发射场测试发射指挥监控系统可靠性分析

单锦辉　曹宗胜　张爱良　牛胜芬
（北京特种工程设计研究院）

摘　要　测试发射指挥监控系统（简称 C^3I 系统）在发射场发挥着重要的作用，对其可靠性提出了很高的要求。本文对 C^3I 系统可靠性分析方法进行研究，提出 C^3I 系统可靠性评定指标，收集 C^3I 系统可靠性数据，对 C^3I 系统可靠性进行分析，查找其中存在的薄弱环节，分析造成其可靠性下降的原因，并提出可靠性工作建议。

关键词　测试发射指挥监控系统　C^3I 系统　可靠性　分析
分类号　TP311　**文献标识码**　A　**文章编号**　1674-5825（2010）02-0058-07

1 引言

C^3I 系统是指挥、控制、通信与情报等（Command Control Communications and Intelligence）组成的系统。后来，C^3I 系统发展成为 C^4I 系统，即由指挥、控制、通信、计算机与情报等（Command Control Communications Computer and Intelligence）组成的系统。随着科学技术的发展，C^4I 系统的功能和含义也在不断地扩充与完善，继 C^4I 之后又出现了一体化 C^4ISR 系统，即由指挥、控制、通信、计算机、情报、监视、侦察等（Integrated Command Control Communications Computer Intelligence Surveillance and Reconnaissance）组成的系统。

发射场测试发射指挥监控系统是发射场测试、发射的一个指挥、监测、控制平台。该系统在发射场发挥着重要作用，对于载人航天工程，该系统工作正常属最低发射条件之一。该系统的主要功能是：保障决策、指挥、管理火箭、航天器的技术准备和发射；监测测试、发射中的灾害和危险事件、重要设备的性能参数、重要场所的温度、湿度，以及设备的工作状态，出现危险情况能及时报警；控制测试、发射进程和单体设施的动作；监视显示危险场所、关键部位和重要岗位场景；实况显示总装、转运、加注和发射过程；数字显示火箭、航天器测试、发射的技术参数、工作进程；模拟显示火灾发生位置；进行对上、对下的信息交换和数据处理、管理等[1]。通常将发射场测试发射指挥监控系统简称为 C^3I 系统，其实目前它已具备了 C^4ISR 系统的部分功能，本文仍采用传统的简称。

我国可靠性工作起步较晚，历史原因导致我国发射场 C^3I 系统可靠性设计分析工作也相对滞后，缺少系统的可靠性设计指标。近年来，随着我国航天事业的迅速发展，各发射场任务密度不断增大，这对 C^3I 系统的可靠性提出了更严格的要求。需要更加准确地分析 C^3I 系统的可靠性现状，掌握其可靠性水平，以便保证试验任务的圆满完成。

文献[2]分析国外航天发射场可靠性工程现状特点及发展趋势，以及我国航天发射场可靠性工程现状与特点，论述我国未来发射场可靠性设计的必要性，提出我国未来发射场可靠性设计指导思想，阐述我国未来发射场可靠性设计工作要点与组织实施，提出我国未来发射场可靠性设计预期目标。文献[3]研究中国载人航天工程航天发射场地面设施、设备安全性可靠性复核思路，分析航天发射场地面设施、设备可靠性管理工作现状；针对当前我国航天发射场地面设施、设备任务可靠性复核工作，推荐可靠性复核方法，提出可靠性复核的原则，阐述可靠性复核的总体思路与主要步骤；提出关于加强可靠性复核基础能力建设的启示。文献[4]研究航天发射场可

来稿日期：2010-04-28；修回日期：2010-06-09。
作者简介：单锦辉（1970.06-），男，博士，高级工程师，主要从事 C^3I 系统设计、软件质量管理工作。

靠性、安全性评估与分析技术，并对航天发射场供配电系统、火箭推进剂加注系统进行可靠性评估，对加注系统进行安全性分析。

本文对 C^3I 系统的可靠性分析方法进行研究，对于今后评估 C^3I 系统可靠性水平、改进现有 C^3I 系统设计、设计新的高可靠 C^3I 系统具有一定的参考意义。

2 C^3I 系统基本结构

C^3I 系统以现代计算机及其网络和通信、显示设备为核心，充分体现指挥、通信、控制、情报资料和计算机辅助决策的功能[1]。应用于载人飞船发射指挥的 C^3I 系统组成如图 1 所示。

