

信息屏障技术的示范装置

——能谱遮盖控制器

刘素萍 龚 建 胡广春 章剑华

(中国工程物理研究院核物理与化学研究所 绵阳 621900)

(2004 年 11 月 18 日收到 2005 年 12 月 7 日收到修改稿)

能谱遮盖控制器是信息屏障技术的示范装置,意在通过简单的实例说明信息屏障技术的双重作用以及为了实现这些作用所必需满足的基本设计要求,为该技术的深入研究奠定基础.简要介绍了样机的作用、设计要素和所采用的信息屏障措施.既要考虑到核查技术的有效性,又要尽可能堵塞各种泄密途径,同时还要使系统的设计信息公开化,使得核查人员能够通过系统设计认证,增加对核查结果的信任度.

关键词:信息屏障,能谱遮盖控制器,核查技术

PACC:0150M,0650D

1. 引言

在核不扩散和军控条约的核查监督中,越来越强调带有信息屏障的透明措施或核查技术^[1,2].这是因为:一方面,缔约国为了建立国际信用,促进互信,需要采取一些透明措施,主动发布信息,表明本国所从事的活动与其所申报的完全一致;另一方面,核不扩散和军控条约的核查监督活动会涉及到许多敏感信息,在保证有效核查的同时,必须采取必要的信息屏障措施,防止敏感信息的泄露.简而言之,在军控领域,没有百分之百的透明,只有将敏感信息过滤删除之后的信息才能够透明.

处理敏感信息的过滤删除需要用到信息屏障技术,该技术在“三边倡议”的推动下得到了蓬勃发展.“三边倡议”是美、俄、IAEA 三方于 1996 年签署的一个多边协议^[3],协议同意在不泄露敏感信息的前提下将储存在 Mayak 和 Savannah 河场地的多余武器易裂变材料交 IAEA 进行保障监督.也就是说,IAEA 在这两个军用材料库所采用的任何一项保障监督措施,都必须经过美、俄双方或单方的安全认证,以便将其入侵性控制在许可的范围.因此,美国能源部和国防部联合成立了信息屏障工作组^[4],几个武器实验室也相继开展了利用辐射指纹核查敏感对象(如核弹头、核部件、军用核材料)的核查技术,重点关注带有信息屏障的属性测量和模板测量技

术,相继推出若干带有信息屏障的核查设备,如 SNL 的 TRIS^[5]系统,BNL 的 CIVET 系统^[6],三大实验室(LLNL,LANL,PNNL)联合研发的 AMS/IB 系统^[7]等等.2001 年 8 月,以带信息屏障的属性测量系统样机 AMS/IB 为中心的 FMTTD(Fissile Material Transparency Technology Demonstration)在美国 LANL 举行^[8].演示意在向俄罗斯代表团说明:1)能够建立带信息屏障的属性测量系统(AMS/IS),其皮实的信息屏障足以让它应用于敏感对象的核查,而不泄漏敏感信息;2)AMS/IS 的建立可以满足核查方全面认证核查系统运行状态的需要.信息屏障技术在 FMTTD 演示中得到了充分的肯定.

2. 信息屏障的设计要求

信息屏障是指在对敏感对象的现场核查中,用来防止东道国的敏感信息泄漏给核查方,同时又能确保核查方对核查对象进行独立、准确测量的技术与过程^[8].从定义可以看出,信息屏障具有双重作用:1)防止东道国的敏感信息以任何方式泄漏给核查方;2)让核查方确信核查结果是准确、可靠的.第一个要求的实现需要用到皮实的屏障技术,第二个要求的实现则需要用到使人信服的认证技术.信息屏障技术中的“屏障”和“认证”是缺一不可的.

