安全核机制的分析*

黎忠文** 熊光泽

(电子科技大学计算机学院 成都 610054)

【摘要】 安全核是安全关键系统的一种新的安全保障机制．通过对安全核原理的分析，讨论了该核的概念及特征，包括其建立的原因、条件、安全策略及结构等重要内容．设计了一种可重用的安全核机制，能较好解决重用安全核带来的一系列诸如应用相关性、安全策略表达的非一致性等问题．

关 键 词 安全关键系统； 安全核； 安全策略； 核化系统

中图分类号 TP306+.3； TP311

长期以来，人们对软件安全技术进行了大量的研究，然而由软件引起的安全(satety)事故在安全关键系统中仍然频频发生，并随着软件应用的日益广泛，事故发生率也呈上升趋势，究其原因在于软件错误，特别是设计型错误已经成为现代系统故障的主流。从硬件借鉴的一些传统安全、可靠性分析法，如 SFTA(软件故障树分析方法)和测试法，已不适于解决设计型软件错误。据统计，对一般复杂度的软件，用测试法只能使软件错误率降低到每小时10^{-4}个，对于复杂度稍高的软件，测试法还达不到这种效果，而安全关键系统的错误率要求是每小时10^{-9}个，甚至有的是每小时10^{-10}个。世界许多国家正在积极探讨解决这一问题的办法，目前的研究分为两类：1) 研究新的软件工程技术和新的安全、可靠性分析法，以尽量减少设计型软件错误；2) 承认软件错误存在的前题下，研究保障系统安全。安全核属于第二类。

1 核的原理

safety(安全)核来源于信息保密系统中较为成熟的安全(security)核，它最先由著名安全学家 Leveson 等人提出[1]。当时 safety 核与 security 核相距甚远，更象是一个纯粹的监视器，没有安全保障及实施策略，Rushby 从 security 核视角看待 safety [2]。King 继承和发扬了 Rushby 的 safety 核概念[3]，并对 MSS 和 UVAR 两系统的安全进行了研究，在 MSS 上建立了 safety 核的雏型。

1.1 核机制的动因

核常用于实施分隔，security 核的设计思想是把系统的安全策略封装在系统的某组件(即 security 核)中，以免被应用软件(即用户)及操作系统侵入，造成泄密、数据的非法修改和对系统合法访问的拒绝。只要应用软件对系统的访问与安全相关，security 核都必须根据安全策略对其进行控制和处理[3]，以确保整个系统的安全。因此不需要系统其他组件的合作，security 核就能独立承担维护系统安全的重任，其原理如图1所示[4]。虽然 safety 有别于 security，它关心的是如何控制应用设备，以避免重大的生命财产损失和环境的破坏，而不象 security 侧重于信息的保密性、完整性和可用性，但是 safety 核与 security 核的原理类似如图2所示。所有应用软件对系统设备的访问，都必须经过 safety 核的审查控制，合法者予以支持，反之则采取相应的安全保障措施，维护系统安全，故能很好地避免软件错误造成的灾难后果。

2000年5月31日收稿

* "九五"国防技术预研基金资助项目

** 女 30岁 博士生

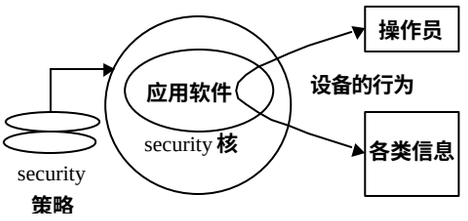

图1　security 核原理

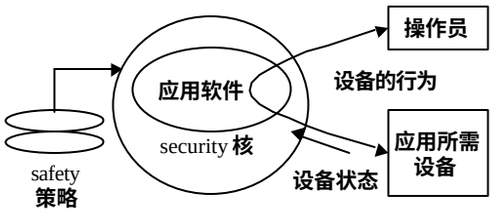

图2　safety 核原理

核机制的优势如下[5]：

1) 统一性：所有的安全策略都能由单一的代码集合来执行；
2) 可修改性：易于对安全机制作出改变和对这种改变进行测试；
3) 紧凑与可验证性：安全核只完成安全功能，其结构相对较小，有利于正确性的验证；
4) 单纯性：把原本由应用软件考虑的安全工作交由核处理，从而减少了应用软件的负担。

