数字化变电站的分布式联锁功能安全性研究

辛建波,上官帖
(江西省电力科学研究院,江西 南昌 330006)

摘要:针对现有定性评价分布式联锁功能安全性方法的不足,应用马尔科夫模型理论,提出了定量分析数字化变电站分布式联锁功能安全性的方法。研究了分布式联锁功能的实现过程;分析了联锁信息的传输特性,建立了导致联锁信息传输时延不确定的永久失效和瞬时失效模型,以及联锁信息的重传和延迟模型;引入安全综合等级,根据分布式联锁功能的工作特点,应用马尔科夫模型理论,综合考虑了永久失效和瞬时失效模式,建立了评价分布式联锁功能安全性的马尔科夫模型,推导出了求解功能安全综合等级的解析表达式。并以一实际分布式联锁功能为例,得到了联锁功能的状态概率和安全性指标,以及合理的联锁信息传输方案可提高联锁功能安全性等结论。

关键词:数字化变电站;分布式联锁功能;时延不确定;马尔科夫模型;安全性评估
中图分类号:TM 76;TP 393.08 **文献标识码**:A **文章编号**:1006-6047(2007)06-0099-05

以太网技术、IEC 61850 标准[1]的发展及其在变电站自动化系统中广泛应用,为实现 IEC 61850 标准支撑的全数字化变电站提供了有力的支持。近年来,对数字化变电站的应用功能[2]、信息传输方法[3]、体系结构[4-5]、通信实现[6-7]等进行了较多研究,然而对分布式功能的安全性研究则较少。

在数字化变电站中,分布式联锁功能采用分布式模式实现[1],即通过网络交换分布在多个物理设备中的不同逻辑节点间的联锁信息,并使用这些信息进行正确协同操作来实现。但是,分布式联锁功能对通信系统的依赖性较强,通信网络信息传输的时延不确定性有可能降低分布式联锁功能的安全性[8]。为此,有必要在实际应用前,对数字化变电站分布式联锁功能的安全性进行认真研究。

考虑到数字化变电站分布式联锁功能的工作过程为马尔科夫随机过程,采用马尔科夫模型法(Markov 法)对其安全性进行定量分析,得到了联锁功能安全性的量化指标。

1 数字化变电站的分布式联锁功能实现

1.1 分布式联锁功能对应的逻辑节点

数字化变电站的分布式联锁主要包括以下几方面功能[1]:联锁逻辑处理、开关控制(控制断路器、隔离刀闸和接地刀闸的分/合)、人机接口(功能配置、开关操作)等功能。以上功能被抽象成多个逻辑节点(LN)的集合:变电站层的操作员访问(LN IHMI)、告警事件处理(LN CALH)、间隔层的开关控制(LN CSWI)和联锁逻辑(LN CILO)、过程层的断路器(LN XCBR)和所有不能断开短路电流的开关(LN XSWI)。考虑可用性和性能要求等因素,将以上逻辑节点分配到 7 个物理设备中:变电站层的监控主机(IED1)、间隔层的控制器(IED2 和 IED3)、过程层的智能断路器(IED4 和 IED6)和智能开关(IED5 和 IED7)。分布式联锁功能主要由位于不同物理设备中的若干 LN 通过网络(包括过程层和变电站层网络)传输开关位置变化信息(简称为联锁信息)协调完成,如图 1 所示。实际应用中,变电站层网络通常采用环型拓扑结构,而过程层网络则采用星型结构。

