doi:10.11887/j.cn.201502018 http://journal.nudt.edu.cn

卫星导航系统的体系安全性分析方法*

张旺勋,李 群,侯洪涛,王维平
(国防科技大学 信息系统与管理学院,湖南 长沙 410073)

摘 要:为了应对卫星导航系统内部复杂关系等体系特征为其安全分析带来的挑战、全面识别和分析卫星导航系统面临的体系安全威胁、提高系统的安全性和服务能力,基于功能依赖网络分析理论提出了从体系角度研究卫星导航系统安全性的建模方法,重点对导航系统内组件系统之间交互关系导致的危险传播、任意失效组合进行了后果分析和原因调查。仿真结果表明该方法能清晰地描述危险传播和失效组合的过程以及进行正逆向的推理分析,也证明了该方法在卫星导航系统安全分析问题上的潜力和适用性。

关键词:卫星导航系统;体系;安全性分析;功能依赖网络分析
中图分类号:TN967.1 **文献标志码**:A **文章编号**:1001-2486(2015)02-092-07

System of systems safety analysis method for GNSS

ZHANG Wangxun, *LI Qun*, *HOU Hongtao*, *WANG Weiping*
(College of Information System and Management, National University of Defense Technology, Changsha 410073, China)

Abstract: In order to address challenges of safety analysis of global navigation satellite systems (GNSS) brought by its system of systems (SoS) characteristics such as complex relationships between its component systems, to identify and study the SoS safety hazards across-the-board, and to improve its safety and enhance the service, a GNSS safety modeling method was proposed in the base of the functional dependency network analysis theory from the view of SoS. The effects and reasons of hazards promulgation and random failures combination caused by complex relationships between component systems in GNSS were analyzed and investigated with some emphasis. The simulation results show that the method is able to describe the influencing process of hazards promulgation and failures combination clearly and conduct both orthodromic and antidromic reasoning analysis. The results also demonstrate the great potential and applicability of the method to SoS safety analysis of GNSS.

Key words: global navigation satellite systems; system of systems; safety analysis; functional dependency network analysis

全球卫星导航系统(Global Navigation Satellite Systems, GNSS)作为信息化时代的指南针,在经济建设各个领域应用越来越广泛[1],然而由于子系统众多、交互关系复杂、空间分布广等特点,系统自身存在一定的脆弱性和安全风险。导航系统脆弱性和安全性研究已经引起了广泛的关注[2-4]。

根据已有文献的研究,卫星导航系统的脆弱性和安全工作研究内容主要集中在三个方面[5-6]:1)定性列举卫星导航系统可能面临的各种威胁手段及相应安全措施;2)信号链路的干扰和抗干扰研究;3)全系统角度研究导航系统的脆弱性和防护问题。通过文献查阅和对比不难看出,已有研究大多偏重于对某个具体威胁或安全防护措施进行分析,而且大多仅从信号质量或链路本身出发,而从全系统或体系角度研究导航系统的安全和防护问题的文献较少,仍处于探索阶段。

GNSS由空间段、地面控制段和用户段三大系统及其链路组成,各大系统又包括若干子系统,系统之间存在复杂的交互和依赖关系,仅从局部组件或单独链路分析已经不能满足其安全防护的需求,因此需要从体系(System of Systems, SoS)的角度研究其安全性,即通过对GNSS体系组成、系统接口、交互关系、体系网络结构、工作模式等进行分析,重点关注并解决体系内系统间相互作用关系和涌现行为可能产生的安全风险。

体系间相互作用产生的危险大致可分为四类:一是组件系统失效或故障通过系统间相互关系在体系中传播;二是多个组件失效或故障的组合效应;三是系统间接口或关系异常导致的危险;

* **收稿日期**:2014-08-25
基金项目:国家自然科学基金资助项目(91024015)
作者简介:张旺勋(1985—),男,陕西韩城人,博士研究生,E-mail:zhangwangxun2010@163.com;
王维平(通信作者),男,教授,博士,博士生导师,E-mail:wang.wp2010@gmail.com

