基于状态事件故障树的信息物理融合系统风险建模

徐丙凤[1] 何高峰[2] 张黎宁[1]
(南京林业大学信息科学技术学院 南京 210037)[1] (南京邮电大学物联网学院 南京 210003)[2]

摘 要 信息物理融合系统(Cyber-physical Systems)中嵌入式系统网络的应用使其容易遭受网络攻击,攻击者可能会利用软件和通信组件中的漏洞获取系统的控制权,从而导致系统失效。现有的信息物理融合系统安全风险建模方法主要基于静态故障树进行,不考虑软件控制系统特有的动态性和时序依赖性,无法推导出网络攻击所导致的最终影响。因此,文中基于状态事件故障树提出一种信息物理融合系统风险建模方法。首先,针对状态事件故障树(Stata/Event Fault Trees,SEFTs)模型进行攻击步骤集成,提出 Attack-SEFTs 模型;在此基础上,给出信息物理融合系统的常见漏洞模式,并基于 Attack-SEFTs 对各种漏洞模式进行建模;接着,给出 Attack-SEFTs 模型的失效路径分析方法;最后通过一个案例说明了所提方法的可行性。

关键词 信息物理融合系统,防危性,安全性,状态事件故障树,攻击树
中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2019.05.016

Risk Modeling for Cyber-physical Systems Based on State/Event Fault Trees

XU Bing-feng[1] HE Gao-feng[2] ZHANG Li-ning[1]
(College of Information Science and Technology,Nanjing Forestry University,Nanjing 210037,China)[1]
(School of Internet of Things,Nanjing University of Posts and Telecommunications,Nanjing 210003,China)[2]

Abstract The cyber-physical system is prone to be attacked by the network attacker because of the application of embedded system network in it,and the attacker may utilize the vulnerabilities in the software and communication components to control the system,resulting in a system failure. The existing modeling methods of integrating safety and security are built on traditional static fault trees,and don't consider the characteristics of dynamic and temporal dependencies of the software control system,so they can't infer the final impacts caused by network attracts. In light of this,this paper presented a modeling method of integrating safety and security of cyber-physical systems. Firstly,the Attack-SEFTs model is proposed based on SEFTs model. On this basis,common vulnerabilities in the cyber physical system are proposed,and various vulnerability patterns are modeled based on Attack-SEFTs. Secondly,the unified representation of the Attack-SEFTs model is presented to support its analysis. Finally,a case study is described specially to show the feasibi-lity of the proposed method.

Keywords Cyber-physical systems,Safety,Security,State/event fault trees,Attack trees

1 引言

信息物理融合系统(Cyber-Physical System,CPS)深度融合计算、通信与控制技术,通过计算进程和物理进程相互影响的反馈循环实现系统的智能感知、自主判断与自动执行,目前已经广泛应用于电力、石油石化、核能等领域[1]。这些典型的信息物理融合系统中存在大量的信息处理和网络通信子系统,使得攻击者可能会利用软件和通信组件中的漏洞获取系统的控制权[2],干扰系统的正确行为,从而破坏关键基础设施。例如,2015年乌克兰电力网络部分电站监控系统遭受恶意代码攻击,导致发电设备故障,最终引发乌克兰西部地区约70万居民用户停电数小时[3-4]。因此,与传统的嵌入式系统和信息系统不同,在对信息物理融合系统进行安全风险评估时,必须考虑由于网络攻击造成的软件系统失效,评估由恶意网络攻击引起随机故障的失效因果链[5]。

为了解决该问题,现有工作从面向过程的方法[6]和基于模型的方法[7]两个方面进行研究。其中,面向过程的方法考虑防危性(Safety)和安全性(Security)的生命周期,依赖防危性/安全性标准规定的要求,主要应用于系统工程的早期阶段,特别是概念和需求阶段;而基于模型的方法是基于系统的

到稿日期:2018-03-30 返修日期:2018-06-03 本文受国家自然科学基金青年科学基金项目(61802192,61702282),江苏省高等学校自然科学研究项目(18KJB520024,17KJB520023),南京林业大学校青年创新基金(CX2016026),南京邮电大学引进人才科研启动基金(NY217143),省教改项目(164070911)资助。

徐丙凤(1986-),女,博士,讲师,CCF会员,主要研究方向为CPS安全、软件安全;何高峰(1984-),男,博士,讲师,CCF会员,主要研究方向为CPS安全、匿名通信,E-mail:hegaofeng@njupt.edu.cn(通信作者);张黎宁(1974-),女,硕士,副教授,主要研究方向为软件工程。