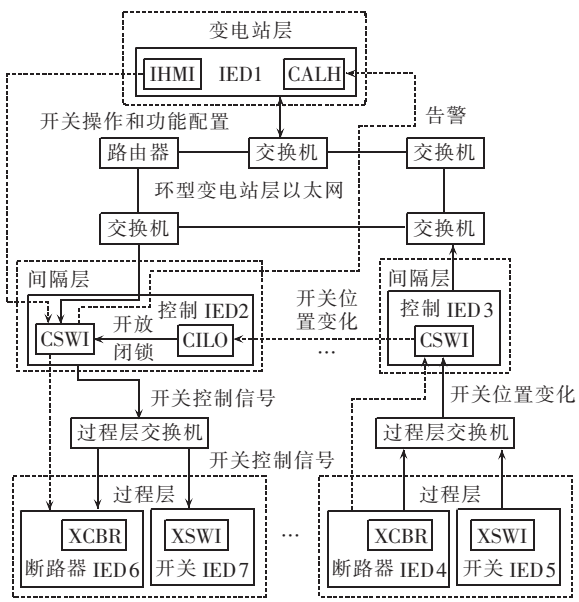

图 1 分布式联锁功能对应的逻辑节点

Fig.1 Logical nodes of distributed interlock function

1.2 分布式联锁功能的实现流程

分布式联锁功能主要分 4 步实现。

a. 在功能执行前,需要进行功能配置,即通过变

收稿日期:2006-09-13;修回日期:2007-01-15

电站层IED1内的IHMI建立不同间隔控制器间的通信关系对应表和每个间隔控制器对应各种操作的联锁逻辑规则库。

b. 正常情况下,间隔层IED2内的CSWI处理所有来自变电站层IED1内的IHMI发送的开关操作命令,校核命令权限,监视命令执行,并且当命令非正常结束时,向变电站层IED1的CALH发送告警信号。

c. 若影响联锁功能的开关设备(断路器、隔离刀闸、接地刀闸)的位置改变,过程层断路器IED4内的XCBR或智能开关IED5内的XSWI将开关位变化信息通过过程层网络传送至间隔层IED3内的CSWI,然后CSWI通过变电站层网络将此信息传送至间隔层IED2内的CILO。

d. 间隔控制单元IED2内的CILO接收到与联锁相关的开关位置变化信息后,进行联锁逻辑运算,确定该操作是否合法、安全;然后,CILO将允许或禁止(开放或闭锁)需要执行的开关操作结果传送给同一物理设备的CSWI。若允许控制,CSWI发送控制命令给过程层断路器IED6内的XCBR或智能开关IED7内的开关(XCWI);若发生不合法操作,立即闭锁该操作,撤消控制命令输出,并且发送告警到变电站层IED1的CALH。

由以上分析可知,分布式联锁功能具有实时性强、维护简便、扩充方便等优点。但是,该功能对网络依赖性较大,LN间只有通过网络协同工作才能保证功能的稳定运行,其实现在很大程度上取决于网络为联锁信息传输提供服务的性能。

2 联锁信息传输时延不确定性分析

2.1 导致信息传输时延不确定性的网络失效率模型

在联锁信息传输过程中总是存在时延不确定性,不确定性主要是网络失效造成的。按失效持续时间分,网络失效通常分为永久性和瞬时性2类。永久性失效大多由网络硬件设备故障引起,它的持续时间很长,例如,链路中断或网络节点故障等。瞬时性网络失效的发生大多是随机的,它的持续时间很短,这种故障发生时,设备还能继续提供服务,但服务响应时间可能延长,例如电磁干扰、软件故障、网络拥塞等。永久性失效和瞬时性失效间关系见图2。

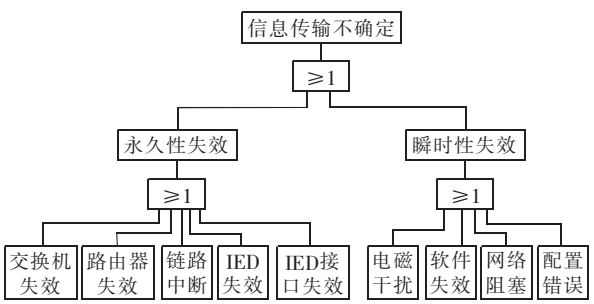

图 2 分布式联锁功能的故障树

Fig.2 Fault tree of distributed interlock function

永久失效率λ_{PF}的计算公式为

$$\lambda_{PF}=N\lambda_{SW}+\lambda_{RT}+M\lambda_{LK}+Q(\lambda_{IED}+\lambda_{IF}) \quad (1)$$

式中 λ_{SW}为交换机的失效率;λ_{RT}为路由器的失效率;λ_{LK}为链路的失效率;λ_{IED}为IED的失效率;λ_{IF}为网络接口的失效率;N和M分别表示交换机和链路数;Q为与联锁功能有关的IED数。

瞬时失效率λ_{TF}由下式确定:

$$\lambda_{TF}=\lambda_{EMI}+\lambda_{ST}+\lambda_{ZS}+\lambda_{CF} \quad (2)$$

式中 λ_{EMI}为电磁干扰导致的瞬时失效率;λ_{ST}为应用层软件故障导致的瞬时失效率;λ_{ZS}为网络阻塞导致的瞬时失效率;λ_{CF}为功能配置错误导致的瞬时失效率。