四是体系演化过程中产生的危险。以卫星导航系统为对象,提出了一种能对上述四类体系危险进行建模分析的方法。

1　研究现状

针对上述四类体系危险,传统安全性可靠性建模分析方法都具有一定的局限性。故障模式和影响分析[7]是把系统分割成子系统或元件,逐个分析元件可能发生的故障和故障模式,不能分析多个子系统组合失效引起的故障;故障树[8]从单个事故出发,分析可能引发该事故的所有事件组合,对于具有多种故障模式的系统,则需要建立多棵故障树;事件树[9]则是从单个事件出发,分析该事件的发生可能导致哪些后果,同样对于复杂系统它需要建立多棵树,另外,事件树只能分析单独事件而不能分析组合事件的影响。Petri 网[10]对大型复杂系统分析时,由于系统规模较大,可达图难以获取,导致定性定量分析难以进行。贝叶斯网络[11]分析要求给出事件的先验概率和条件概率,而这些数据又是不容易获得的,所以其应用受到了限制。因此,需要探索开发新的适应于体系安全分析的方法技术。

当前关于体系安全性的研究已经引起了学术界和工程界的强烈关注,并提出了相关模型和技术,几种典型的方法包括:Perrow 早在 1984 就提出了正常事故理论(Normal Accident Theory, NAT),用来研究由多个系统或组件的相互作用而可能产生的"正常"事故[12];Leveson 根据系统理论和控制科学提出了系统理论的事故模型和过程(Systems Theoretic Accident Modeling and Process, STAMP),将安全问题看作是一类控制问题,事故被看作是由组件间交互而导致系统安全约束的违背的结果[13];Alexander 等结合国防部体系架构,提出了基于 Agent 的仿真分析方法(Simulation-based Hazard Analysis, SimHAZAN)来研究军事体系的威胁分析[14];Redmond 提出了分析接口类危险的输入输出事故(Input/Output Mishap, IOM)方法[15]。

作为一个新兴领域,尽管体系安全性已经引起了一定的关注,但是仍然缺乏普适的方法论,通过表 1 可以看出上述方法都各有侧重或针对特定领域。借鉴前人理论,提出一种基于功能依赖网络的导航系统的体系安全性建模分析方法。

表 1　4 种体系安全性分析方法比较

Tab. 1　Comparision of four SoS safety analysis methods

方法名称	特点	不足
NAT	"交互复杂性"和"紧耦合"必然导致复杂系统的"正常事故"	1. 应用范围有限; 2. 没有明确概念和量化方法 3. 定性分析较多
STAMP	1. 将安全看作控制问题 2. 多层次多因素	1. 量化不够 2. 分析过程不清晰
Sim-HAZAN	多 Agent 结合机器学习支持探索性分析	1. 方法过于复杂 2. 尚未在大型系统试验
IOM	1. 模型简单清晰 2. 针对接口类危险	1. 仅考虑确定接口和交互 2. 对正常交互的考虑不足

2　基于功能依赖网络分析的安全性分析

2.1　方法介绍

Garvey 和 Pinto 等最早提出功能依赖网络分析[16](Functional Dependency Network Analysis, FDNA)方法,用来分析某个系统性能的失效对其他依赖的性能引起的连锁反应。该方法提供了评估拓扑结构和单个或多个系统功能退化对体系中各节点的影响的能力[17-18]。目前,该方法已经被应用到多个领域:Drabble 将其用于分析协作网络中的信息转移问题[19];Guariniello 和 DeLaurentis 对其进行了适当扩展,并进行了较为广泛的应用,将其用于航空体系的维修问题、体系架构分析、体系信息和赛博安全问题[20];王玥和张旺勋等对其在卫星导航系统的安全性分析领域进行了探索[21-22]并正在开展更深入具体的研究。

从依赖的角度将系统中的实体分为提供者和接受者两类,简称为供点和受点。受点的性能水平受到两个属性的影响,即依赖强度(Strength of Dependency, SOD)和依赖关键度(Criticality of Dependency, COD)。SOD 描述依赖关系对基本运行水平的贡献;而 COD 描述依赖关系对基本运行水平的制约或牵制。

如图 1 所示,在节点 v_i 作用下节点 v_j 的性能 P_j 如式(1)所示:

$$P_j = f(\alpha_{ij}, \beta_{ij}, P_i) \tag{1}$$

式中,α_{ij}和β_{ij}分别表示节点 v_j 对节点 v_i 的依赖强度参数(SOD)和依赖关键度参数(COD)。

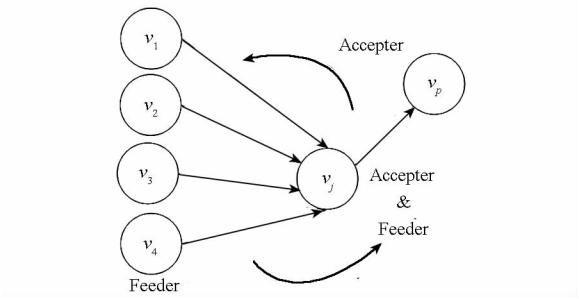

图 1 FDNA 示例图

Fig. 1 An example of FDNA

更一般的情况,对于有 k 个提供者的情况,则接受者节点 v_j 的性能 P_j 可以表示为:

$$P_j = F(\alpha_{1j}, \beta_{1j}, P_1, \alpha_{2j}, \beta_{2j}, P_2, \cdots, \alpha_{kj}, \beta_{kj}, P_k) \tag{2}$$