功能/非功能的形式化或半形式化表示，以统一的模型建模系统的防危性和安全性，可以应用于系统开发的所有阶段。因此，本文重点研究基于模型的方法。

在基于模型的方法中，基于故障/攻击树的方法是引入扩展故障树，攻击树被集成到一个预先存在的故障树中，在传统风险分析模型的基础上扩展安全威胁[8]。该方法采用了工业界广泛接受的防危性和安全性建模模型，并且提供了定性分析（即分析系统风险的原因和结果）和定量分析（即分析风险的定量概率）方法以支持风险评估。但是，这些基于故障树的方法均存在所有的逻辑门都只有静态依赖的缺陷，无法建模CPS等复杂系统中软件控制系统的动态行为和失效传播路径。

因此，本文针对CPS安全风险建模与分析进行了深入研究，提出一种基于状态事件故障树（Stata/Event Fault Trees，SEFTs）[9]的CPS风险建模与分析方法。SEFTs通过使用类似于状态图的图形符号将故障树与显示的状态/事件语义相结合，提供了构件以及构件之间消息交互的方法，并且通过状态图给出了构件内部的时序依赖描述，支持软件控制系统的动态建模。本文主要工作如下：首先，结合攻击树，针对SEFTs模型进行攻击步骤建模，提出Attack-SEFTs；其次，给出CPS系统的常见漏洞模式，并基于Attack-SEFTs对各种漏洞模式进行建模；最后，给出支持Attack-SFETs模型分析的统一建模方法，并通过实例说明方法的有效性。

本文第2节对CPS防危性和安全性综合建模分析方法进行分析总结；第3节给出状态事件故障树的形式化表示以及Attack-SEFTs模型的构造方法；第4节给出CPS中的常见漏洞模式，基于Attack-SEFTs进行CPS中的常见漏洞模式建模，并给出Attack-SEFTs模型的失效事件链分析方法；第5节开展应用实例分析；最后总结全文，并给出未来的研究工作。

2 相关工作

CPS风险分析包括防危性和安全性两个方面。防危性旨在避免系统遭遇意外失效，仅考虑意外的组件故障和人为错误所导致的风险；安全性旨在避免系统遭受故意攻击，处理有意识的人类行为造成的故意/恶意威胁[10]。这些差异使得防危性和安全性风险分析通常彼此独立进行。然而，CPS的开放性和网络化特征使得安全威胁可能会导致与防危性事件一样的安全攸关后果，因此必须考虑集成分析框架以满足CPS系统风险分析的新要求。

目前，在CPS集成风险建模及分析方面的研究刚刚开始。整体上，已有的研究工作可分为面向过程的方法和基于模型的方法。其中，面向过程的方法考虑防危性和安全性的生命周期和方法过程，依赖防危性/安全性标准规定的要求[6]。这类方法主要应用于系统工程的早期阶段，特别是在概念和需求阶段处理防危和安全，但难以处理系统设计以及后期阶段安全和防危之间的交互和影响。而基于模型的方法是基于系统的功能/非功能的形式化或半形式化表示，以统一的模型建模系统的防危性和安全性，并实现定性分析（即分析系统风险的原因和结果）和定量分析（即分析风险的定量概率）。基于模型的方法可适用于CPS系统生命周期中的不同阶段，是当前的研究热点。

在基于模型的方法中，基于故障/攻击树[11]的方法的思想是引入扩展故障树，在故障树的基础上扩展恶意威胁，最早由文献[12]给出。基于该思想，文献[13]在构建故障树的基础上将攻击树扩展用于安全事件的建模，并且提供了失效事件的概率分析方法；文献[2]在状态事件故障树的基础上独立建模攻击流程，用于CPS系统安全建模，并提供了概率分析方法。然而，如文献[14]中所强调的，现有的故障/攻击树模型均为静态，难以建模软件控制系统的时序和状态依赖等特性，亦无法有效建模系统故障事件发生之后失效（即意外或者恶意失效）的传播路径，从而无法推导出网络安全攻击所导致的最终影响。

因此，本文的基本思想是设计一种集成防危性和安全性的信息物理融合系统风险建模分析方法。具体做法是：以状态事件故障树模型为基础，以攻击树作为系统安全攻击模型，结合这两种模型的优势进行CPS系统风险场景的综合建模与分析。

3 Attack-SEFTs

攻击树通常描述的是在系统上执行未经授权的操作，即产生意料之外的事件。而SEFTs描述的是发生时会导致损害的事件。因此，可以考虑通过增加导致SEFTs中的基本或者中间事件发生的恶意行为（由攻击树建模）来丰富SEFTs的语义，这也意味着攻击者可以利用系统中的一些故障，最终导致SEFTs顶层事件的发生，即仅当存在以SEFTs中的事件作为攻击树的攻击目标时，SEFTs才能与攻击树集成。基于该思想，本文构造了Attack-SEFTs模型。

