LI Yingchuan, ZHANG Li, et al. Interaction model of protection functions based on IEC 61850[J]. Automation of Electric Power Systems, 2008, 32(21): 41-45.

[18] HUANG H, KIRCHNER H. Formal specification and verification of modular security policy based on colored Petri nets[J]. IEEE Transactions on Dependable and Secure Computing, 2011, 8(6): 852-865.

[19] 张其林, 王先培, 杜双育, 等. 基于 IEC 61850 的智能电子设备交互模型形式化描述与验证[J]. 电力系统自动化, 2012, 36(17): 72-76.
ZHANG Qilin, WANG Xianpei, DU Shuangyu, et al. Formal specification and verification of intelligent electronic device interaction model based on IEC61850[J]. Automation of Electric Power Systems, 2012, 36(17): 72-76.

[20] PAT: process analysis toolkit[EB/OL]. [2011-07-21]. http:// www.comp.nus.edu.sg/~pat/.

收稿日期：2018-08-02； 修回日期：2018-09-26

作者简介：

王洪彬(1984—)，男，硕士，工程师，研究方向为智能变电站继电保护技术；E-mail: whbleehomwhb@163.com

张友强(1981—)，男，硕士，高级工程师，主要研究方向为继电保护状态评估；E-mail: zyq113528@126.com

童晓阳(1970—)，男，通信作者，博士，副教授，博士生导师，主要研究方向为电网故障诊断、广域后备保护、智能变电站。E-mail: xytong@swjtu.cn

(编辑 张爱琴)