2.2 建模和分析步骤

FDNA 具有网络化的表现形式、可视化强、计算原理清晰易懂、能够描述组合失效等诸多优势,因此对于描述导航体系安全评价和分析问题同样具有很好的适用性。基于 FDNA 的导航系统的体系安全性建模和分析步骤如下:

1)建立系统的基本依赖网络模型。用 $G = \{V, E\}$ 表示整个网络,节点 $v_i \in V$ 表示导航系统中的各实体,如卫星、地面站等;节点间的依赖关系 $e_{i,j} \in E$ 用来描述各站点或卫星之间的相互作用、协作等依赖关系。在节点选择和关系建立时,要借鉴设计文档、历史经验、专家意见等。

2)描述和确定依赖参数。用 α_{ij} 和 β_{ij} 分别表示节点 v_j 对节点 v_i 的依赖强度参数和依赖关键度参数。α_{ij} 可以通过式(3)计算:

$$100(1 - \alpha_{ij}) = x \tag{3}$$

式中,x 是在没有提供者的情况下,接受节点的基本性能水平。如在没有提供者的情况下,节点 v_j 的性能水平为 50,则 $\alpha_{ij} = 0.5$。α_{ij} 越小表示节点 v_j 对节点 v_i 的依赖越弱,$0 \leqslant \alpha_{ij} \leqslant 1$。

COD 表示提供者对接受者的制约限制情况,即使其他提供者都正常工作,或者允许接受者有更高的性能,但是某个节点的 *COD* 限制了其性能。节点 v_j 的性能不能超过 $P_i + \beta_{ij}$,P_i 是提供者的性能水平,且 $0 \leqslant P_i \leqslant 100$。即有式(4)成立:

$$P_j \leqslant P_i + \beta_{ij},\ 0 \leqslant \beta_{ij} \leqslant 100 \tag{4}$$

3)定义体系事故。体系中各系统的状态或性能异常并不一定会导致整个体系发生事故。这一步需要定义哪些情况可能导致体系事故。这里根据危险与可操作性分析(Hazard and Operability Analysis, HAZOP)或故障树分析(Fault Tree Analysis, FTA)等传统安全性分析方法,或者专家经验、历史数据等列出可能导致系统事故的条件或状态。设体系中共有 N 种可能事故 $\Omega = \{M_1, M_2, \cdots, M_N\}$,用 $S_i = \{s_{i1}, s_{i2}, \cdots, s_{im}\}$ 表示可能导致体系中第 i 种事故的最小状态集合,其中 $S_i \neq \varnothing$ 且 $S_i \subseteq S$,s_i 表示某个子系统的状态,S 表示所有子系统状态的集合。

设某一时刻体系的状态集合为 $S' = \{s_1, s_2, \cdots, s_n\}$,则第 i 种事故发生可以表示为 $M_i = \{true \mid S' \supseteq S_i\}$。若网络中有体系事故发生,则必然有 $\exists S_i$,使得 $S' \supseteq S_i$。若没有体系事故发生,则对于 $\forall S_i$,有 $(S' \cap S_i) \subset S_i$。

4)危险后果分析。分析单个系统或多个系统的性能参数或状态发生变化对其他节点以及对整个系统的影响。

根据木桶原理将式(1)定义为式(5):

$$P_j = \min[g(\alpha_{ij}, P_i), h(\beta_{ij}, P_i)] \tag{5}$$

其中,

$$\begin{aligned} g(\alpha_{ij}, P_i) &= SODP_j = \alpha_{ij} P_i + 100(1 - \alpha_{ij}) \\ h(\beta_{ij}, P_i) &= CODP_j = P_i + \beta_{ij} \end{aligned} \tag{6}$$