3.1 SEFTs的形式化描述

状态事件故障树（SEFTs）模型中集成了基于状态的模型元素和故障树元素，并在传统故障树的基础上严格区分了状态和事件；引入显式的事件符号和因果边，采用逻辑门进行连接，在基于状态转换的基础上表达失效事件发生的因果链。图1给出了反应堆安全系统的SEFT模型示例，描述了反应堆爆炸失效的发生过程。该SEFT包含两个构件，在压力超过安全关键限制的情况下，阀或者传感器故障都可能会导致反应堆爆炸。

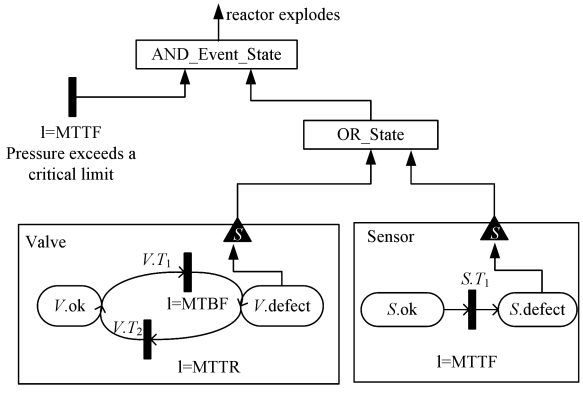

图1 反应堆安全系统的SEFT模型

Fig. 1 SEFT model of reactor safety system

下面给出 SEFTs 的形式化描述。采用状态事件故障树 $SEFT_k$ 表示顶层事件与构件之间的逻辑结构，e_i 表示单独事件，$EU=\{e_i\}$ 表示事件的集合，$E_k=\{e_l:e_l\in EU,e_l\in SEFT_k\}$ 表示 $SEFT_k$ 中的事件。事件之间的关系采用逻辑门表示，用 p_k 表示逻辑门，$PU=\{p_k\}$ 表示逻辑门的集合，$P_k=\{p_l:p_l\in PU,p_l\in SEFT_k\}$ 表示属于状态事件故障树 $SEFT_k$ 的逻辑门。逻辑门 p_k 具有 n_k 个输入 $IN_jp_k(j=1,\cdots,n_k)$ 和一个输出 $OUTp_k$，以及一个逻辑功能函数 $fp_k=fp_k(IN_1p_k,IN_2p_k,\cdots,IN_{n_k}p_k)$。事件、状态和逻辑门之间通过边进行连接，边 $d_{a,b}$ 连接节点 n_a 和 n_b，集合 $DU=\{d_{a,b}\}$ 是边的集合，$D_k=\{d_{a,b}:d_{a,b}\in DU,d_{a,b}\in SEFT_k\}$ 表示状态事件故障树 $SEFT_k$ 边的集合。基于以上描述，给出状态事件故障树的形式化定义。

定义 1　一个状态事件故障树可以采用以下集合表示：$\langle E_i,P_i,C_i,D_i,TOP_i\rangle$，其中 E_i 表示事件，P_i 表示逻辑门，C_i 表示构件，D_i 表示边，TOP_i 表示顶层事件。事件与事件之间、逻辑门与逻辑门之间不允许直接相连，即 $D_{i,j}\subset\{(n_i,n_j)\in\{(E_i\times P_i)\cup(P_i\times E_i)\}\}$，其中 (n_i,n_j) 表示元素 n_i 和 n_j 之间的边。

3.2　攻击树的形式化描述

攻击树采用结构化的方式建模网络攻击。以攻击目标作为根节点（即顶层事件），以部分攻击作为中间节点或叶节点，事件之间的组合采用 AND 和 OR 逻辑门进行表达。任何一条从叶节点到根节点的路径表示实现这个攻击目标而进行的一次完整的攻击过程。

图 2 描述的是一个攻击树的例子，其建模了一个可以通过局域网或无线局域网访问的计算机系统，获得授权需要额外的身份验证。对 LAN 的访问受到媒体访问控制地址过滤器的限制，该过滤器只允许访问位于该列表上的 MAC 地址的客户端。对 WLAN 的访问受到了 WiFi 保护访问的加密限制。

