新闻回顾

韩国核电站信息遭泄露

官方称已提升安保水平

本报综合报道 自去年12月15日起,一个自称“反核电集团”的网络用户多次在“推特”上公开韩国水力原子能公司(KHNP)的内部资料,包括古里和月城核电厂的设计图、说明书等重要资料,核电厂10000多名员工的名字、工号、职位、入社时间、退休时间、手机号码等信息也遭到泄露。

12月19日,韩国产业部发布网络危机“关注”预警,并要求各级机关和保安监控中心进入紧急工作状态。12月22日,韩国核电厂运营商准备进行模拟演习,以测试应对网络攻击的能力。

12月24日,KHNP在首尔总部以及古里、月城、韩光、韩蔚等4个核电本部成立了紧急状况小组,进行24小时监督;两天后,KHNP表示,未出现异常,但网络攻击随时都可能发生,将继续保留紧急状况小组,直至风险消除。

12月28日,KHNP社长赵石表示,自12月9日公司被恶意代码电子邮件攻击以后,网络攻击比以前增多了。但“反核电集团”并不会影响核电站运转,只是在攻击日常业务网。

12月30日,韩国能源部长发表声明,攻击核电厂控制系统的这种恶意软件最有可能是工作人员未经授权使用U盘而引入系统当中。韩国官方表示已从一些核电厂控制系统清除一种“电脑蠕虫”,并提升安保水平。

相关链接

信息泄露不只在韩国

据公开报道,世界核电领域近年来发生了多起重大信息安全事件。

2001年1月9日 英国核电厂被黑客攻击,改变了控制系统的访问控制。

2003年1月 美国Davis Besse核电厂被蠕虫控制网络长达4小时50分钟,无法正常访问安全参数显示系统。

2006年8月 美国Browns Ferry核电厂3号机组被黑客攻击,造成反应堆循环泵和冷凝水除盐装置控制器失灵。

2007年5月19日 黑客攻击俄罗斯核电厂网站,这次有计划的行动封锁了几乎所有能够进入自动辐射环境控制系统(ASKRO)的路径。

2008年3月7日 美国乔治亚州Hatch核电厂2号机组设备监控系统被攻击,控制系统数据被重置,放射性核燃料棒的冷却装置失灵,自动安全系统关闭。

2010年9月 “震网”蠕虫病毒攻击伊朗的铀浓缩设备,这种病毒专门为袭击离心机而设计,它突然更改了离心机中发动机的转速,进而摧毁离心机的运转能力并使其无法修复。

2012年2月21日 英国核电厂被攻击,机密数据泄露。

保障信息安全需设几道闸?

王晓峰

图为韩国新古里核电站。 资料图片

韩国核电站信息泄露事件,为应对信息时代的核安全风险再次敲响警钟。计算机网络技术在核电领域的广泛应用实现了信息收集的自动化和系统控制的智能化,提高了核电厂运行的效率,增强了安全性和可靠性。

然而,新的安全问题也随之而来:系统和网络可能遭受的黑客、病毒、蠕虫、木马等偶然或者恶意、有预谋的网络攻击,使得核电厂的系统、网络和设备的可靠性、可控性和可用性以及信息和数据的保密性、完整性受到损害,甚至可能导致核设施和核电厂被强制关闭,威胁生命和环境安全甚至国家安全。

信息安全对于关乎国计民生的核电行业来说至关重要。为应对核电系统信息安全威胁,2011年,国际原子能机构核安全系列第十三号导则(IAEA nuclear security series no.13, INFCIRC/225/Revision 5)——《关于核材料和核设施实物保护的建议》的第五次修订版中专门增加了一项关于信息安全的规定:用于实物保护、核安全以及核材料衡算和控制的计算机系统和网络必须采取措施加以防护,以应对网络攻击、数据操纵或篡改等威胁。2011年4月《核安全公约》第五次审议大会上,IAEA提请各缔约方需共同关注的问题有10项,其中一项即为:各成员国需加强对核电行业信息安全和网络安全的关注,应颁布并执行相关政策、法规,对本国所受的网络安全威胁进行评估并确定对策,同时增加信息安全专业的工作人员数量。