λ_{ZS}主要取决于网络负载,λ_{CF}与功能实现的复杂程度和涉及的设备数有关。λ_{EMI}计算如下:

$$\lambda_{EMI}=3600\times f_w R_{UB} \quad (3)$$

式中 f_w为每秒传输的帧数,$f_w=1/t_{end}$,t_{end}为下文定义的端到端延迟;R_{UB}为误帧率[9],$R_{UB}=1-(1-\varepsilon)^{L_f}$,$\varepsilon$为误比特率,$L_f$为帧长(bit)。

λ_{ST}可用Logarithmic exponential模型[10]确定,即

$$\lambda_{ST}=\lambda_0 e^{-\theta u} \quad (4)$$

式中 λ_0为初始失效率;θ为失效减少率系数;u为系统运行中累计发现的错误。

于是,永久失效占总失效的比例因子α可由以下公式确定:

$$\alpha=\lambda_{PF}/\lambda_{NET} \quad (5)$$

式中 λ_{NET}为总失效率($\lambda_{NET}=\lambda_{PF}+\lambda_{TF}$)。

2.2 联锁信息的重传模型

在IEC 61850中,联锁信息采用基于分布者/订阅者通信机制的面向系统范围事件的通用对象(GOOSE)服务模型实现。GOOSE传输模型中,发布者和订阅者之间的通信采用独立于网络和通信协议的抽象通信服务接口(ASCI),它必须通过特殊通信服务映射(SCSM)方法映射到具体的通信协议和通信网络上。由于联锁信息传输的高实时性和可靠性要求,为避免在协议栈延时,报文将直接映射到以太网的数据链路层,并分别在媒体访问控制(MAC)层和应用层采取32位CRC校验和组播方式按节律传输或重传。

为了满足联锁信息传输的实时性,需要减少重传次数,但又降低了信息传输的可靠性;重传次数增加可提高可靠性,但可能实时性要求达不到,因此满足信息传输的实时性和可靠性是相矛盾的。此外,为了保证实时性,重传间隔时间必须足够小,如果这个值太小,不仅会浪费网络容量,而且会影响其他数据传输。为此,这里建立了以下重传模型:

$$t_{rt}=t_{rt}^{min}\times 2^{R-1} \quad (6)$$

式中 R为重传次数;t_{rt}为第1次发布信息后的重传间隔时间;t_{rt}^{min}为最小重传间隔。

t_{rt}^{min}可选一个略大于网络延迟t_{net}与逻辑处理延

迟 t_{sub} 之和的值。另外，为监视设备健康状态，即使开关状态没有改变，也应以最大重传间隔 t_{rt}^{max} 为周期定期发送报文。

2.3 联锁信息传输的端到端延迟模型

在分布式联锁功能中，联锁信息的端到端延迟是指从过程层某个开关设备的位置发生改变的时刻起，到执行联锁逻辑的 IED 接收到开关位置止，所经历的时间，主要由开关位置变化检测延迟 t_{event}、发布 IED 的处理延迟 t_{pub}、网络延迟 t_{net} 和订阅 IED 的联锁逻辑处理延迟 t_{sub} 4 部分构成，即

$$t_{end}=t_{event}+t_{pub}+t_{net}+t_{sub} \tag{7}$$

式中 t_{event} 与过程层网络和开关 IED 的处理性能有关，对于采用星型结构的过程层网络，网络产生的延迟很小，t_{event} 主要取决于 IED 的处理性能，通常小于 5 ms；而 t_{pub} 和 t_{sub} 主要与 IED 所采用的操作系统、协议编/解码算法、CPU 的调度和协议栈、排队延迟、中断处理有关，通常小于 5 ms。

t_{net} 与报文经过的交换机和链路的数目、交换机的处理速度、报文的长度、网络负荷情况、链路传输速率及所采用的协议有关。假定联锁信息从一个逻辑节点传输到另一个逻辑节点需要经过 j 个交换机和 k 条链路，则有

$$t_{net}=\sum_{i=1}^{j}(t_{frame}+t_{switch})+\sum_{i=1}^{k}t_{prop} \tag{8}$$

式中，t_{frame} 表示将帧中所有位都发出的时间，主要取决于帧的长度和以太网的通信速率。它可以定义为 $t_{frame}=L_{frame}/C$，其中 L_{frame} 表示帧长度（单位是 bit），C 表示链路的数据率，单位是 bit/s。