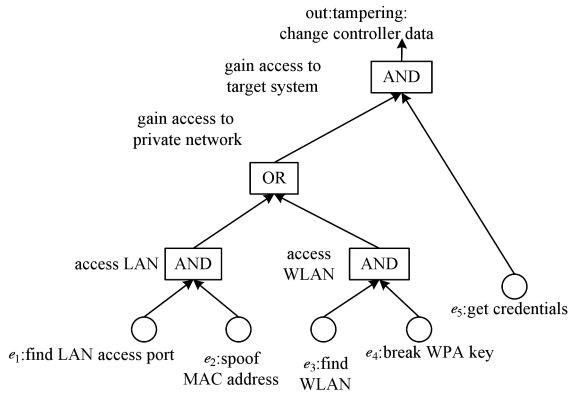

图 2　攻击树示例

Fig. 2　Example of attack tree

下面给出攻击树的形式化描述。集合 $A=\{a_i\}$ 表示所有攻击树的集合；集合 $G=\{\text{goal } at,\forall at\in A\}$ 表示攻击树 at 的攻击目标，该目标表示成功利用攻击的最终结果，也可以看作攻击成功时会发生的事件。A_k 为所有具有相同攻击目标的攻击树集合，其具体定义如下：$A_k=\{at:\text{goal } at=g_k,g_k\in G,at\in A\}$。在此基础上，我们定义一个特殊的逻辑门 TOP_OR_k，该逻辑门是具有 n_k 个输入和一个输出的 OR 门。

$$n_k=|A_k|:inputTOP\_OR_k=at_i,i=1,\cdots,n_k$$

$$outputTop\_OR_k=g_k,g_k\in G$$

攻击树 MA_k 由 g_k，TOP_OR_k 及其输入组成，该攻击树可以到达特定的攻击目标。

3.3　Attack-SEFTs 模型

定义 2　$MA=\{MA_k\}$ 是所有攻击树的集合，状态事件故障树 $SEFT_k$ 可以与攻击树 MA_k 集成 Attack-SEFTs 模型，当且仅当：$\exists e_i\in EU_k:e_i=goalMA_j,MA_j\in MA$。即，攻击树与状态事件故障树可以进行集成，当且仅当存在攻击树的目标与状态事件故障树中的事件是一致的。

在攻击树与状态事件故障树可以集成的前提下，Attack-SEFTs 模型的生成步骤为：

1）在状态事件故障树中，子树 $e_{i\_subtree}$ 产生 e_i 事件，将其从状态事件故障树中分离出来。

2）将具有两个输入（A 和 B）的 Event_OR 逻辑门（merge_gate）连接到 e_i 事件。从逻辑的角度来看，e_i 是 merge_gate 的输出。

3）攻击树 MA_j 连接到 merge_gate 的输入 A。这里将攻击的目标视为攻击成功时发生的事件，这样就可以保留一个形式良好的状态事件故障树组合规则（攻击树的输入类型是状态事件故障树的子集）。

4）攻击树 MA_j 的目标被修改为“成功攻击导致事件 e_i 发生”。这里应该避免 merge_gate 的输入和输出是相同的事件。

5）虚拟事件“原始 e_i”被引入并连接到 merge_gate 的输入 B。

6）子树 $e_{i\_subtree}$ 连接到虚拟事件上。

通过以上步骤，可得到状态事件故障树的一个扩展模型 Attack-SEFTs，该模型在状态事件故障树的基础上丰富了攻击树的语义。图 3 给出了一个 Attack-SEFTs 模型的构造示例。在该示例中，i_1 节点既是 SEFT 中的事件，又是 Attack tree 中的攻击目标，通过集成可以建模网络攻击导致的软件系统失效。

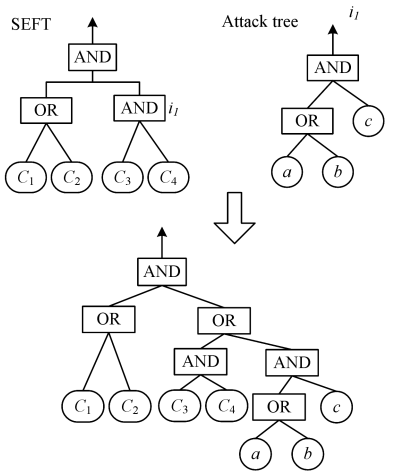

图 3　Attack-SEFTs 模型的示例

Fig. 3　Example of Attack-SEFTs model

4 CPS 风险建模及分析

在 Attack-SEFTs 模型的基础上，可以进行 CPS 安全攻击的建模以及分析工作。

4.1 CPS 风险建模

CPS 容易发生物理和网络空间攻击，由于攻击者能够直接攻击物理构件或者通过与它们进行信息交互对其进行攻击，这就意味着软件和硬件都可能成为攻击者的攻击对象。由于 SEFTs 可以同时建模软硬件的故障，且 Attack-SEFTs 在 SEFTs 的基础上扩展了攻击模型，因此可以采用 Attack-SEFTs 建模 CPS 漏洞模式。如文献[2]所述，CPS 中可能的基本漏洞模式如下：