放眼世界,美国政府一直把核电厂列为信息安全保障的重点关键基础设施,多次发布行政令强调核电厂是信息安全重点保护对象。例如2001年英国核电厂被黑客攻击后,美国核管会(NRC)发布了《核电厂临时保障措施和安全补偿措施》(NRC Order EA-02-026),其后的2003年、2007年、2010年也分别发布了《核电信息安全设计基准威胁》(NRC Order EA-03-086),《核电厂网络信息安全过渡性审查导则》(DI&C-ISG01),《数字计算机、通信系统和网络的安全保护管理导则》(RG5.71)等法规。

我国核电发展在不断的探索过程中形成了与国际接轨的核安全法律法规体系,这些都为核电安全发展奠定了良好的基础。然而,综观我国的核安全法规体系、国家核安全局部门规章、核安全导则和技术文件,仅有的关于计算机的导则是国家核安全局于2004年发布的HAD102/16《核动力厂基于计算机的安全重要系统软件》,涉及到了软硬件、仪控系统的安全性问题,但这只是信息安全问题的一部分,涉及到计算机硬件、软件、网络、系统等信息安全方面的要求还比较少,而针对核电厂网络信息安全方面审查和监管的要求和规范尚属空白。

以邻为鉴,可以少走弯路。新形势下如何加强核电厂信息安全监测、预防、应对、缓解和恢复以及应急响应等工作的方法手段和标准要求,进一步健全和完善我国的核安全审查、监管法规和标准体系,对保证我国核能与核技术利用的持续安全发展具有重要意义。要想避免类似事件发生,核电厂网络安全应做好以下几方面的工作。

一是在纵深防御和分等级保护中加强核电信息安全工作

纵深防御是核安全技术的基础,贯穿核安全的全部活动,同样也应严格执行于核电系统的信息安全防御中。美国《数字计算机、通信系统和网络的安全保护管理导则》的细则中明确要求,必须为系统设置多层次安全边界,也就是将系统进行逻辑分层并将之置于多重保护之中,提供深度防护,即使一种手段失效,还有其他安全手段进行保护。

但导则并没有给出具体如何进行逻辑分层的实施建议,而国际工业系统标准中有较详细的分层次建议,这一标准将系统分为5个层次,每层采取一定的信息安全防护措施,搭建逐级深入的安全策略。

美国联邦法规《数字计算机、通信系统和网络的安全保护法规》(以下简称《安全保护法规》)要求数字计算机、通信系统和网络中的信息资产按照重要性等级及实际安全需求进行分类管理,分级实施保护策略。同时只允许数据单向流动,数据流必须从高安全级别系统流向低级别系统。《数字计算机、通信系统和网络的安全保护管理导则》则详细地将信息系统和设备等数字资产按重要性划分为4级,其中,与核安全、核安保、应急(包括应急功能的场外通信)相关的支持系统和设备被称为关键数字资产和关键系统,应给予最高级别的防护。

对系统进行评估和定级是个复杂而关键的过程,需要对所拥有的数字化信息资产进行系统分析和梳理,根据系统基础资源和信息资源的价值大小、用户访问权限的大小、各系统重要程度的区别、系统承载业务情况等进行划分和定级,设计合理的、满足等级保护要求的总体安全方案,并制定出安全实施规划。我国监管部门应加强审查能力建设。

二是综合运用管理、技术和操作3方面资源建立信息安全保障体系

在《安全保护法规》的大纲中规定,一个完整而有效的信息安全保障方案应该包含3方面要素:技术、操作、管理。

其中,技术资源涉及到硬件、软件、协议;涉及到终端网络与应用系统以及信息安全产品的开发集成、配置与运行维护等;操作包括媒介保护,实体隔离,人员安全措施,系统运行控制日志和记录,系统和信息完整性防护,应急计划,事件响应,安全意识培养,技术培训等;管理包括各种法律、行政手段,例如安全体系、政策、规章制度的建立,安全评估和风险管理,数字资产的增加和修改等。只有综合运用这3个要素,通过合理配置各项资源,才能建立一个管理与技术相互协调的信息安全保障体系。

