医院信息系统安全性需求分析与总体设计初探

朱　莹　　（江苏省中医院计算机室　210029）
金凌紫　朱鸿　（南京大学计算机软件研究所　210093）

摘要：安全性需求分析旨在需求分析阶段识别应用系统对安全性的特殊要求，为系统设计、实现和测试提供科学依据。本文以医院信息系统为例，探讨计算机应用系统安全性需求分析的方法以及针对安全性需求进行软件系统结构设计的方法。

关键字：计算机应用　安全性需求分析　软件设计

近年来，我国计算机应用在医院、铁路、航空、金融、工业控制等领域发展迅速。在这些应用领域中，计算机系统的正确、可靠和高效运行往往关系到人的生命财产和生态环境的安危，因此，如何保障计算机系统的质量，尤其是安全性，已成为一个迫切需要解决的问题[1]。这里，安全性是指不造成危及人的生命财产和生态环境的灾难性事故的性质。

本文通过一个医院信息处理系统为例探讨计算机应用系统安全性需求分析与针对安全性需求进行软件体系结构设计的方法与技术。

一、安全性需求分析

安全性需求分析的目的是在应用系统需求分析阶段识别计算机应用系统对保障安全性方面的特殊要求，从而为在设计和实现阶段针对这些特殊要求进行系统设计和在测试阶段针对这些要求进行系统测试提供科学的依据。

安全性需求分析的基础是系统功能需求描述。图 1 以数据流图的形式[2]，给出了一个医院信息处理系统的主要功能需求，其中各个处理部分的功能需求如下：

医护信息处理：(1)接收医生的医嘱，以病历的形式储存病人的基本信息、病史、治疗经过、各种检查报告、诊断书、医嘱及其执行情况等等；(2)根据医嘱向检查科室发出检查请求单，并接收检查处理部分输入的检查报告；(3)根据医嘱向药房输出处方，并接收药房关于处方处理结果的报告；(4)向住院处发出病人入院和出院通知，在出院时，向住院处提供住院治疗经过，以便计算病人住院治疗费用；(5)向护士输出病人的有关信息和医嘱，接收护士执行医嘱情况的报告；(6)向药材科发出药材供应请求。

检查信息处理：(1)接收病房检查请求单，对检查请求进行排队调度，向病房发出进行检查的通知，检查后，向病房发出检查报告；(2)向药材科发出药物供应请求。

处方处理：(1)接收病房处方，向药剂师输出处方；(2)接收药剂师关于处方处理结果的报告，发送给病房；(3)储存药物库存信息，及时向药材科发出药物采购请求。

病人帐务管理：(1)接收病房住院和出院通知，登记病人出入院信息；(2)在病人办理出院手续时，根据病房提供的治疗经历信息以及财务处提供的价格信息，计算住院费用；(3)向财务处报告财务情况。

财务管理：(1)以数据库的方式储存财务帐目，并提供各种查询功能；(2)接收住院处的财务报告；(3)向住院处提供该项医疗和各种药物的价格；(4)接收药材科药物采购开支的信息。

药材采购信息处理：(1)接收检查科室、病房、药房等单位的药材供应请求；(2)以数据库的形式储存药材库存情况；(3)根据药材供应请求和库存情况，安排药材的采购；(4)向财务处报告药材采购开支。

该系统还要求各个功能由分布在医院的各个科室、病房的计算机系统实现，并通过局域网连接起来。

安全性需求分析的过程大致可分为两个步骤，一是识别系统在使用中可能发生的潜在危险，称为潜在危险识别，二是分析可能造成灾难性事故的因素以及系统故障模式，称为因果关系分析。一般的系统潜在危险识别技术有多种，其中包括假设情况分析方法（What－if）、失