1)构件之间交互消息的拒绝服务。

2)构件之间的消息欺骗。

3)通过阻止一个或多个切换转换的构件 DoS。

4)绕过构件的状态。攻击者有可能通过改变状态之间的转换引入状态之间的捷径来修改构件。

5)构件状态图的重构。攻击者能够引入新状态并且完全改变内部结构。

上述所有漏洞(除消息欺骗漏洞外)都可能与网络空间和物理世界相关。下面使用 Attack-SEFTs 建模这些攻击模式，如图 4 所示。

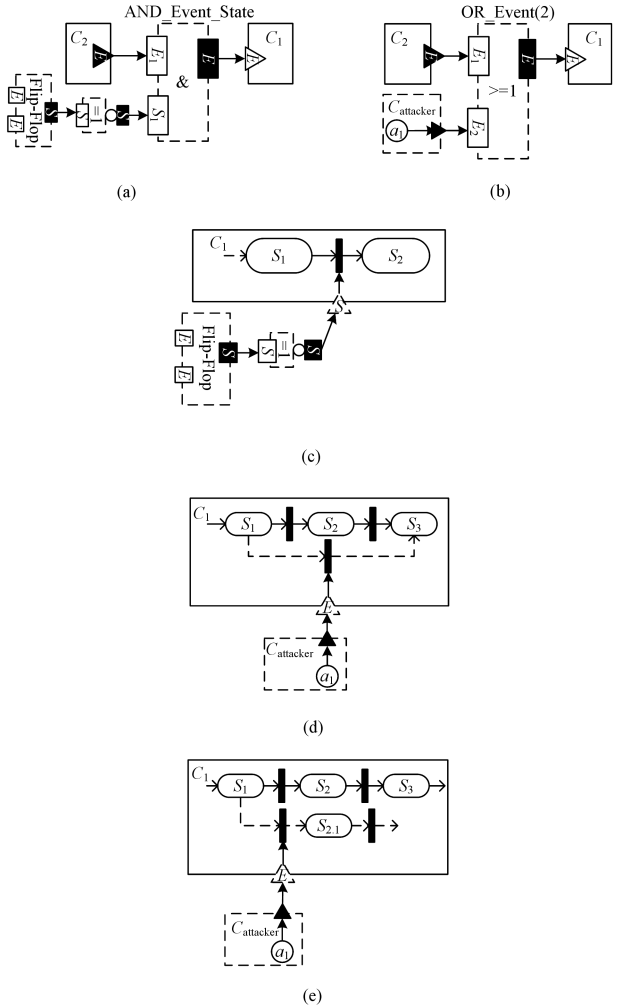

图 4 CPS 漏洞模式建模

Fig. 4 Vnlnerability patterns modeling for CPS

在通信信道的 DoS 情况下，攻击者具有拦截构件之间消息或命令的能力，如妨碍通过无线信道接收的消息，这可能导致系统构件出现消息遗漏。在通信信道中，不需要网络访问就可以利用 DoS 漏洞，因此，以这种方式攻击系统比较容易。图 4(a)描述了这种 DoS 模式，当且仅当系统 S_1 状态为当前的活动状态时才可能发送消息，在发生攻击的情况下，通信不再继续。相比之下，消息欺骗攻击(见图 4(b))允许消息的散布，如将接收构件转移到另一状态或者使得接收构件认为一切正常。构件的 DoS 攻击(见图 4(c))与通信信道的 DoS 攻击不同，攻击者可以直接访问构件，从而阻止其切换至另一个状态。此外，攻击者可以通过事件 E 跳过状态 S_2(见图 4(d))；重编程攻击模式(见图 4(e))中攻击者可以通过事件端口 E 的触发来改变状态图的完整行为。在图 4 中，所有与安全相关的都用虚线框进行建模。

4.2 CPS 失效事件链分析

在获得基于 SEFTs 语义表达的 CPS 风险模型之后，可基于该模型分析系统失效发生的失效事件链。特别地，可以分析出网络攻击造成的系统失效事件链。

首先，依据文献[15]中所提出的 SEFTs 定性分析方法步骤构造其可达图；其次，根据可达图搜索系统失效事件链。基本步骤包括：1)针对 SEFTs 构造可达图模型；2)针对可达图，采用深度优先搜索算法找到所有的失效路径，具体的算法如算法 1 所示；3)针对搜索到的失效路径，根据表 1 所给出的规约规则进行失效路径的计算，将带有逻辑符号的失效事件链转换为仅有事件序列的失效事件链。例如：表 1 分布律中的规则 $E_1 \rightarrow (E_2 \vee E_3) \Leftrightarrow E_1 \rightarrow E_2 \vee E_1 \rightarrow E_3$ 表示事件 E_1 在事件 E_2 或 E_3 之前发生，可以转换为 E_1 在 E_2 之前发生和 E_1 在 E_3 之前发生两个事件链。