t_{switch} 表示交换机的处理时延，即转发接收到的报文所需要的处理时间。它由交换时延 t_{mux} 和排队时延 t_{queue} 2 部分组成，即：$t_{switch}=t_{mux}+t_{queue}$；其中，$t_{mux}$ 基本固定，典型值为 45 μs；而 t_{queue} 随网络拥塞状况和竞争流量数而异，通常由保证服务的调度策略决定。

t_{prop} 表示一个数据位从发送方到达接收方所需的时间，取决于距离和链路传输介质，与带宽无关。它可以定义为 $t_{prop}=D_{link}/v$；其中，D_{link} 表示链路的距离；v 表示信号沿链路传播的速度，典型的铜媒体和光纤是光速的 0.67 倍。对于 100 m 范围内的变电站网络，传播延迟很小，即 t_{prop} 趋近于零。

间隔 IED 通过过程层网络向智能开关发送的开关控制信号的延迟 t_{tran} 可采用上述类似的方法得到。

3 分布式联锁功能安全性研究

3.1 分布式联锁功能安全性的评价指标

对于直接关系人身和大宗财产的安全相关功能，安全性是衡量其性能的重要指标。功能安全性是指在系统出现故障时，防止功能处于潜在危险或不安全状态的能力[11]。2002 年发布的 IEC 61508[11] 标准引入了“安全综合等级”SIL（Safety Integrity Level）的概念，对所有与安全相关的电子/电气/电子可编程序控制器系统的功能安全性设计和评价进行了规范，并且针对不同等级的 SIL 规定了不同的故障概率，具体指标如表 1 所示。

表 1 安全度等级的划分

Tab.1 Safety integrity levels

SIL	按要求模式 平均失效概率	连续模式 每小时失效概率
4	$\geqslant 10^{-5}\sim<10^{-4}$	$\geqslant 10^{-9}\sim<10^{-8}$
3	$\geqslant 10^{-4}\sim<10^{-3}$	$\geqslant 10^{-8}\sim<10^{-7}$
2	$\geqslant 10^{-3}\sim<10^{-2}$	$\geqslant 10^{-7}\sim<10^{-6}$
1	$\geqslant 10^{-2}\sim<10^{-1}$	$\geqslant 10^{-6}\sim<10^{-5}$

分布式联锁功能的行为直接关系电网、设备及人员的安全，是一种典型的按要求模式执行的安全相关功能，因此，采用 PFD（Probability of Failure on Demand）衡量该功能的安全性，PFD 定义为

$$PFD=p_i \tag{9}$$

式中 p_i 为功能处于不安全状态的稳态概率。

3.2 马尔科夫模型法简介

目前，常用的求取安全性指标的方法主要有模拟法和解析法 2 大类。模拟法不受系统规模的限制，但耗时多、准确度不高，在安全性评估中较少应用。解析法又可分为网络法和模型法 2 类。网络法以系统的拓扑结构为基础，包括故障树、事件树等算法。由于马尔科夫具有简单明了、物理概念清晰、可获得系统安全度的解析表达式等特点，因此是一种优先模型法[12]。马尔科夫随机模型法[13]是由苏联数学家 Markov 所提出和研究的一类随机模型，该模型具有马尔可夫性，也称为无后效性，即在已知系统现在所处的状态下，系统将来的演变与过去无关。按其状态空间和时间参数是离散或连续的可以分为 4 种类型：离散状态空间/离散时间参数、连续状态空间/连续时间参数、离散状态空间/连续时间参数、连续状态空间/离散时间参数。

马尔科夫模型法分析功能安全性问题的基本步骤是：首先列举系统的状态空间，根据各状态的关系建立状态转移模型；然后求解马尔科夫状态方程，计算各状态的平稳概率；最后得到安全性指标。

3.3 分布式联锁功能安全性研究

当开关位置发生变化、通信失效或重新修复后，分布式联锁功能将从一个状态转移到另一个状态。下一步的运行状态完全由当前状态决定，而与如何进入当前状态无关，即具有无后效性；由于发生故障是随机的，且电力网络、通信网络和 IED 故障之间又相互独立，可以认为故障发生的概率服从泊松分布。由此可知，分布式联锁功能的工作过程可采用时间连续、状态空间离散的连续时间 Markov 链 CTMC（Continuous Time Markov Chain）描述。计及永久失效和瞬时失效模式的分布式联锁功能的 CTMC 模型，如图 3 所示。