更一般的情况,对于有多个提供节点的情况,则节点 v_j 的性能,即式(2)可以表示为式(7):

$$0 \leqslant P_j = \min(SODP_j, CODP_j) \leqslant 100 \tag{7}$$

其中,

$$SODP_j = \mathrm{avg}(SODP_{j1}, SODP_{j2}, \cdots, SODP_{jh}) \tag{8}$$

$$SODP_{ji} = \alpha_{ij} P_i + 100(1 - \alpha_{ij}) \tag{9}$$

$$CODP_j = \min(CODP_{j1}, CODP_{j2}, \cdots, CODP_{jh}) \tag{10}$$

$$CODP_{ji} = P_i + \beta_{ij} \tag{11}$$

根据式(5) ~ (11),则可以计算网络中单个或多个节点的性能参数发生变化对相邻接受节点的影响,进而获得对整个网络所有节点的影响。

5)事故原因分析。针对不同的事故,分析可能导致事故发生的原因。对异常状态集 $S_N = \{s_1, s_2, \cdots, s_n\}$,分析每个状态异常的根原因,最终的根原因集合表示为 $R = \{r_1, r_2, \cdots, r_k\}$。事故原因分析实际就是依赖关系的逆向分析,根据功能依赖网络中的依赖关系,有受点逆向的需找其供点,并分析其性能变化。

3 应用示例

3.1 背景和假设

假设某部门 UR 需要在某特定区域完成某项任务,该区域在任务时间可见的导航卫星有 6 颗,分别记为 STL1 ~ STL6。6 颗卫星与地面监测站

SVL1 ~ SVL3 和上行注入天线 ATN1 ~ ATN3 进行交互,完成卫星健康诊断、更新星历和时钟等活动。主控站 MCS 负责数据收集和处理,它由各监测站提供数据,然后将处理过的数据通过上注天线上载给卫星。示意图如图 2 所示。

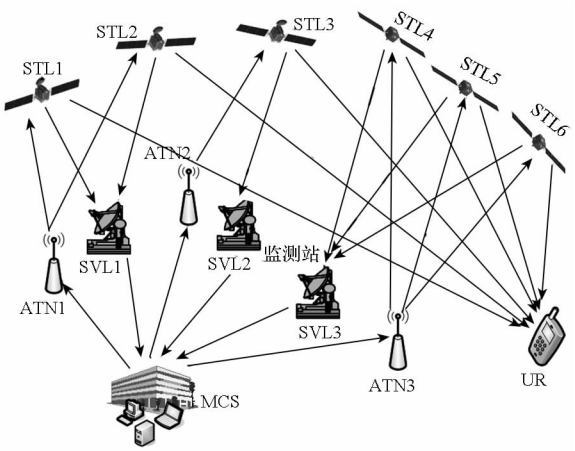

图 2　导航系统示例图

Fig. 2　Demonstration of a GNSS

3.2　分析过程

下面根据上一节的方法和具体步骤,对上述应用问题开展安全性分析。

1)建立系统的基本依赖网络模型。本例中的节点包括 6 颗卫星、3 个监测站、3 个天线、1 个主控站和 1 个用户,共 14 个节点。构建的基本依赖网络如图 3 所示。

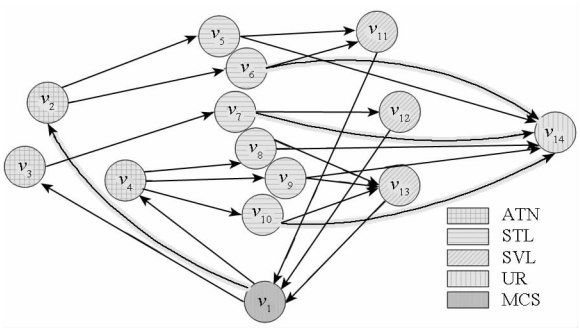

图 3　基本依赖网络模型

Fig. 3　Basic dependency network model

2)描述和确定依赖参数。根据系统运行原理、相关专家知识,网络中各节点的依赖参数值如表 2 所示。

3)定义体系事故。通过 HAZOP、FTA 等经典方法,确定的 GNSS 体系中的几类体系事故如表 3 所示。

表 2　α_{ij} 和 β_{ij} 取值表

Tab. 2　Values of α_{ij} and β_{ij}

i/j	α_{ij}	β_{ij}	i/j	α_{ij}	β_{ij}
1/2	1.00	0	8/13	0.35	65
1/3	1.00	0	9/13	0.40	60
1/4	1.00	0	10/13	0.25	75
2/5	0.30	70	11/1	0.30	70
2/6	0.20	80	12/1	0.45	55
3/7	0.20	80	13/1	0.55	45
4/8	0.25	75	5/14	0.20	80
4/9	0.20	80	6/14	0.25	75
4/10	0.35	65	7/14	0.15	85
5/11	0.55	45	8/14	0.30	70
6/11	0.45	55	9/14	0.25	75
7/12	1.00	0	10/14	0.20	80