效模式及效应分析方法(FMEA)、潜在危险与可操作性分析(HAZOP)等等[3]。在将这些技术应用于软件系统时,还需根据软件的特点,考虑软件系统易发生的错误。

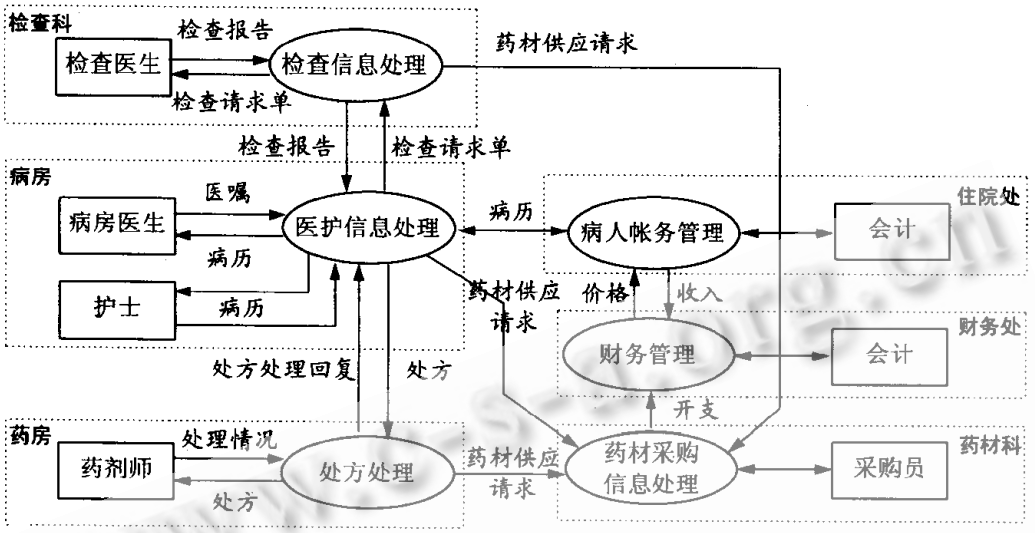

图 1　系统功能需求示意图

表 1　医院信息系统假设情况分析结果表

系统成分	故障	后果
检查信息处理	计算结果不正确	错误的计算结果传输给医护信息处理部分后,给医生错误的信息,造成医疗事故。
	存储的信息丢失	丢失检查请求单或检查结果报告都将造成病人检查时间的延误,从而造成医疗时机的延误。
	处理时间过分延迟	将造成病人检查时间的延误,从而造成医疗时机的延误。
医护信息处理	计算结果不正确	错误的计算结果输出给医生将给医生错误的信息,从而造成医疗事故。
		错误的计算结果输出给护士将造成执行医嘱的错误,从而造成医疗事故。
		错误的计算结果输出给处方处理部分,将造成投放药物的错误,从而造成医疗事故。
		错误的计算结果输出给药材采购信息处理部分,将造成药材供应的混乱,在特殊情况下,如果急救药材供应的混乱,将影响病人的急救,从而造成病人本可避免的死亡。
		错误的计算结果输出给病人帐务处理部分,将造成财务混乱,或者造成医院财产损失,或者引起经济纠纷。
	存储的信息丢失	病历的丢失将造成治疗的混乱,严重的情况下可能造成医疗事故。
		病历的丢失将造成病人帐务处理的混乱,造成经济纠纷和财产损失。
	处理时间过分延迟	处理时间的过分延迟,将造成医嘱不能得到及时处理,造成病人的检查、处方等不能得到及时处理,从而耽误医疗时机。
处方处理	计算结果不正确	错误的计算结果输出给药剂师可能造成药物使用的错误,从而造成医疗事故。
		错误的计算结果输出给医护处理部分,可能造成医生对处方处理结果的错误认识,从而影响医生对药物的选用,影响治疗效果。
		错误的计算结果输出给药材采购信息处理部分,将造成药物供应的混乱,严重的情况下可能影响病人的治疗。
	存储的信息丢失	处方的丢失将影响治疗。
	处理时间过分延迟	将造成病人不能及时得到药物,影响治疗,在给药时间特别重要的情况下,可能造成医疗事故。
药材采购信息处理	计算结果不正确、存储的信息丢失、处理时间过分延迟	错误的计算结果输出给财务处理部分,将造成财务混乱。
		错误的计算结果输出给采购员,将造成药材供应的混乱,在严重的情况下可能大范围地影响医院的医疗工作秩序。
财务管理	计算结果不正确、存储的信息丢失、处理时间过分延迟	在严重的情况下将造成财务混乱,财产损失。
病人帐务管理	计算结果不正确、存储的信息丢失、处理时间过分延迟	造成病人帐务混乱,在严重的情况下,或者造成医院财产损失,或者造成病人与医院的经济纠纷。

例如,软件系统中的信息处理子系统易发生的错误有:(1)计算结果不正确;(2)存储的信息丢失;(3)处理时间过分延迟等等。信息传输子系统易发生的错误有:(1)信息的丢失;(2)传输时间过分延迟;(3)传输的信息失真等等。针对这些易发生的错误,应用假设情况分析方法,我们分析了在上述医院信息系统中可能造成的后果,分析结果见表 1。

从上述分析可知,该系统的主要潜在危险是因医疗事故而致使病人的生命受到威胁,一个次要的潜在危险是因财务混乱而造成医院财产的损失和经济纠纷。下面我们针对前者应用故障树分析方法[3,4],进一步分析造成该危险的因素和系统故障模式。