图 3 中的 S_1、S_2、S_3 表示分布式联锁功能所处的状态。

S_1 为正常操作状态，从 HMI 发送开关操作命令

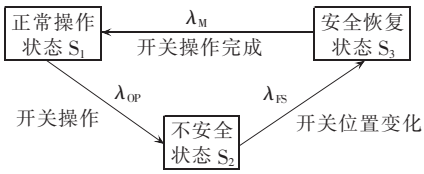

图 3 分布式联锁功能的 CTMC 模型

Fig.3 CTMC model of distributed interlock function

开始,到 CSWI 接收到操作命令为止,等价于执行 CSWI 的开关控制功能。

S_2 为不安全操作状态,开关位置发生变化开始,到进行开关操作的 IED 接收到状态变化为止的一段时间,由于 CILO 的联锁逻辑使用过时的数据,使联锁功能处于不安全状态。

S_3 为恢复安全操作状态,开关操作的 IED 接收到开关位置变化信息,并经过联锁逻辑判断和开关操作后的安全状态。

图 3 中各状态间带箭头的连线,表示在执行的操作或事件驱动下,由一个状态转移到另一个状态。当开关位置变化时,S_1 进入 S_2 的状态转移率为 λ_{OP},其大小可用开关操作率(单位时间的开关操作次数)衡量。

$$\lambda_{OP}=N_{SW}/(24\times60\times60) \tag{10}$$

式中 N_{SW}为变电站每天操作开关的次数。

当进行开关操作的 IED 接收到开关位置变化信息时,S_2 转移到 S_3 的状态转移率为 λ_{FS},其大小与 α、R、t_{end}、t_{rt}、t_{rt}^{max}有关,其表达式为

$$\lambda_{FS}=(1-\alpha)\times\frac{1000}{t_{end}+\sum_{R=1}^{R}t_{rt}}+\alpha\times\frac{1000}{t_{rt}^{max}} \tag{11}$$

当开关操作完成时,S_3 回到 S_1 的状态转移率为 λ_M,其大小取决于开关动作信号的网络传输时延 t_{tran} 和开关的机械性能 t_{run},其表达式为

$$\lambda_M=1000/(t_{tran}+t_{run}) \tag{12}$$

利用图 3 所示的 CTMC 模型,可以计算出处于各个状态的稳态概率。此 CTMC 的转移率矩阵为

$$\boldsymbol{Q}=\begin{bmatrix}-\lambda_{OP} & \lambda_{OP} & 0\\ 0 & -\lambda_{FS} & \lambda_{FS}\\ \lambda_M & 0 & \lambda_M\end{bmatrix} \tag{13}$$

假设图 3 中 3 个状态的驻留稳态概率矩阵为

$$\boldsymbol{\Pi}=[\pi_0\ \pi_1\ \pi_2]$$

$\boldsymbol{\Pi}$ 必须满足条件

$$\sum_{j=0}^{2}\pi_j=1 \tag{14}$$

因为

$$\boldsymbol{\Pi}\times\boldsymbol{Q}=0 \tag{15}$$

由以上 2 式,可得下面方程组:

$$\begin{aligned}&-\pi_0\lambda_{OP}+\pi_2\lambda_M=0,\ \pi_0\lambda_{OP}-\pi_1\lambda_{FS}=0\\&\pi_1\lambda_{FS}-\pi_2\lambda_M=0,\ \pi_0+\pi_1+\pi_2=1\end{aligned} \tag{16}$$

由式(16)得功能处于不同状态的稳态概率,即

$$\pi_0=\lambda_{FS}\lambda_M/(\lambda_{OP}\lambda_{FS}+\lambda_{OP}\lambda_M+\lambda_{FS}\lambda_M)$$
$$\pi_1=\lambda_{OP}\lambda_M/(\lambda_{OP}\lambda_{FS}+\lambda_{OP}\lambda_M+\lambda_{FS}\lambda_M)$$
$$\pi_2=\lambda_{FS}\lambda_{OP}/(\lambda_{OP}\lambda_{FS}+\lambda_{OP}\lambda_M+\lambda_{FS}\lambda_M)$$