1.2　核化系统的特点

定义 1　当系统做了不希望做的事情时，定义为系统发生了消极型错误。比如，自动飞行控制软件在飞机处于飞行状态时，启动着陆装置。

定义 2　希望系统做的事情，系统没有完成时，定义为系统发生了积极型错误。

一般来说，积极型错误比消极型错误易于检查和评估，采用的方法也比较多。核机制与大多数传统的安全、可靠性方法不一样[6]，它善长处理消极型错误。事实上，无论安全核外其他系统组件如何工作，安全核都必须要维持安全策略的不变性。另外，无论安全核设计得多么好，都没法保证系统其他组件是否能正常调用。相反，通过对核的仔细设计能避免一些意外事件的发生。所以，诸如安全保障这类侧重于消极型错误处理的系统才利于核化。另一方面，安全策略的不变性决定了只有一部分安全策略能在核内实施，它们应满足的条件可形式化表示为[2]

$$\forall a \in op^{*} : P(op) \tag{1}$$

式中　op^{*}是核提供的所有功能组成的集合，其元素可以是核的一个或多个功能；$P(\cdot)$则表示核对 a 输入/输出的控制。事实上，核为系统提供的每一次安全服务，都可看成是一系列有序的核功能集。因此式(1)说明，无论系统其他组件(特别是应用软件)行为如何，核都要保持安全策略的正确实施。

2　safety 核的外部结构

security 核与 safety 核机制建立的出发点存在重要的区别：safety 核假设系统中没有恶意的应用软件——有意避开 safety 核对系统进行破坏。而 security 核则刚好相反，它是针对恶意软件设计的。因此它们在系统中的嵌入位置是不同的：Security 核往往被设计为操作系统的一部分，如著名的安全操作系统 SCOMP 和 UCLA；safety 核却类似于应用软件，其外部结构一般有集中式和分散式两种。

集中式结构中，safety 核被直接置于硬件平台上，如图3所示。这种结构适用于应用软件比较简单、能在单机上完成的情况。但是对于复杂的应用软件，比如大型图像处理，单机很难满足其计算要求，这时就需把应用软件中与安全(safety)控制无关的部分放在其他机上执行，于是形成了 safety 核的第二种外部结构——分散式，如图4所示。分散式结构的特点是 safety 核强烈的依赖于系统软件的支持(如果不用系统软件，safety 核就不得不提供类似远程管理的系统功能，这与简化 safety 核的总体目标相抵触)，当系统软件出错时，可能会导致 safety 核的非正常工作。为此引入

safety 核监视器的硬件机制，监视 safety 核和应用设备的状态，一旦发现 safety 核出现问题，立刻让系统进入安全状态。

以上两种结构各有优势，视应用的复杂度来选择。

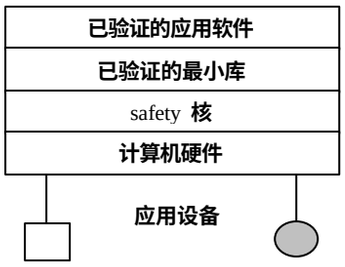

图3 safety 核的集中式结构

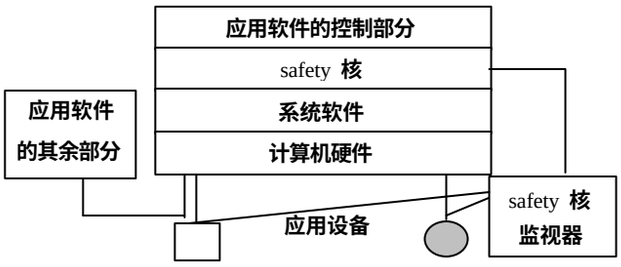

图4 safety 核的分散式结构

3 safety 核的实现

目前，safety 核都是针对具体的应用软件进行设计：核内安全策略直接取决于应用软件的安全需求。这种针对性很强的安全核不利于移植和重用，其每一次设计都需从头开始，做大量的重复工作。事实上，许多行业都已基本制定出相关的安全标准，比如 MIL-STD-882B 和 MCD 00-31、MOD 00-56、IEC-880等。属于相同行业的应用都遵守业内标准，其 safety 核的结构是相同的，只是参数不同而已。因此可以采用相同的 safety 核生成过程。此外，除了应用 safety 核外，系统也应有维持自身安全运转的 safety 核，能独立的应用。