故障树分析包括两个主要步骤,构造故障树和分析故障树。故障树的构造从对非期望事件的定义开始,即对系统设计者所不期望发生的具有潜在危险的事件进行描述和定义。这一事件与故障树的根节点相联系。然后,分析造成这一事件发生的直接原因,这些原因事件与根节点的子节点相联系,能够使父节点事件发生的原因事件的组合方式以布尔表达式的形式表示,并与父节点相联系。然后,对每一个原因事件进行上述分析,直至所有的原因事件都是原始事件为止。

图 1 给出了医院信息系统造成医疗事故的故障树。从该故障树可知,医护信息处理、检查信息处理、处方处理三个功能直接关系到整个系统的安全性,这是因为这

些功能的输出结果错误和计算时间的过分延迟都可能造成医疗事故的发生。此处输出结果的错误可能由计算错误或者存储的信息丢失而造成。

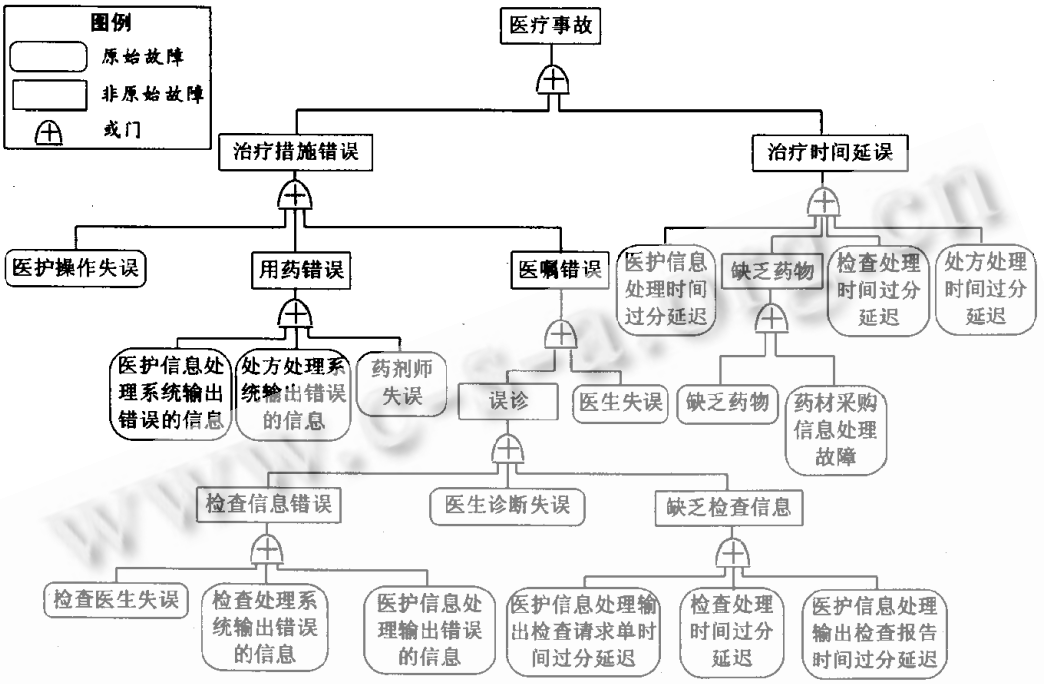

图 2　医院信息系统故障造成发生医疗事故的故障树

二、安全性设计

这一节讨论如何针对故障因素进行软件体系结构设计，从而降低发生危险的可能性，减少系统故障可能造成的危害。安全性设计是为了保障系统的安全性而在系统设计上所采取的特定措施。这些措施原则上应针对安全性分析中所发现的原始故障逐一采取防范措施，然而，在实践中，往往因客观条件的限制，不可能达到完全杜绝危险情况的发生。因此，安全性措施往往只能将发生危险的概率和及其可能造成的后果控制在一个可接受的范围之内。这样的措施可分为两类，一为预防性措施，即避免故障的发生，或降低发生故障的概率与可能性；二为减灾性措施，即减少发生故障时可能造成的损失。

针对医院信息系统的功能需求和安全性需求，我们把整个系统分解成六个子系统，分别完成六个主要功能需求，并分别安装在不同的计算机上，参见图 3。

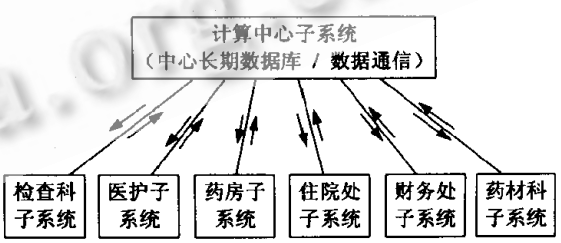

图 3　软件结构示意图

每一个子系统除了实现其功能的程序外，还具有一个局部数据库，保存能够在一定时间范围内相对独立地完成其主要功能的数据，参见图 4。这样，一方面可以实现空间上的分布性，另一方面还减少了各个部分之间的通信量，降低了对网络通信系统的依赖，也降低了各个功能子系统之间的相互干扰的可能性，从而降低了因系统中一个部分发生故障而影响整个医院的正常工作的概