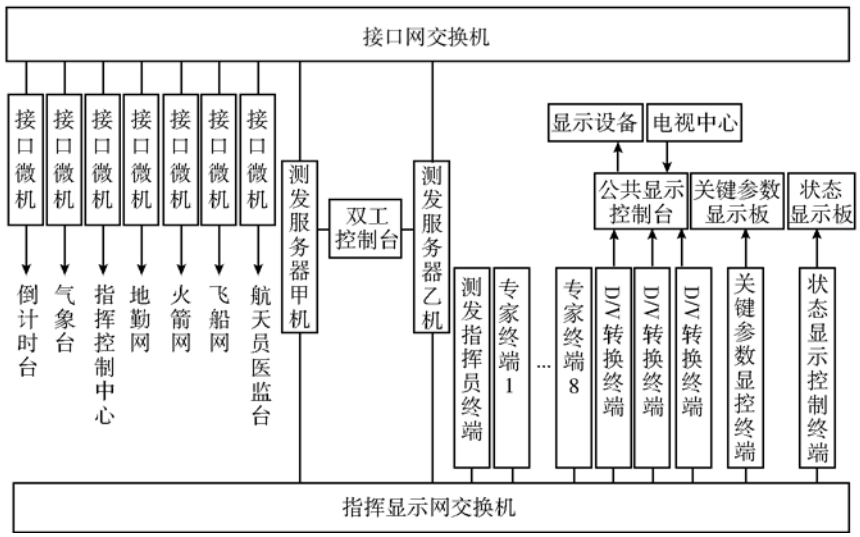

图 1　用于载人飞船发射指挥的 C^3I 系统组成框图

该系统由测发服务器、指挥显示设备、地勤监测、控制设备、接口设备、电视监视、显示设备和通信设备等组成，构成服务器、指挥显示网、接口网和地勤网四个分系统。整个系统由两条交换式以太网即指挥显示网和接口网连接测发服务器、指挥显示设备及接口设备。

测发服务器是整个 C^3I 系统的数据处理中心和信息交换枢纽，各分系统的信息进入测发服务器进行处理，然后根据需要将各类信息送往不同分系统。两台测发服务器通过双工控制台组成热备份。指挥显示网完成系统的指挥、监视和控制功能。接口网实现本系统与指挥控制中心、火箭、飞船、地勤以及航天员医监台等分系统的联接，完成信息交换。地勤分系统担负着对发射场地面勤务设备监控信息的收集，并转发测发服务器向地面设备发出的控制命令等任务。

3 C^3I 系统可靠性分析

C^3I 系统可靠性分析包括以下几个方面的内容：

（1）确定 C^3I 系统可靠性评定指标。

（2）收集 C^3I 系统可靠性数据。

（3）采用故障树分析方法、故障模式及影响分析方法、可靠性模型分析法[3]等方法对 C^3I 系统可靠性进行分析，查找 C^3I 系统薄弱环节，提出改进措施。

（4）利用 C^3I 系统可靠性数据对 C^3I 系统可靠性进行评估，得到其可靠性水平。

3.1 C^3I 系统可靠性评定指标的确定

C^3I 系统硬件设备主要由服务器、微机、网络交换机、投影仪、LED 屏等电子设备组成，其可靠度为 $R(t) = e^{-\lambda t}$，其中 λ 为系统失效率，t 为时间。故采用平均故障间隔时间（Mean Time Between Failure，简称 MTBF）作为 C^3I 系统可靠性评定指标，并采用 MTBF、平均修复时间（Mean Time To Repair，简称 MTTR）、使用寿命、状态参数作为 C^3I 系统各分系统、设备的可靠性评定指标。

C^3I 系统作为测试、发射任务的组织指挥平台，虽然整个任务期间 C^3I 系统的累计工作时间较短（最长连续工作时间为 12 小时），但是系统的可靠性对任务影响较大，需要以较高的 MTBF 保障试验任务的顺利实施。因此将 C^3I 系统的 MTBF 指标确定为不低于 1000 小时（$MTBF = 1 / \lambda$，连续工作 24 小时后系统的可靠度为 97.6%）。