表 1 失效事件规约规则

Table 1 Failure events reduced rules

分布律	$E_1 \rightarrow (E_2 \vee E_3) \Leftrightarrow E_1 \rightarrow E_2 \vee E_1 \rightarrow E_3$
	$(E_1 \vee E_2) \rightarrow E_3 \Leftrightarrow E_1 \rightarrow E_3 \vee E_2 \rightarrow E_3$
	$E_1 < (S_1 \vee S_2) \Leftrightarrow E_1 < S_1 \vee E_1 < S_2$
	$(S_1 \vee S_2) < E_1 \Leftrightarrow E_1 < S_1 \vee E_1 < S_2$
结合律	$(E_1 \rightarrow E_2) \rightarrow E_3 \Leftrightarrow E_1 \rightarrow E_2 \rightarrow E_3$
交换律	$E_1 \vee E_2 \Leftrightarrow E_2 \vee E_1$

算法 1 失效事件序列搜索算法

输入：可达图 RG

输出：失效事件序列 $E_1 \rightarrow E_2 \rightarrow \cdots \rightarrow E_n$

```
1.  FailurePathSet:={};FailurePath:=InitialNode;
2.  repeat
3.      node:=FailurePath 中的最后一个节点;
4.  if node 没有新的后继节点
5.      then 删除 FailureSequence 中的最后一个节点;
6.    else begin node:=取 node 的一个新的后继节点;
7.      if node 对应的节点是目标节点
8.          then 将 FailurePath 加入 FailurePathSet;
9.        else 将该后继节点加入 FailurePath;
10.       end
11.  until FailurePath=<    >.
```

5 案例分析

胎压监测系统(Tire Pressure Monitoring System，

TPMS)是一个安装在轮胎上的安全关键系统。该系统的主要部件包括：1)安装在轮胎内侧的 2 个轮胎压力传感器；2)2 根接收传感器信号的天线；3)用于数据处理的电子控制单元(Electrical Controlling Unit，ECU)；4)通知驾驶员轮胎气压不足的仪表板。该系统中无线接口的存在使其极易被攻击，而且目前该系统的安全机制尚不完善，极易被黑客攻击。

文献[16]中指出，一种可能的攻击方式是发送比实际值低的胎压值给 ECU，通过消息欺骗模式进行攻击，这可能导致驾驶员误以为有危险而被迫停在路边。更为严重的是，某些车辆判断胎压过低就会自动刹车，如果在高速路上行驶，这会对用户造成生命危险；另外，某些轮胎具备在胎压过低时自动充气的功能(如固特异轮胎)，若黑客持续攻击，会导致轮胎因充气过足而爆裂等危险事故发生。

针对该攻击，下面采用本文提出的方法进行 CPS 集成建模。首先，采用 Attack-SEFTs 对“胎压发生故障”的因果链进行建模，如图 5 所示。通过对该 Attack-SEFTs 进行遍历，并且结合实际系统网络攻击点的考虑可以发现，若攻击者发送比实际值低的胎压值给 ECU，则会导致胎压故障。依据 4.1 节中给出的消息欺骗漏洞模式建模方式，在 SEFTs 的 ECU 中直接将该攻击建模为具有 3 个事件输入的 OR_Event(3)门，其中 2 个输入来自传感器，1 个输入来自消息欺骗网络攻击。该攻击的第一步是处理接收的 ID 包，该事件成功之后将触发下一步，通过与系统的消息欺骗漏洞进行连接并执行消息欺骗攻击操作来模拟虚假信息的传输。攻击步骤的具体建模如图 6 所示。如果轮胎有故障，则顶层事件发生。图 6 描绘了 TPMS 的集成安全模型，该模型综合描述了网络攻击对该系统安全性的影响。