屏障是采取必要的手段(包括软件的、硬件的、行政的)防止核查过程中敏感信息的直接或间接泄

漏、屏障措施是非敏感的,需要透明。屏障必须做到防止敏感数据的泄漏,防止设备的非授权使用,防止设备软、硬件的非授权篡改(包括修改、替换、插入、删除等)。此外,屏蔽不能隐藏设备的运行状态指示,一旦运行状态出错,屏蔽要能及时防止敏感数据的泄漏或错误核查结果的提供。

认证是使核查方相信核查设备所提供的信息能够准确反映核查对象的真实状态的过程。认证需要确信核查设备是严格按照设计图纸装配的,而且在不同环境下,设计功能均能正常运行。认证还需要确信核查设备中没有任何让非法物品蒙混过关的隐藏机关,这就需要增加系统设计的透明度,包括软件(操作平台和应用软件)和硬件(元器件和系统),当然,也包括敏感数据的处理方法和过程。

信息屏障的作用和任务在核查设备的设计过程中必须充分考虑到,“防泄密”和“可认证”是系统设计的两大原则或称基本设计要求,它贯穿于系统设计的各个环节。为了满足这两个设计基本要求,通常可以采取下列措施^[49]:

- 1) 软、硬件的资料齐全,透明度高;
- 2) 模块化设计;
- 3) 软硬件功能单一、没有(或废掉)冗余;
- 4) 可信的 CPU(Trusted Processor);
- 5) 软件操作系统尽量小或没有;
- 6) 防止电磁辐射泄密或干扰;
- 7) 采用点对点连接,杜绝冗余接口;
- 8) 使用易失性内存;
- 9) 诊断和指示设备的运行状态。

另外,必要时可使用标签、封记来指示设备是否遭到篡改。核查设备或重要部件的备件可以让核查方对现场核查设备和事后详细检查设备进行随机抽样,有助于提高对核查设备的信任度。

3. 能谱遮盖控制器的研制

能谱遮盖控制器(简称“控制器”)是我们在过去几年研发的信息屏障技术的示范装置,意在通过简单的实例说明信息屏障技术的双重作用以及为了实现这些作用所必需满足的基本设计要求,为该技术的深入研究奠定基础。

3.1. 样机介绍

高纯锗 γ 谱仪所获取的能谱数据存放在多道分

析器 DSPEC 中,控制器的作用是从 DSPEC 中读取(且只读取)用户感兴趣的测量数据,如特定能段信息,并将读取的数据以能谱方式直接显示在显示器上。能谱遮盖控制器的作用框图如图 1 所示。图中箭头所指的方向表示信号的通讯方向: γ 射线探测器所获取的能谱数据存放在 DSPEC 的内存中;控制器与 DSPEC 的数据通信采用 RS-232C 串行通信,由控制器向 DSPEC 发出各项控制命令,并接收 DSPEC 发送的数据信息,经过控制器筛选过的数据信息,如特定能段的能谱信息,将通过 RS-232C 串行口输出到显示器上。

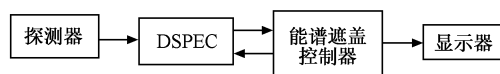


图 1 能谱遮盖控制器的作用框图

图 2 所示是控制器的实物照片。该装置除了完成能谱遮盖控制器的设计任务外,还在它的基础上设想了后续研发,即将之进一步研发成能谱过滤器,因此,在操作面板的制作上预留了一些设置,在下面的介绍中将用“预留”字样标出。

图 3 所示是控制器的操作面板,操作面板上各部分的功能为

1) 信号通信。最左边是三个通信串口:“输入”、“输出”和“控制”(预留)。“输入”和“输出”分别作为多道分析器 DSPEC 到控制器的信号输入口和控制器到显示器的信号输出口。

2) 数字键、 F_n ($n = 1, 2, 3, 4$) 功能键和显示窗口。中部的数字键、功能键 F_n ($n = 1, 2, 3, 4$) 和显示窗口用来验证控制器操作人员的身份,显示控制器的运行错误信息。

3) 能段档位、时间档位、输出方式选择开关。右上方的能段和时间档位选择开关提供四个能段和五个采谱时间的选项;右边中部的输出方式选择开关“输出”有“PC”和“ANA”(预留)两个档位。