结合系统实际使用情况，依据服务器分系统、指挥显示分系统、接口网分系统、地勤网分系统等的重要性、复杂程度、可维性和元器件质量等确定加权系数，采用可靠性工程加权分配方法进行可靠性分配，可获得各分系统的可靠性指标（MTBF 值）。根据经验统计数据和相关厂家发表的 C³I 系统各设备失效率 λ 值数据，根据公式 MTBF = 1 / λ 计算得到网络交换机、服务器、微机、磁盘阵列、双工控制台、时统设备等的 MTBF 值。详见附录。

C³I 系统指挥显示分系统中的投影仪灯泡和 LED 屏的 LED 单元模块具有一定的使用寿命，要求其使用寿命分别不低于 1200h 和 50000h。光缆、网络机柜、光收发器的使用寿命一般为 10 至 15 年，C3I 系统光缆、网络机柜、光收发器寿命取低限 10 年（从系统交付竣工时开始计算）。双绞线的使用寿命一般为 8 至 10 年，C³I 系统双绞线寿命取低限 8 年（从系统交付竣工时开始计算）。RJ45 接头等动作元件以插拔动作次数作为指标量值衡量其使用寿命，通常其插拔寿命为插拔 60 次，插拔超过 60 次后应予以更换。C³I 系统网络丢包率不应超过 10^{-5}。

根据文献[5]要求，C³I 系统各服务器、微机内存一般应留有 20%的余量。CPU 也应留有一定的余量，这里要求不低于 40%。根据文献[6]要求，C³I 系统应用软件的软件单元的 McCabe 圈复杂度应不大于 10。一旦 C³I 系统出现故障，需要以较快的速度修复故障，使之能够尽快重新投入使用，因此要求 MTTR≤0.5 小时。

C³I 系统各分系统、设备的可靠性评定指标量值

表 1　C³I 系统各分系统、设备的可靠性评定指标量值

分系统名称	设备名称	评定指标类型	评定指标量值
服务器分系统		平均故障间隔时间	3200h
	主交换机、备份交换机	平均故障间隔时间	40000h
		丢包率	≤10^{-5}
	主服务器、备份服务器	平均故障间隔时间	16000h
		内存余量	≥20%
		CPU 余量	≥40%
	双工控制台	平均故障间隔时间	14000h
	时统设备	平均故障间隔时间	16000h
	磁盘阵列	平均故障间隔时间	40000h
	网络机柜	使用寿命	10 年
	光收发器	使用寿命	10 年
	光缆	使用寿命	10 年
	双绞线	使用寿命	8 年
	RJ45 接头	使用寿命	插拔 60 次
	服务器分系统应用软件	软件单元的 McCabe 圈复杂度	≤10
指挥显示分系统		平均故障间隔时间	4300h
	投影仪灯泡、灯箱	使用寿命	1200h
	投影仪	平均故障间隔时间	25000h
	切换矩阵	平均故障间隔时间	40000h
	LED 屏	平均故障间隔时间	25000h
	LED 单元模块	使用寿命	50000h
	投影控制微机、LED 屏控制微机、指挥员微机、专家微机	平均故障间隔时间	30000h
		内存余量	≥20%
		CPU 余量	≥40%
接口网分系统		平均故障间隔时间	4300h
地勤网分系统		平均故障间隔时间	4300h

见表 1。

3.2 C^3I 系统可靠性数据的收集

有效的信息和数据是开展可靠性分析的基础，是可靠性分析评估和决策的依据。通过填写“系统基本情况”、“故障情况及处置措施” 等表格的方式，收集了酒泉发射场、西昌发射场、太原发射场各 C^3I 系统的部分可靠性数据。表 2 为部分典型故障。

3.3 C^3I 系统可靠性分析

故障树分析方法、故障模式及影响分析方法、可靠性模型分析法[3]等是常用的可靠性分析方法，可从不同方面对系统可靠性进行分析，应结合使用。

故障树分析是一种自顶向下的可靠性分析方法，即从系统不希望发生的事件（顶事件），特别是对人员和设备的安全产生重大影响的事件开始，向下逐步追查导致顶事件发生的原因，直至基本事件（底事件）。

图 2 所示为 C^3I 系统公用显示墙无显示故障树，其原因有指显网交换机故障、接口网交换机故障、服务器故障或公共显示设备故障。而导致公共显示设备故障的原因有投影仪和 LED 屏硬件故障或控制