三是重视信息安全教育与人才培养,促进建立信息安全文化

美国《安全保护法规》要求,确保所有工作人员具有信息安全意识,将信息安全作为他们的职责和责任,并接受定期网络安全培训。必须建立专门的信息安全部门,明确人员角色和职责。

事实上,工作人员具备高度信息安全意识和采取有效的安全措施是系统和网络安全的第一道防线;同时,培养信息安全专业人才也至关重要。一支雄厚的安全技术队伍是核行业信息化建设的必备条件,从业人员不仅要自身掌握扎实的信息安全技术,而且应通过教育培训、应急演习等,增强应对信息安全突发事件的能力。

四是加强应急能力建设,有效应对信息安全突发事件

美国《安全保护法规》规定各核电厂必须加强信息安全应急能力建设:一是制定详细的信息安全应急方案,方案中的内容需包括事件响应和恢复措施,如何识别、侦查和应对网络攻击,如果缓解和减轻危害,如何修复漏洞以及如何恢复受到攻击的系统和网络等;二是建立网络安全事件响应组织(CSIRT),专门应对突发事件,并从发生的事件中吸取经验教训,从而制定和修改信息安全方案。

应急能力建设需要从多个层面来加强:例如不断完善应急预案,加强培训和演练;建立定时备份与定期数据恢复机制;建立必要的重发机制来保证信息传递中的完整性;通过建立灾难备份系统来保证信息系统在受到灾难性攻击时的可用性;通过设置黑名单的方式将信息系统中多次出现的非法用户排除在合法使用集合之外。

五是加强信息安全合作交流,实现信息共享

10多年来,在美国核电信息安全法规标准的演变过程中,NRC一直保持着与美国国土安全部(ICS)、美国核能研究院(NEI)和美国联邦能源管理委员会等联邦机构的密切配合,多方机构协调开展工作,以应对网络安全这一持续存在且不断演变和发展的威胁。

同时,NRC与美国计算机应急响应组织、工业控制系统网络应急响应组织共享网络木马、漏洞、病毒等威胁信息,能够对潜在的威胁因素做出快速反应,并用以评估预警等工作。

近年来,我国信息安全的管理在不断地发展和健全中,先后成立了全国信息安全标委会和若干信息安全评估机构。国家计算机网络应急技术处理协调中心联合国内重要信息系统单位建立了信息安全漏洞信息共享知识库,定期更新和发布网络病毒、木马等信息。

核能行业应加强与这些机构的密切合作,共享网络攻击信息,加强预警,共同分析攻击信息,控制问题的影响范围,以更好地应对网络威胁的攻击。

同时,核安全无国界,加强国际合作与交流也是必要的。

核心看点

专项行动之后就能松心?

王争亚

今年5月,针对南京探伤放射源丢失事故暴露的问题,环境保护部在全国组织开展了放射源安全专项检查行动。据相关部门介绍,为期半年的放射源安全专项行动发现并解决了不少问题,消除了一批安全隐患,取得了明显成果。

由此可见,在一个时期内集中性地开展某项专项行动,以推动重点难点环境问题的解决,无疑是非常及时、也是十分必要的。

然而,眼下的问题是,专项行动之后我们该怎么办?是满足于已经取得的成果,以为就此可以高枕无忧,还是乘势而上,继续保持专项行动中的工作状态和好势头?这无疑是摆在各级环保部门和众多核技术应用单位面前一个十分现实的课题。

面对这一课题,大部分人头脑清醒,注重在成绩面前找差距,持续保持强有力的监管力度。但也有一些监管部门和被监管单位从认识到实践,都还存在着一些偏差。有的人认为,此次专项行动,各级部门对涉核单位翻箱倒柜地折腾了好几遍,该发现的问题发现了,该消除的隐患消除了,在“歇歇脚、松口气”的思想支配下,工作随即出现了松劲的现象;还有人认为,自己的辖区内,就那么屈指可数的几枚低类别放射源,出不了什么大事,消极保安全的思想又重新露头;还有一些企业一旦把上级的检查对付过去之后,短板依旧,问题如故。