系统功能处于不安全状态的概率为 π_1,由式(9)可得分布式联锁功能的 PFD 为

$$PFD=\pi_1 \tag{17}$$

4 算例分析

以一实际分布式联锁功能为例进行安全性评估。该功能由 2 台间隔层 IED 和 1 台过程层 IED 通过变电站层通信网络和过程层网络交换联锁信息实现,其中变电站层网络由 10 台交换机和 1 台路由器采用环型拓扑结构串接构成,过程层网络采用星型结构,所有通信链路采用光纤 100 Mbit/s 链路。以上假设可知,$M=11$,$N=11$,$Q=3$,$C=100$ Mbit/s。在求解安全性指标时需要作 6 点说明。

a. 根据设备厂商提供的数据[14]可得各种网络设备的失效率如表2 所示。

表 2 永久失效率计算结果

Tab.2 Calculated permanent failure rates 次/h

λ_{SW}	λ_{RT}	λ_{IK}	λ_{IED}	λ_{IF}
42×10^{-6}	577×10^{-6}	100×10^{-6}	55×10^{-6}	285×10^{-6}

b. 假设联锁信息的报文长度为以太网的最长帧 $L_f=1518$ 字节;报文重传次数 $R=3$;$t_{rt}^{min}=10$ ms;网络阻塞失效率 $\lambda_{ZS}=120\times10^{-6}$ 次/h,功能配置失效率 $\lambda_{CF}=100\times10^{-6}$ 次/h。

c. 由式(7)得端到端延迟 $t_{end}=16.831$ ms;光纤链路的误码率[9] $\varepsilon=3\times10^{-12}$;$f_w=60$/帧;由式(3)得电磁干扰失效率 $\lambda_{EMI}=7\,869\times10^{-6}$次/h;由软件失效率数据[15],取 $\lambda_0=120\times10^{-6}$次/h,调试中发现错误数 $u=22$,失效减少率系数 $\theta=0.126$,根据式(4)得软件失效率 $\lambda_{ST}=7.5044\times10^{-6}$次/h。

d. 由式(1)和(2)分别得永久失效率 $\lambda_{PF}=3\,159\times10^{-6}$次/h,瞬时失效率 $\lambda_{TF}=8\,096.81\times10^{-6}$次/h,永久失效占总失效的比例因子 $\alpha=0.281$。

e. IEC 61850 中规定自操作人员发出命令至开关开始变位的时间应小于 1000 ms,于是,定期重传间隔时间 $t_{rt}^{max}=1\,000$ ms;根据现场运行经验 $N_{SW}=10$ 次;对于高压开关[16] $t_{run}=20$ ms。

f. 由表 2、3 及式(10)~(12)(17)得状态转移率及联锁功能的 PFD,如表 3 所示。

表 3 安全性评估结果

Tab.3 Assessed SIL 次/h

λ_{OP}	λ_{FS}	λ_M	PFD
1.157×10^{-4}	8.561	39.74	1.357×10^{-5}

由表 3 可知,分布式联锁功能的 PFD 在 $10^{-5}\leqslant PFD\leqslant10^{-4}$ 之内。由表 1 可知,该功能的安全级别为 SIL 4 级,符合高安全性的要求。需要说明的是,本案例分布式联锁功能的高安全性,其关键在于端到端延迟较小,联锁信息重传 3 次后正确收到。

5 结论

对数字化变电站的分布式联锁功能的安全性进

行了系统的研究,建立了导致时延不确定性的永久和瞬时失效模型,基于 Markov 模型方法,定量评价了时延不确定性对分布式联锁功能安全性的影响。该研究为分布式联锁功能的设计和选择,构建满足该功能的数字化变电站提供了重要的理论依据。

参考文献:

[1] IEC. IEC 61850 Communication networks and systems in substations: part 1~10[S].[S.l.]:IEC,2002.

[2] ALLEN D E,APOSTOLOV A,KREISS D G. Automated analysis of power system events[J]. IEEE Power and Energy Magazine, 2005,3(5):48-55.

[3] 辛建波,段献忠. 基于优先级标签的变电站过程层交换式以太网的信息传输方案[J]. 电网技术,2004,28(22):26-30,47.
XIN Jian-bo,DUAN Xian-zhong. A transfer scheme based on priority-tag in switched Ethernet for substation process-level [J]. Power System Technology,2004,28(22):26-30,47.