表 3　GNSS 体系事故列表

Tab. 3　SoS accidents list of GNSS

编号	描　　述
Ⅰ	用户性能低于 90,$P_{14}<90$
Ⅱ	3 颗卫星性能明显下降
Ⅲ	2 号监测站 v_{12} 性能严重下降
Ⅳ	2 号上注天线 v_3 性能严重下降
Ⅴ	1 号 v_{11} 和 3 号 v_{13} 监测站性能同时严重下降
Ⅵ	1 号 v_2 和 3 号 v_4 天线性能同时严重下降

单颗卫星明显下降的定义:

$$State_{\mathrm{STL}}=\{serious\mid P_{\mathrm{STL}}\leqslant 90\}$$

监测站或上注天线性能严重下降的定义:

$$State_{\mathrm{Ground}}=\{serious\mid P_{\mathrm{Ground}}\leqslant 80\}$$

4)危险后果分析。根据上述模型、参数和定义的事故类型,分析不同的异常状态对系统中各节点的影响,并判断是否会引起体系事故。

a. 确定性分析

以天线 v_4 性能降低为 40 为例进行确定性分析,研究其对其他节点和系统的影响。

首先根据式(5)、式(6)以及表 1 中的数据对受点卫星 v_8,v_9 和 v_{10} 的参数状态进行计算。v_8 的计算如下所示:

$$P_8=\min[g(\alpha_{48},P_4),h(\beta_{48},P_8)]=85$$

同理,$P_9=88$,$P_{10}=79$。

然后对 v_8,v_9 和 v_{10} 的受点 v_{13} 和 v_{14} 的性能进行计算,这两点都有多个受点,需要根据式(7) ~ (11)计算,v_{13} 的计算如下所示:

$$P_{13}=\min(SODP_{13},CODP_{13})=94.9$$

同理,$P_{14}=98.03$。

进一步,对 v_{13} 的受点 v_1 性能计算得到 $P_1=$

99.02。将系统各节点的状态参数与表3的事故表对比,最终,网络中各节点的性能如表4所示。

表4 v_4 性能降为40对各节点的影响

Tab.4 Effects of $P_4=40$ on all the nodes

v_1	v_2	v_3	v_4	v_5	v_6	v_7
99.02	99.02	99.02	40.00	99.71	99.80	99.80
v_8	v_9	v_{10}	v_{11}	v_{12}	v_{13}	v_{14}
85.00	88.00	79.00	99.88	99.80	94.90	98.03

表4数据显示 v_4 性能降低为40对卫星 v_8,v_9 和 v_{10} 影响较大,其他节点的影响不大。对比体系事故表,因为有三颗卫星性能明显下降,出现了Ⅱ类事故。

b. 随机性分析

确定性分析是 v_4 取固定值对其他节点的影响分析,随机分析则通过仿真,在 v_4 取较低值($\mu=20,\sigma=5$ 的正态分布)和较高值($\mu=80,\sigma=5$ 的正态分布)时各仿真1万次,如图4所示,得到其他节点性能的概率密度曲线变化情况如图5所示,从而分析 v_4 对其他节点的影响。