类似这种的“专项行动来了紧一阵、专项行动过后松一阵”的现象恐怕还绝非个别,它折射出一些监管部门和被监管单位工作指导思想上的偏差。加强监管究竟是为了确保辐射环境安全,还是为了应付一两次专项行动?接受监管到底是为了杜绝消除辐射安全隐患,还是为了把上级的检查对付过去?看来,确立什么样的工作出发点和着眼点的问题,在一些部门和单位并没有真正解决。

由此也可以看出,工作指导思想不端正是监管不持续、不经常的根源。从根本上讲,监管者工作出发点、着眼点不端正的问题远比辐射安全方面本身存在的漏洞具有更大的危害性。

专项行动不是工作的终点,而是新的起点。专项行动之后如何采取更加积极的行动和常态化的措施来确保辐射环境的安全?

我以为应当从以下几方面入手:首先,要把专项行动中的一些有效做法梳理固化好。专项行动好比一场战役,能够取胜,得益于采取的措施正确给力。因此要把这些管用有效的举措固化成一种常态化的机制,真正做到打一仗、进一步,使专项行动的成果能够进入经常化的工作实践之中。其次,要把专项行动中发现的问题跟踪解决好。要对纳入整改的问题企业紧盯不放,锲而不舍地加大督导力度,确保规定的时限内使问题能够整改到位,真正做到问题不解决不撒手。再次,要把进一步加强经常性监管的措施研究制定好。核与辐射安全监管重在经常、贵在经常、也难在经常。因此,专项行动不应该成为一种常态,只有把工作的着眼点放到注重平时、注重经常的思路上来,环境监管的基础才能更加扎实、更加稳固。因为从某种意义上讲,运动式、突击性的工作方式只是治标之策,而经常性、基础性的工作才有治本之效。

总之,那种以为专项行动之后便可一劳永逸、高枕无忧的思想是万万要不得的。辐射环境监管只有进行时,没有完成时。唯有坚持经常,久久为功,确保辐射环境安全的目标才能得以实现。

核讯快览

于敏获2014年国家最高科技奖

多年从事原子核物理理论研究

本报综合报道 2014年度国家科学技术奖励大会日前在北京举行。中国著名核物理学家、核武器研究和国防高技术发展的杰出领军人之一于敏院士荣获2014年度国家最高科技奖。国家最高科学技术奖得主每人奖金500万元人民币,此前已有24位著名科学家先后获此殊荣。

于敏院士生于1926年8月,天津市宁河人,1949年毕业于北京大学物理系。历任二机部九院理论部副主任、九院副院长、核工业总公司科技委副主任等职。现任中国工程物理研究院高级科学顾问。他于1980年当选中国科学院数学物理学部委员(院士),1999年获“两弹一星”功勋奖章。

上世纪50年代,于敏率先在国内开展原子核物理理论研究,与合作者提出了原子核相干结构模型,填补了中国原子核物理的空白。他曾与北京大学杨立铭教授编辑出版中国第一部原子核理论专著《原子核理论讲义》。他还是中国惯性约束聚变和X光激光领域理论研究的开拓者。

此外,在氢弹突破中,于敏组织攻克实现氢弹自持热核燃烧的关键技术,形成从原理、材料到构型完整的氢弹物理设计方案,带领科研队伍完成了核装置的理论设计,并定型为中国第一代核武器。“氢弹突破和武器化”项目获1985年度国家科学技术进步奖特等奖。

广西举行核事故应急联合演习

同时启用4个核应急指挥中心

本报讯 1月13日,广西壮族自治区举行“红沙-2014”广西核事故应急联合演习,这是广西首次举行核事故应急演习。

演习事故情景模拟核电站遭受强台风袭击,导致核电站失去两路场外电源,1号机组发生放射性泄漏事故,且机组故障进一步发展,最终导致3道屏障功能丧失,放射性物质向环境释放,影响到周围环境。自治区核应急指挥部报国家有关部门批准启动一级应急响应,同时为了防止核电厂下风向区域的公众受放射性污染危害,将核电厂周围5公里范围内的公众撤离,5公里~10公里范围的公众实行就地隐蔽。经过抢修,核电厂事故机组故障修复,放射性物质停止向外释放,应急响应行动终止。