[4] 吴在军,胡敏强. 基于 IEC 61850 标准的变电站自动化系统研究[J]. 电网技术,2003,27(10):61-65.
WU Zai-jun,HU Min-qiang. Research on a substation automation system based on IEC 61850[J]. Power System Technology,2003,27(10):61-65.

[5] 徐礼葆,刘宝志,郝燕丽. 开放式数字化变电站自动化系统的讨论[J]. 继电器,2004,32(6):40-44.
XU Li-bao,LIU Bao-zhi,HAO Yan-li. The discussion of open type transformer substation automation system[J]. Relay,2004, 32(6):40-44.

[6] 殷志良,刘万顺,杨奇逊,等. 基于 IEC 61850 标准的过程总线通信研究与实现[J]. 中国电机工程学报,2005,25(8):86-91.
YIN Zhi-liang,LIU Wan-shun,YANG Qi-xun,et al. Research and implementation of the communication of process based on IEC 61850[J]. Proceedings of the CSEE,2005,25(8):86-91.

[7] 高鹏宇,游大海,刘国民. 符合 IEC 61850 标准的数字化变电站内部通信的实现[J]. 继电器,2006,34(12):69-72.
GAO Peng-yu,YOU Da-hai,LIU Guo-min. Implement of communications according to IEC 61850 in the digital substation [J]. Relay,2006,34 (12):69-72.

[8] BRAND K P,OSTARTAG M,WIMMER W. Safety related,distributed functions in substations and the standard IEC 61850[C]//IEEE Bologna Power Tech Conference. Bologna,Italy:[s.n.], 2003:315-319.

[9] STALLINGS W. High-speed networks and internet:performance and quality of service[M]. 2nd ed. New York:Pearson Education,2002.

[10] BOWLES J B. A combined hardware, software and usage model of network reliability and availability[C]//Proceeding of Ninth Annual International Phoenix Conference on Computers and Communications. Arizona:[s.n.],1990:649-654.

[11] IEC. IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems[S]. Geneva, Switzerland:International Electrotechnical Commission,2002.

[12] ROUVROYE J L,BROMBACHER A C. New quantitative safety standards:different techniques,different results?[J]. Reliability Engineering and System Safety,1999,28(9):121-125.

[13] 毛用才,胡奇英. 随机过程[M]. 西安:西安电子科技大学出版社,2000.

[14] SCHEER G W,DOLEZILEK D J. Comparing the reliability of Ethernet network topologies in substation control and monitoring networks[C]//Western Power Delivery Automation Conference. Spokane,Washington:[s.n.],2000:4-12.

[15] 王钢,丁茂生,李晓华,等. 数字继电保护装置可靠性研究[J]. 中国电机工程学报,2004,24(7):47-52.
WANG Gang,DING Mao-sheng,LI Xiao-hua,et al. Reliability analysis of digital protection[J]. Proceedings of the CSEE, 2004,24(7):47-52.

[16] 丁凡,路甬祥. 新型 500 kV 超高压断路器液压操动机构的研究[J]. 中国机械工程,1998,9(6):50-52.
DING Fan,LU Yong-xiang. Research on the 500 kV super high voltages breaker of hydraulic pressure operate machine[J]. China Mechanical Engineering,1998,9(6):50-52.

(**责任编辑**:汪仪珍)

作者简介:

辛建波

辛建波(1970-),男,江西万载人,工程师,博士,主要从事数字化变电站、电能质量和电网动态稳定性等方面的科研工作(**E-mail**:mandyzhuhai@163.com);

上官帖(1958-),男,江西鹰潭人,教授级高级工程师,主要从事继电保护及安全自动装置的技术工作。

Safety of distributed interlock function in digital substation

XIN Jian-bo,SHANGGUAN Tie

(Jiangxi Electric Power Research Institute,Nanchang 330006,China)

Abstract: Based on Markov model theory,a quantitative analysis method is proposed to assess the safety of distributed interlock function of digital substation as a supplement to the qualitative methods. The implementation process of the distributed interlock function and the transmission characteristic of the interlock information are analyzed. The models of permanent and instantaneous failures,which bring the indeterminable delay in interlock information transmission,and the models of repeating interlock information transmission and delay are set up. Based on these models,a model using SIL(Safety Integrity Level) to assess the distributed interlock function is established and its analytic expression is deduced. The state probability and SIL of a case are calculated as an example,showing that the rational transmission scheme of interlock information can improve its safety.

Key words: digital substation; distributed interlock function; indeterminable delay; Markov model; safety assessment