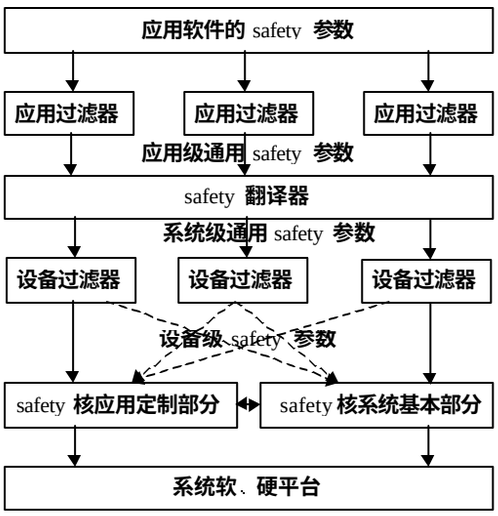

图 5 可重用 safety 核模型

本文把 safety 核分为应用软件定制和系统基本两部分，设计了可重用 safety 核的一种实现模型，如图5所示。其主要过程如下：各应用软件以参数的形式把安全需求通知系统；系统使用一系列的翻译器，如与应用相适应的过滤器、安全翻译器、设备过滤器等，把用户级的安全需求参数翻译成与应用设备相对应的安全参数，从而生成 safety 核的应用定制部分。safety 核的系统基本部分与系统级的安全有关，它为应用定制部分的生成提供支持。通过本模型，不同的应用软件均可构造相应的 safety 核，此过程既可实现重用，又有利于机器化。

4 结 束 语

safety 核是一种新的安全保障机制，它对现代安全关键系统的安全保障起着非常重要的作用，有广阔的应用前景。若 safety 与 security 核同样成熟，还需做大量的工作。

参 考 文 献

1 Leveson N G, Shimeall T J, *et al*. Design for safe software. In Proceedings AIAA Space Sciences Meeting, Reno, Nevada, 1983

2 Rushby J. Kernels for safety? Safe And Secure Computing Systems Symposium. London: Blackwell Scientific Publications, 1989: 210~220

3 周世杰，秦志光，耿　技. 办公自动化系统中的安全性. 电子科技大学学报，2000，29(2):201~204

4 King R. Safety kernel enforcement of software safety policies: [Doctor′s Thesis]. USA: University of Virginia, 1995

5 蒋继洪，黄月江. 计算机系统、数据库系统和通信网络的安全与保密. 成都:电子科技大学出版社, 1995

6 雷　航，熊光泽，刘锦德. 基于任务模块的实时软件可靠性模型. 电子科技大学学报，1997, 26(1): 69~73

Analysis of Mechanism of Safety Kernel

Li Zhongwen　　Xing Guangze

(College of Computer Science and Engineering, UEST of China　Chengdu　610054)

Abstract　Safety kernel is a new mechanism providing safety assurance in safety-critical system. In this paper, many important concepts and characteristics of safety kernel are discussed by analyzing kernel method, such as the reason for its building, the requirements for its actualization, safety policies and architectures, etc. In addition, a reusable safety kernel mechanism is designed in this paper, which can address common problems found in safety kernel supporting reuse, such as dependencies on specific application software, in harmony of safety parameter expressiveness, etc.

Key words　safety critical system;　safety kernel;　safety policy;　kernel structured system

---

(上接第48页)

Identification of Spectra Lines of Ni- and Co-like Ions of Laser-produced Ta Plasma

Wang Ruirong

(Shanghai Institute of Laser Plasma　Shanghai　201800)

Abstract　One-dimension spatial resolution soft X-ray spectra of laser-produced Ta plasmas is obtained by using a bent crystal spectrometer. Some resonance transition of the type 4f-3d in the Ni and Co-like isoelectronic sequence are identified. The Ni -like isoelectronic sequence wavelengths and Co-like 4f-3d resonance transition possible value are introduced. Wavelengths are measured with an uncertainty of $\pm 5 \times 10^{-5}$ nm.

Key words　bent crystal spectrometer；laser-produced plasma；soft X-ray；spectra identification