率。因此，这一体系结构设计是一个减灾性措施。此外，如图 3 所示，系统结构中还包含计算中心子系统，其主要功能有二，一是完成各个子系统之间的数据通信，它除了完成通常的网络服务器的作用外，还要针对安全性需求分析中所发现的可能造成医疗事故的通信进行通信信息正确性的检查和通信时间延迟检查；二是提供一个中心数据库，作为各个子系统中的局部数据库的备份，长期保存系统中的各种数据。这两个措施前者是一个预防性措施，用以发现通信错误，预防由通信错误所造成的安全性事故，而后者则是一个减灾性措施，当一个子系统的局部数据库因故障而遭到破坏时，可使用中心数据库的保留备份进行回复，从而降低故障可能带来的损失。上述设计要求计算中心子系统具有较高的可靠性，在条件允许的情况下，可考虑由两台服务器分别完成数据通信和中心数据库功能。此外，在硬件设备的选择上还应该考虑到医护子系统、检查科子系统和药房子系统的可靠性要求高于住院处子系统、药材科子系统和财务处子系统。

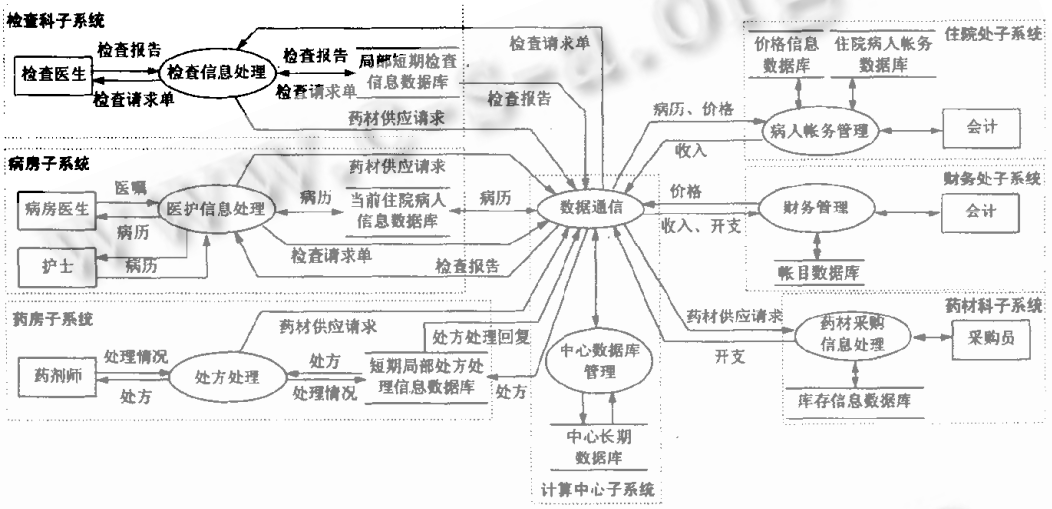

图 4　系统结构－功能关系图

三、结语

安全性需求分析是软件安全性研究中的一个关键问题，Leveson 等针对形式化需求规约提出了一套软件安全性分析的方法[5]。然而，由于书写形式化需求规约的困难和巨大开销，需要在需求分析更早的阶段(即形式化需求规约尚未形成之前)进行安全性分析。如何在这样的情况下分析计算机应用系统的安全性需求则是一个尚未解决的问题。本文以医院信息系统为例，探讨了应用一般系统安全性分析技术进行计算机应用系统安全性分析的过程和方法，还讨论了如何针对安全性需求设计计算机软件结构，以保障应用系统的安全性。值得指出的是，安全性分析应该贯穿于系统分析、设计和实现的全过程，在不同的开发阶段应该使用不同的分析方法。

参考文献

[1] 朱鸿、金凌紫，《软件质量保障与测试》，科学出版社，北京，1997 年 8 月。

[2] Yourdon, E., Modern Structured Analysis, Englewood Cliffs, New Jersey: Prentice－Hall, 1989.

[3] 梅启智、廖炯生、孙惠中，《系统可靠性工程基础》，科学出版社，1987 年 2 月。

[4] Vesely, W. E., et al., Fault Tree Handbook, Rept. NUREG－0492, 1981.

[5] Leveson, N., G., Safeware: System Safety and Computers, Addison－Wesley Publishing, 1995.

(来稿时间：1998 年 4 月)