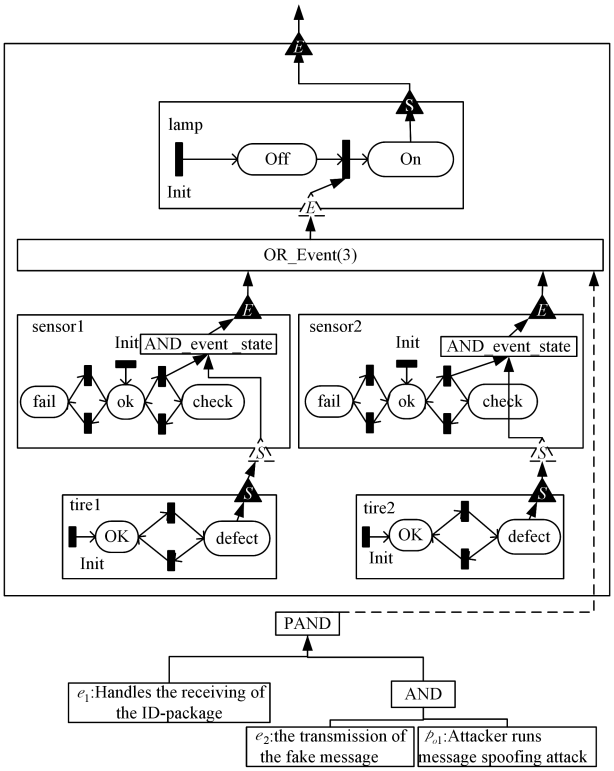

图 5　TPMS 的分析模型

Fig. 5　Analysis model of TPMS

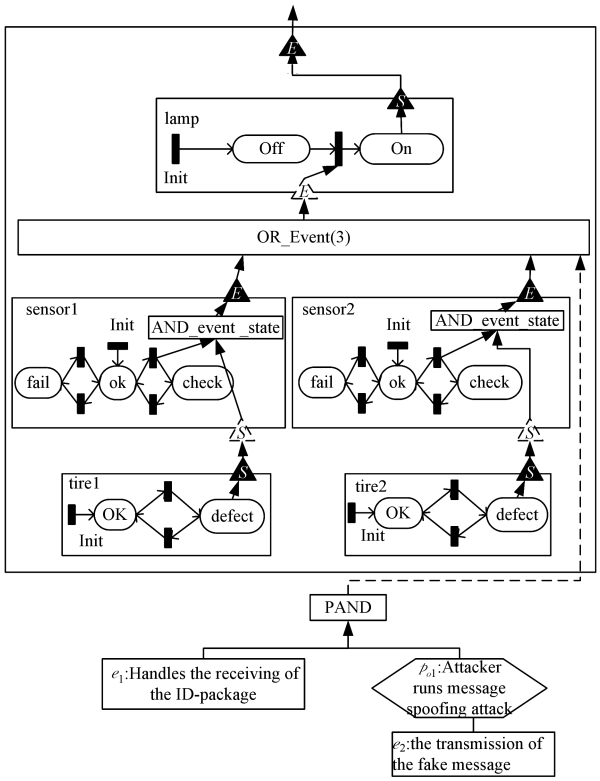

图 6　TPMS 的集成安全模型

Fig. 6　Integrated security model of TPMS

下面针对该模型进行分析。首先进行模型的预处理，重点针对攻击模型部分进行处理。处理之后的模型如图 5 所示。每个构件内部采用基于状态机的语义进行建模，构件与构件之间的消息传递通过接口进行。对于攻击步骤，PAND 逻辑门描述攻击步骤的时序，可以有效描述网络攻击导致最终系统失效发生的过程。在图 5 的基础上，采用 4.2 节所给出的定性分析方法进行失效事件链分析，结果如下：

$((e_1 \rightarrow (e_2 \wedge p_{o1})) \vee (\text{tire1.defect} \rightarrow \text{sensor1.check}) \vee (\text{tire2.defect} \rightarrow \text{sensor2.check})) \rightarrow \text{lamp.on}$

采用表 1 所给的规约规则可以得出所有的失效事件链，包括：

1) $e_1 \rightarrow e_2 \rightarrow p_{o1} \rightarrow$ lamp.on；

2) $e_1 \rightarrow p_{o1} \rightarrow e_2 \rightarrow$ lamp.on；

3) tire1.defect→sensor1.check→lamp.on；

4) tire2.defect→sensor2.check→lamp.on。

从分析结果可以看出，引起顶层事件发生的失效事件链中，1)和 2)是由网络攻击引起的，3)和 4)是由系统自身故障引起的。因此，采用本文的建模分析方法可以对 CPS 风险进行防危性和安全性集成建模。

结束语　本文针对集成防危性与安全性的 CPS 风险建模分析，基于状态事件故障树提出 Attack-SEFTs 模型。首先给出了攻击树模型和状态事件故障树模型的形式化描述方法，并在此基础上给出了 Attack_SEFTs 模型的构造步骤；然后根据 CPS 的漏洞模式，采用 Attack_SEFTs 模型对其进行建模，并给出了失效事件链的分析方法；最终通过一个实例说明了该建模方法的有效性。未来工作包括：基于状态事件故

障树的建模分析工具 ESSaRel 研究 Attack-SEFTs 的自动建模前端;研究攻击失效路径的自动分析方法,并基于攻击路径给出具体的防御建议;在此基础上,通过更多案例来验证本文方法的有效性。

参 考 文 献

[1] BAHETI R,GILL H. Cyber-physical systems[J]. The impact of control technology,2011,12(1):161-166.