据了解,此次演习同时启用自治区、防城港市、钦州市以及防城港核电厂等4个核应急指挥中心,自治区42个部门和单位、广州军区、驻桂部队、广西军区、武警广西总队等参加了演习,动用参演人员约1800人以及车辆、船舶、大型装备等150余台(辆),组成11个专业组按照预案和实施程序开展应急响应和处置。

演习检验了自治区各级核应急委员会开展核应急指挥决策和处置的能力,锻炼了核应急队伍,为确保防城港核电厂的安全运行筑牢最后一道防线。防城港核电厂是国家西部大开发的重点工程,是西部少数民族地区建设的第一座核电厂,它的投产运行,对广西调整能源结构,实现可持续发展均具有重要的意义。

据悉,广西壮族自治区党委、政府高度重视核应急工作,自治区政府成立了由42个成员单位组成的自治区核电厂核事故应急委员会,负责领导、组织、协调全自治区的核事故应急管理工作。

目前,广西已形成全区核应急组织体系、协调架构和预警机制,建设自治区放射性分析实验室及移动监测系统,在核电厂周边建设防城港前沿站及12个自动监测子站,建立了上下联通的各级核应急指挥中心,形成全区核应急技术支持和救援响应能力。 梁玉桥 孔晓梦

核反应堆“心脏”实现中国造

打破国外长期技术垄断

本报讯 由中国广核集团(以下简称中广核)牵头组织的国家科技支撑计划项目——“百万千瓦级压水堆核电站控制棒驱动系统研发”科研项目近日通过了科技部组织的专家组验收评审,这意味着中广核已掌握适用于12英尺和14英尺燃料组件的控制棒驱动系统关键技术,打破了国外长期的技术垄断,实现了核反应堆“心脏”的自主化和国产化。

据介绍,控制棒驱动系统是核反应堆本体中唯一动作的部件,承担着反应堆启动、功率调节等控制和保护职责,是反应堆安全运行的“心脏”。此前中国在运和在建的百万千瓦级压水堆核电机组中,这一设备均使用国外品牌技术,关键部件和材料要从国外进口。

此次“百万千瓦级压水堆核电站控制棒驱动系统研发”项目下设4个课题,分别从设计技术、金属材料、有机材料及制造技术4个方面,开展控制棒驱动系统的设计自主化和材料、制造国产化研究。4个课题分别由中广核所属中科华核电技术研究院、中科院金属研究所、吉林大学和成都瑞迪机械实业有限公司承担。

据了解,项目研制成果适用于12英尺和14英尺燃料组件的控制棒驱动机构及棒控棒位系统,达到或超过国外同类设备的技术水平。2014年8月,中科华核电技术研究院正式签订阳江5、6号机组棒控棒位系统供货合同,顺利实现了这一成果的工程应用。

来自中科院、上海核工程研究设计院、航天科工306所、中国机械工业联合会、上海交通大学、中国核工业集团、国家核电技术公司、东方电气集团的多名业界专家组成的专家组对项目进行了验收,对项目的执行及其研究成果给出了较高评价,一致同意项目通过验收。 综编

福建举行核应急军地联动演练

分阶段重点演练5个课题

本报讯 福建省核应急办与驻榕某部队近日在福州联合开展了一场核应急军地联动演练。

演习以模拟福建省某核电厂发生核事故需要动用部队支援为背景,分阶段重点演练了5个课题:一是军地指挥协调,包括军地应急指令传送、部队动员发动、军地监测数据对接和传输等;二是辐射监测,包括军地联合开展巡测和采样,并将有关监测数据上传至福建省核应急指挥中心;三是工程抢险,由部队出动大型重型机械化桥,模拟实施应急损毁桥梁铺通;四是交通保障,模拟调用部队车辆支援福建省交通运输保障组;五是去污洗消,在现场开设了两个车辆洗消点、两个人员洗消点和1个特殊装备洗消点实施去污洗消作业。

演练中,福建省核应急指挥中心与参演部队行动现场保持视频通讯联系,并实时接收辐射监测数据。

曾咏发