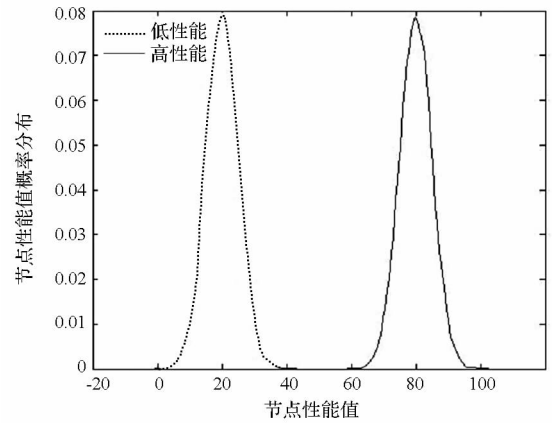

图4 v_4 性能概率密度曲线

Fig.4 Probability distribution curves of v_4 performance

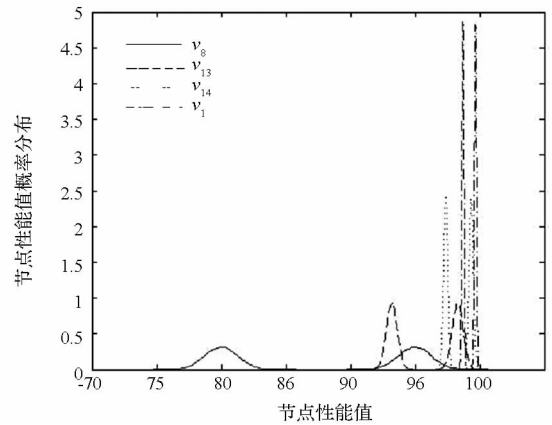

图5 观察节点概率密度曲线

Fig.5 Effects of v_4 performance change on other nodes

根据图5,v_4 由低值变为高值的过程中,对直接接受点 v_8 的影响最大(均值由80变化到了95);其次是间接受点 v_{13}(93.2到98.3)和 v_{14}(97.4到99.3);影响最小的是 v_1(98.7到99.7)。

同时仿真过程中统计的各类体系事故出现的次数表明,在 v_4 取较低值时必然导致事故Ⅱ发生,其他事故未发生;取较高值时没有任何体系事故发生。

下面分析组合失效作用下对体系的影响。假设 v_4 故障($\mu=20,\sigma=5$ 的正态分布)与卫星 v_7 故障($\mu=20,\sigma=5$ 的正态分布)同时发生。仿真1万次,6类事故的出现频率如表5所示。

表5 v_4 和 v_7 组合失效事故结果

Tab.5 Accident results caused by composed failure of v_4 and v_7

事故类型	Ⅰ	Ⅱ	Ⅲ	Ⅳ	Ⅴ	Ⅵ
出现频次	17%	100%	100%	84.2%	0	84.2%

表5表明:较之仅有 v_4 故障的情况,v_4 和 v_7 同时故障,体系事故类型明显增多:仅 v_4 故障时只出现了Ⅱ类事故;而 v_4 和 v_7 同时故障时,除事故Ⅴ之外,其他5类事故均有发生。各观察节点的性能如图6所示。

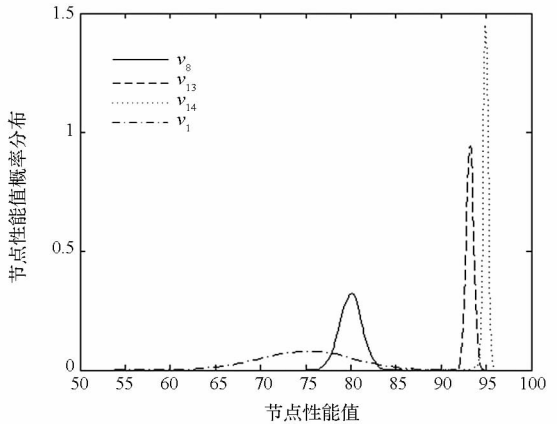

图6 v_4 和 v_7 组合失效事故结果

Fig.6 Effects of combined faults of v_4 and v_7 on other nodes

由图6可以看出,较之单点异常,v_4 和 v_7 同时故障时,v_8 和 v_{13} 变化不大;v_{14} 变化较大,而 v_1 变化最大,均值到了75左右,而由于上注天线对 v_1 具有很强的依赖性,所以其性能下降也很明显,从而Ⅳ和Ⅵ事故都有很高的发生频率。这是因为 v_8 和 v_{13} 与 v_7 没有较近的依赖关系;而 v_{14} 和 v_1 对 v_4 和 v_7 都有较强的依赖关系。

另外,可以根据导航服务性能的降阶和不同

事故发生的频次,将威胁等级分为非常严重、严重、一般、较轻四个等级。

表 6　威胁等级

Tab. 6　Levels of threat

威胁等级	定　义
非常严重	$P_{14}<60$ 或三种以上事故发生
较严重	$P_{14}<80$ 或两种以上事故发生
一般	仅有一种事故发生
较轻	$P_{14}>95$ 且无事故发生