4) 状态指示灯。右边中部是五个状态指示灯:RUN, HV, AC, CON(预留), POWER, 其状态意义列于表 1。

5) 命令开关。右边下部是三个命令开关:“高压”、“采集”和“控制”(预留)。“高压”用于显示、启动高压调节;“采集”用于启动/强制终结采集能谱。

表 1 指示灯的状态与意义

指示灯符号	符号意义	状态	指示意义
HV	高压	恒亮	高压正常
		闪烁	升/降高压 高压异常
		熄灭	高压关闭
AC	能谱采集	闪烁	采集能谱
		熄灭	采集结束
POWER	电源	恒亮	供电
		熄灭	断电
RUN	运行	AC 闪烁 ,RUN 恒亮	正在采集能谱
		HV 闪烁 ,RUN 恒亮	正在升/降高压
		熄灭	运行结束

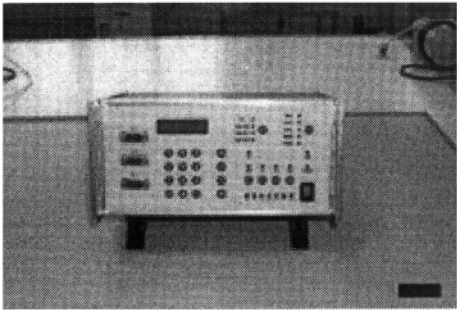


图 2 能谱遮盖控制器的实物照片

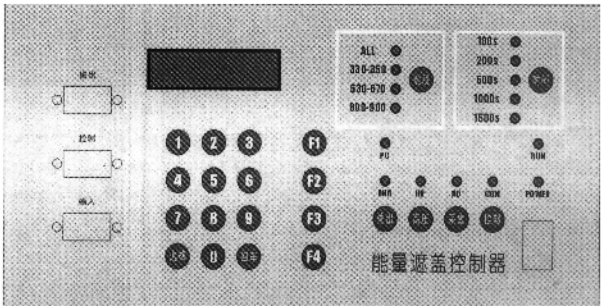


图 3 能谱遮盖控制器的面板

3.2. 设计要素

根据信息屏障的设计基本要求“防泄密”和“可核查”,结合控制器的作用和实验室条件,我们制定了控制器研制的基本原则——功能单一、冗余性小、安全性高、稳定性好。

- 具体地讲,研制考虑了下列要素:
- 1) 控制器只具备完成任务所必需的部件和功能,不得有冗余;
 - 2) 控制器应设置必要的操作开关和状态指示;

- 3) 一旦断电,控制器将不保留任何测量数据和分析数据,并能及时销毁多道内存中的原始数据;
- 4) 仅当合法输出设备(显示器)与控制器连接正常后,控制器才能将遮盖能谱数据输出,且数据只用于能谱显示,不得储存和作它用;
- 5) 控制器的使用和参数修改需经授权许可;
- 6) 在任何环节,控制器的操作只允许规定的动作发生,其他任何操作均无效。

3.3. 信息屏障措施

- 控制器的研发采用了以下的信息屏障措施:
- 1) 选择国产通用型单片机 AT89C51 作为控制器的微处理器,其上集成的部件均可用于本设计中,且各项资料详尽。
 - 2) 将 DSPEC 中的非易失存储元件改造为易失性的,将控制器中所有处理的数据保存在易失存储元件中,同时关联 DSPEC 与控制器的电源,使得切断电源时,所有相关的数据将全部丢失。
 - 3) 显示器采用经过特殊处理的笔记本电脑。这里“特殊处理”是指使用裁减后的 DOS 操作系统,只能安装唯一的能谱显示应用软件,除该应用程序所必须的控制键外,该电脑不得有任何输入外部设备,数据只用于显示,不得储存和作它用。
 - 4) 正常采谱结束后,控制器需要检查确定输出设备的合法性方能按相应的输出格式将数据输出。
 - 5) 模拟了一种现场核查设备的管理模式,将设备的操作人员分为三个级别,并分别赋予不同的操作权限:三级操作员(核查人员)能设定确保探测器正常运行的必要参数,如高压阈值和死时间参数(预留),进行能谱数据的采集操作;二级操作员(被核查方)只能设定控制器的能段选择、时间选择参数;一级操作员(第三方或双方代表),只负责密码的分配和修改。