[2] ROTH M,LIGGESMEYER P. Modeling and analysis of safety-critical cyber physical systems using state/event fault trees[C]// SAFECOMP 2013-Workshop DECS (ERCIM/EWICS Workshop on Dependable Embedded and Cyber-physical Systems) of the 32nd International Conference on Computer Safety,Reliability and Security. Toulouse,France:Springer International Publishing,2013:1-11.

[3] GUO Q L,XIN S J,WANG J H,et al. Comprehensive Security Assessment for a cyber physical energy system:a lesson from Ukraine's Blackout [J]. Automation of Electric Power Systems,2016,40(5):145-147. (in Chinese)
郭庆来,辛蜀骏,王剑辉,等.由乌克兰停电事件看信息能源系统综合安全评估[J].电力系统自动化,2016,40(5):145-147.

[4] TANG Y,CHEN Q,LI M Y,et al. Overview on Cyber-attacks Against Cyber Physical Power System [J]. Automation of Electric Power Systems,2016,40(17):59-69. (in Chinese)
汤奕,陈倩,李梦雅,等.电力信息物理融合系统环境中的网络攻击研究综述[J].电力系统自动化,2016,40(17):59-69.

[5] BRUNNER M,HUBER M,SAUERWEIN C,et al. Towards an Integrated Model for Safety and Security Requirements of Cyber-Physical Systems[C]// 2017 IEEE International Conference on Software Quality,Reliability and Security Companion (QRSC). Prague:IEEE Press,2017:334-340.

[6] WOSKOWSKI C. A pragmatic approach towards safe and secure medical device integration[C] // International Conference on Computer Safety,Reliability,and Security. Florence:Springer,2014:342-353.

[7] NAGARAJU V,FIONDELLA L,WANDJI T. A survey of fault and attack tree modeling and analysis for cyber risk management [C]// 2017 IEEE International Symposium on Technologies for Homeland Security (HST). Waltham,MA,USA:IEEE Press,2017:1-6.

[8] MACHER G,MESSNARZ R,ARMENGAUD E,et al. Integrated Safety and Security Development in the Automotive Domain:2017-01-1661 [R]. USA:SAE Technical Paper,2017.

[9] KAISER B,GRAMLICH C,FÖRSTER M. State/event fault trees—A safety analysis model for software-controlled systems [J]. Reliability Engineering & System Safety,2007,92(11):1521-1537.

[10] KRIAA S,PIETRE-CAMBACEDES L,BOUISSOU M,et al. A survey of approaches combining safety and security for industrial control systems[J]. Reliability Engineering & System Safety,2015,139(3):156-178.

[11] KORDY B,PIÉTRE-CAMBACÉDÉS L,SCHWEITZER P. DAG-based attack and defense modeling:Don't miss the forest for the attack trees[J]. Computer Science Review,2014,13:1-38.

[12] FOVINO I N,MASERA M,DE CIAN A. Integrating cyber attacks within fault trees[J]. Reliability Engineering & System Safety,2009,94(9):1394-1402.

[13] MAX S. Integrating Security Concerns into Safety Analysis of Embedded Systems Using Component Fault Trees [D]. Kaiserslautern:Technische Universität Kaiserslautern,2016.

[14] CHOCKALINGAM S,HADŽIOSMANOVIĆ D,PIETERS W,et al. Integrated safety and security risk assessment methods:a survey of key characteristics and applications[C]// International Conference on Critical Information Infrastructures Security. Paris:Springer,2016:50-62.

[15] XU B,HUANG Z,HU J,et al. Minimal cut sequence generation for state/event fault trees[C]// Proceedings of the 2013 Middleware Doctoral Symposium. Beijing:ACM,2013:3-10.

[16] ISHTIAQ ROUFA R M,MUSTAFAA H,TRAVIS TAYLORA S O,et al. Security and privacy vulnerabilities of in-car wireless networks:A tire pressure monitoring system case study[C]// 19th USENIX Security Symposium. Washington DC:USENIX Association,2010:11-13.