根据上述威胁等级,v_4 性能降低为 40 的威胁等级一般;而 v_4 和 v_7 同时故障的威胁等级为非常严重。

5)事故原因分析。以前面组合失效的第 5 次仿真为例,此次仿真中发生了Ⅱ、Ⅲ、Ⅳ和Ⅵ类事故,事故原因调查即是由事故到原因的逆向过程,以查找Ⅳ类事故原因为例。

Ⅳ类事故的定义是"2 号上注天线 v_3 性能严重下降",首先,根据节点信息 $I_3=\{v_1\}$ 以及图 3 的网络和表 2 中的依赖关系强度可以看出,2 号上注天线 v_3 的性能完全依赖于节点 v_1($\alpha_{13}=1$)。在上例中,v_1 性能为 72.94。

而 v_1 自身没有故障或失效,因此继续查看 v_1 的供点,发现 v_1 的供点集合 $I_1=\{v_{11},v_{12},v_{13}\}$ 中,v_{11}(96.5)和 v_{13}(92.8)性能有轻微退化,v_{12}(17.9)性能则严重偏低。

而这几个节点并没有直接的故障或失效,因此继续向上查找它们各自的供点集合。对于 v_{12} 和 v_{13},分别再进行 1 次和 2 次类似的逆推找到了 v_7 和 v_4 分别为各自的根原因;但对于 v_{11},再经过 3 步又回到了 v_1,进入了一个循环,很难再靠人工或手动继续下去了。因此需要借助于计算机程序找到它的根原因是$\{v_4,v_7\}$。

至此,找到了Ⅳ事故的根源,即 v_4 和 v_7 性能太低。具体的分析过程如图 7 所示。

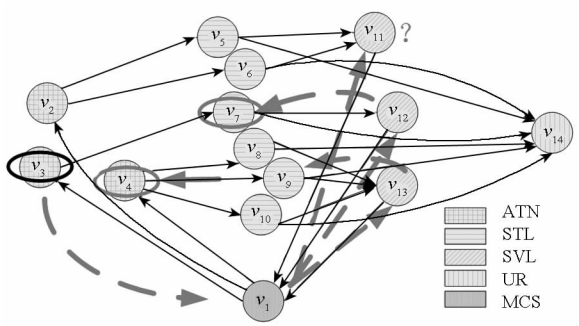

图 7　事故原因分析过程

Fig. 7　An accident reason investigation process

找到事故原因后,则可以通过提高根源节点的防护性能或调节改善对应链路的依赖关系来降低此类事故再次发生的可能性。

虽然仿真示例仅演示了方法对危险传播、组合失效的分析过程,但对交互异常即关系和接口异常、演化过程产生的危险同样适用。

4　结论

当前有关 GNSS 安全问题的研究绝大多数聚焦在具体攻防手段尤其是干扰抗干扰技术,很少有从系统全局或体系角度考虑 GNSS 的安全问题的。因此需要从体系的角度研究其安全性,重点关注并解决体系内系统间相互作用关系和涌现行为可能产生的安全风险,具体的包括危险传播、组合失效、交互异常和演化危险四类新问题。

文章提出了基于 FDNA 方法的 GNSS 体系安全分析方法和详细过程,并通过示例进行了演示,仿真示例结果证明了该方法对 GNSS 体系安全问题有很好的适用性:1)可以描述 GNSS 体系的基本信息和系统间的相互关系;2)能够描述和分析危险传播、组合失效、交互异常、演化危险等几类体系危险;3)可以借助于计算机技术来完成主要的计算和分析工作。

虽然 FDNA 对于解决 GNSS 安全分析问题具有较好的适用性,但本文只是一个探索的开始,仍然需要进一步的研究,如 GNSS 网络模型的进一步细化,考虑更多的节点和链路关系;网络的敏感性和重构分析。

参考文献(References)

[1] Kaplan E, Hegarty C. Understanding GPS: principles and applications [M]. Massachusetts: Artech House Inc Press, 2006.

[2] Thomas M, Norton J, Jones A, et al. Global navigation space systems: reliance and vulnerabilities[R]. London: The Royal Academy of Engineering, 2011.

[3] 张旺勋, 侯洪涛, 王维平. 基于 MATE 的卫星导航系统安全防护设计[J]. 系统工程与电子技术, 2013, 35 (6): 1231 - 1235.
ZHANG Wangxun, HOU Hongtao, WANG Weiping. MATE based design for protection of GNSS[J]. System Engineering and Electronics, 2013, 35 (6): 1231 - 1235. (in Chinese)

[4] 王东会, 徐博, 刘文祥, 等. 一种新的卫星导航星间链路测距体制及其定轨性能分析[J]. 国防科技大学学报, 2014, 36(1): 62 - 66.
WANG Donghui, XU Bo, LIU Wenxiang, et al. A novel navigation inter-satellite links ranging hierarchy and its orbit determination performance[J]. Journal of National University of Defense Technology, 2014, 36(1): 62 - 66. (in Chinese)

[5] Zhang W X, Hou H T. Study on safety & protection ability of GNSS receiver from the view of main materiel system[J].