表 2　两个系统典型故障

设备名称		故障模式及原因	故障影响	严酷度	发生概率
指显网分系统	一台投影仪	投影仪主灯报警，无法使用。原因是投影仪主灯使用寿命为 1200 小时，达到使用寿命。	影响正常试验	II	较高
地勤网分系统	地勤网交换机	地勤网交换机启动不正常，使用时数据传输不正常，有丢包现象。原因是该交换机元器件问题。	影响正常试验	II	低

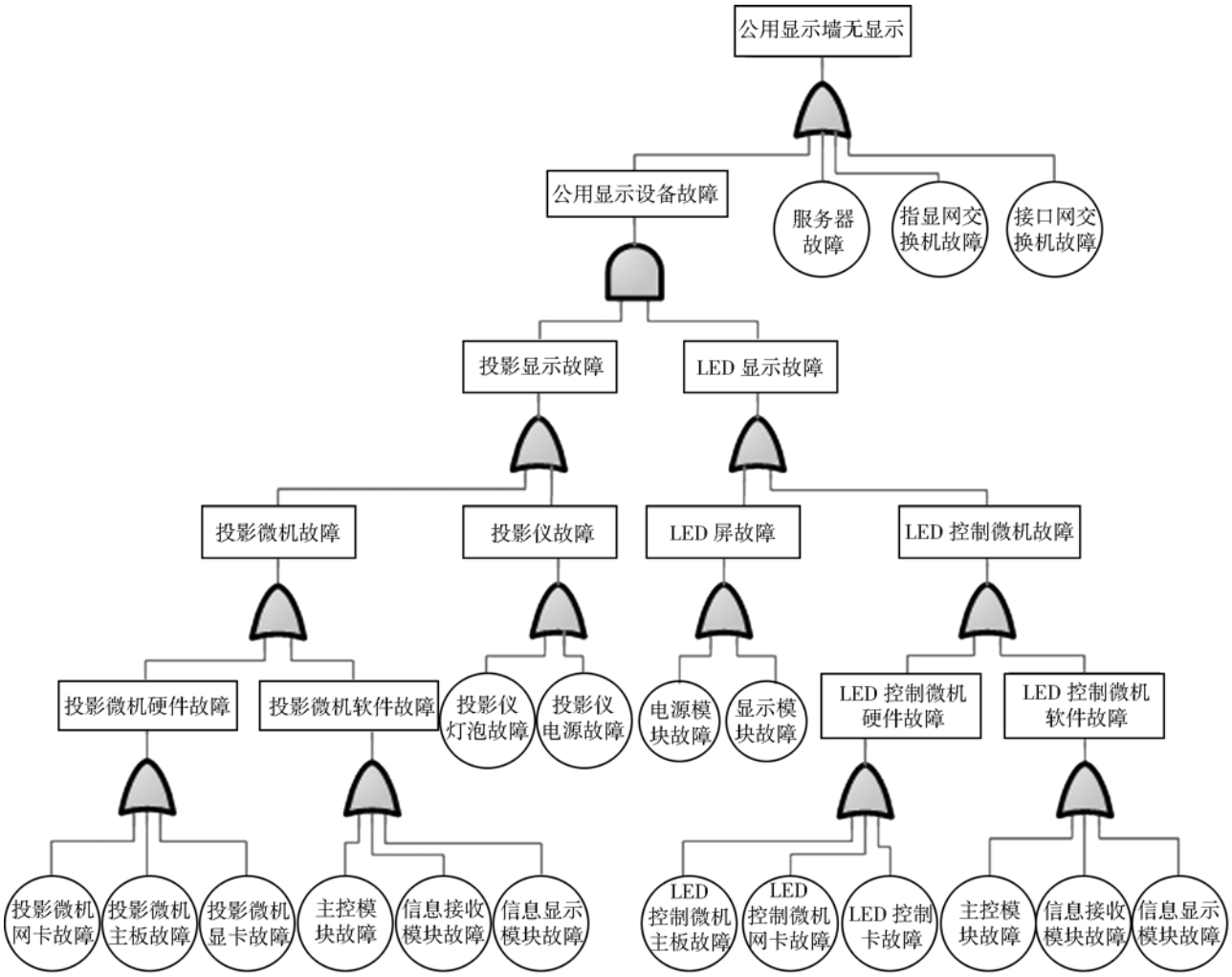

图 2　C^3I 系统公用显示墙无显示故障树

微机的硬件或软件故障。

故障模式及影响分析方法自底向上，按照一定的格式有步骤地分析每一部件(或每一种功能)可能有的故障模式，每一故障模式对系统的影响及失效后果的严重程度。对 C³I 系统进行故障模式及影响分析的部分结果见表 3。