4. 样机研制的启示

控制器的研发是对信息屏障技术的一次尝试,通过研发和试用,加深了对该技术的认识。信息屏障技术不是单纯的技术,而是一个概念。“防泄密”和“可认证”是核查系统的两大设计原则,亦称设计基本要求,它贯穿于系统设计的各个环节。也就是说,如果一套核查系统是带有严格意义上的信息屏障技术,则其系统设计必须是整体化的,既要考虑到核查

技术的有效性,又要尽可能堵塞各种泄密途径,同时还要使系统的设计信息公开化,使得核查人员能够通过系统设计认证,增加对核查结果的信任度.另

外,信息屏障的严格程度是弹性的,它依赖于敏感信息的界定、泄密风险和途径的评估、有关各方的信任程度等因素.

-
- [1] Comley C , Comley M , Eggins P *et al* " *Confidence , Security and Verification : The challenge of global nuclear weapons arms control* , " Prepared for the United Kingdom Ministry of Defence , AWE/TR/ 2000/001 .
- [2] David Spears , " *2001 Technology R&D for Arms Control* , " Published by U. S. Department of Energy , National Nuclear Security Administration and Defense Nuclear Nonproliferation Programs .
- [3] Shea T E and Laura Rockwood (IAEA) , Alexander Panasyuk (Russian) John Murphy(U. S) , " *The Trilateral Initiative : IAEA Verification of Weapon - Origin and Other Fissile Material Released from Defense Program* . "
- [4] The Joint United States DOE-DOD Information Barrier Working Group , " *The Functional Requirements and Design Basis for Information Barriers* (PNNL - 13285 , May , 1999) .
- [5] Seager K D , Mitchell D J , Laub T W *et al* " *Trusted Radiation Identification System* , " Presented in the 42nd INMM Annual Meeting .
- [6] Vanier P E , Peter Zuhoski , Leon Forman , Andrey Sviridov *et al* " *Study of the CIVET Design of a Trusted Processor for Non - intrusive Measurements* , " The Annual Meeting of the Institute of Nuclear Materials Management(Indian Wells , CA. July , 2001)
- [7] MacArthur D W , LANL , " *Attribute Measurement System With Information Barrier (AMS/IB) : Conceptual Design* . "
- [8] *Technical Overview of Fissile material Transparency Technology Demonstration-Executive Summary* , See http://www-safeguards.lanl.gov/FMTT/index_main.htm
- [9] Geelhood B D , Pitts W K , Hansen R R *et al* " *Design Guidelines for Authenticable Systems* , " Prepared for the Defense Threat Reduction Agency and the U. S. Department of Energy (PNNL-13386 , July 2001)

A spectral blanking-out controller for demonstration of information barrier technology

Liu Su-Ping Gong Jian Hu Guang-Chun Zhang Jian-Hua

(*Institute of Nuclear Physics and Chemistry , China Academy of Engineering Physics , Mianyang 621900 , China*)

(Received 18 November 2004 ; revised manuscript received 7 December 2005)

Abstract

Information barrier technology has become more and more important in the R&D of radiation fingerprint verification associated with classified items such as nuclear warheads , nuclear components and military – used nuclear materials. The function of information barriers is two-fold : one is to prevent the classified information from leaking out ; the other is to provide creditable verification. To fulfill these two functions , the information barriers for a viable verification system (including all its hardware and software) must be designed on the basic principles of protecting classified information and the ability to authenticate. The Spectral Blanking-out Controller (SBC) is developed to illustrate the two functions of the information barriers and to explore some practice measures to meet the required design fundamentals. This paper briefs the task assigned to the SBC , the specific design concerns and the practical information barrier measures. The R&D of the SBC embodies the concepts of information barrier technology and has to conform to the basic guidelines : If a verification system is expected to possess strict information barriers , the design of the system must be integrative with due considerations given to the factors such as the efficiency of the verification technique , the possible measures to protect the classified information from directly or indirectly leaking out , the complete openness in all aspects of the system for the inspectors to authenticate the system for the sake of achieving certain degree of confidence on the verification results.

Keywords : information barrier , spectral blanking – out controller , verification technology

PACC : 0150M , 0650D