Applied Mechanics and Materials, 2014, 511 – 512: 1048 – 1052.

[6] 严凯. GNSS 脆弱性仿真评估平台技术研究[D]. 上海: 上海交通大学, 2013.
YAN Kai. Research on GNSS vulnerability simulation and assessment platform technology [D]. Shanghai: Shanghai Jiaotong University, 2013. (in Chinese)

[7] 周经伦, 龚时雨, 颜兆林. 系统安全性分析[M]. 长沙: 中南大学出版社, 2003.
ZHOU Jinglun, GONG Shiyu, YAN Zhaolin. System safety analysis [M]. Changsha: Central South University Press, 2003. (in Chinese)

[8] 董豆豆, 周忠宝, 冯静, 等. 基于故障树的系统安全风险实时监测方法[J]. 国防科技大学学报, 2006, 28 (2): 111 – 116.
DONG Doudou, ZHOU Zhongbao, FENG Jing, et al. Real-time monitoring method for system safety based on fault tree [J]. Journal of National University of Defense Technology, 2006, 28 (2): 111 – 116. (in Chinese)

[9] 樊运晓, 罗云. 系统安全工程[M]. 北京: 化学工业出版社, 2009.
FAN Yunxiao, LUO Yun. System safety engineering [M]. Beijing: Chemical Industry Press, 2009. (in Chinese)

[10] 金光. HPN 基于网络结构的冲突关系[J]. 国防科技大学学报, 2002, 24 (4): 86 – 90.
JIN Guang. Structural conflicts in HPN [J]. Journal of National University of Defense Technology, 2002, 24 (4): 86 – 90. (in Chinese)

[11] 董豆豆, 周经伦, 赵炤, 等. 基于大规模贝叶斯网络的安全性分析算法[J]. 国防科技大学学报, 2007, 29 (4): 130 – 134.
DONG Doudou, ZHOU Jinglun, ZHAO Zhao, et al. Safety analysis algorithm based on large scale bayesian networks[J]. Journal of National University of Defense Technology, 2007, 29 (4): 130 – 134. (in Chinese)

[12] Perrow C. Normal accidents: living with high-risk technologies[M]. New York: Basic Books, 1984.

[13] Leveson N. Engineering a safer world: systems thinking applied to safety[M]. Massachusetts: Massachusetts Institute of Technology Press, 2011.

[14] Alexander R, Kelly T. Supporting systems of systems hazard analysis using multi-agent simulation [J]. Safety Science, 2013, 51 (1): 302 – 318.

[15] Redmond P. A system of systems interface hazard analysis technique [D]. Monterey, California: Naval Postgraduate School, 2007.

[16] Garvey P R, Pinto C A. Advanced risk analysis in engineering enterprise systems [M]. Florida: Chemical Rubber Company Press, 2012.

[17] Guariniello C, DeLaurentis D. Integrated analysis of functional and developmental interdependencies to quantify and trade-off ilities for system-of-systems design, architecture, and evolution [J]. Procedia Computer Science, 2014, 28: 728 – 735.

[18] Guariniello C, DeLaurentis D. Dependency analysis of system-of-systems operational and development networks[J]. Procedia Computer Science, 2013, 16: 265 – 274.

[19] Drabble B. Information propagation through a dependency network model [C]//2012 International Conference on Collaboration Technologies and Systems (CTS), Denver, Colombia, IEEE, 2012: 266 – 272.

[20] Guariniello C, DeLaurentis D. Communications, information, and cyber security in systems-of-systems: assessing the impact of attacks through interdependency analysis [J]. Procedia Computer Science, 2014, 28: 720 – 727.

[21] Wang Y, Zhang W X, Li Q. Functional dependency network analysis of security of navigation satellite system[J]. Applied Mechanics and Materials, 2014, 522 – 524: 1192 – 1196.

[22] Zhang W X, Wang Y, Li Q. An improved functional dependency network model for SoS operability analysis [J]. Applied Mechanics and Materials, 2014, 602 – 605: 3355 – 3358.