表 3　C³I 系统故障模式及影响分析(FMEA)表(部分)

识别号	产品功能标志	功能	故障模式	故障原因	任务阶段及工作方式	故障影响			故障检测方法	预防与补偿措施	严酷度	发生概率
						局部影响	对上一级影响	最终影响				
JKWJHJ	接口网交换机	接口信息网络通信	无法接收转发外系统信息	交换机硬件损坏	产品测试、加注、发射	无法转发外系统信息	功能丧失，无外系统信息接入	任务失败	目测	更换新交换机	Ⅱ	低
FWQ1	测发服务器甲机	接收、存储、处理、分发各类测试发射信息	无法接收、处理、分发信息	计算机硬件损坏或应用软件失效	产品测试、加注、发射	无法接收、处理、分发信息	系统性能降级，不能与测发服务器乙机构成热备份	系统功能降级	自动检测、目测	主副机切换、软件维护	Ⅳ	较低
SGT	双工控制台	两台测发服务器的双工控制	无法对两台服务器进行双工管理	硬件损坏	产品测试、加注、发射	无法对两台服务器进行双工管理	功能丧失	任务失败	自动检测、目测	更换新部件	Ⅱ	较低

可见，一个系统服务器分系统可靠性框图如图 3 所示。测发服务器甲机与时统卡 1、测发服务器乙机与时统卡 2 分别构成一个串联可修复系统，双工控制台与这两个串联可修复系统共同构成一个串并联可修复系统，可参考文献[7]的方法计算其可靠度。

通过分析所收集的各发射场 C³I 系统的典型故障案例，并结合采用故障树分析方法、失效模式及影响分析方法、可靠性模型分析法对各发射场 C³I 系统进行分析，发现 C³I 系统的薄弱环节在于网络交换机、服务器、双工切换(软件/硬件)设备、投影仪等。

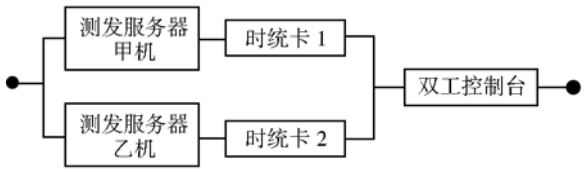

图 3　服务器分系统可靠性框图

网络是 C³I 系统信息传输的基础设施，网络交换机是信息的汇聚、转发中心。网络交换机一旦失效，将导致所有外系统信息无法传送到 C³I 系统，或指挥显示网上无任何信息显示，将导致任务失败。

服务器是信息存储、分发中心，一旦失效，将导致系统瘫痪，任务失败。因此，通常都设置两台互为热备份的服务器，由专门研制的双工切换（软件/硬件)设备来控制两台服务器的主副机工作状态。如果双工切换(软件/硬件)设备失效，两台服务器将失去双工控制，造成主副机工作状态混乱。

投影仪灯泡具有一定的使用寿命。投影仪使用时间比较长后性能下降，投影效果变差。

3.4 C³I 系统可靠性分析举例

一个 C³I 系统建成投入使用后，光缆、网络机柜、光收发器、双绞线、RJ45 接头均处于 3.1 节“C³I 系统各分系统、设备的可靠性评定指标”(简称评定指标)的使用寿命期限内。根据执行任务和平时维护的使用情况统计，该 C³I 系统网络交换机丢包率低于 10^{-5}。

计算 MTBF 量值需要“等待”设备出现两次以上故障。该 C³I 系统所有设备均未出现两次以上的故障。对于一直未出现故障的设备(占大多数)记录其截止目前的累计无故障工作时间；对于出现过一次故障(如投影仪、图形控制器、投影信源工控机)的设备，记录其从故障发生并采取了解决措施后至目前的累计无故障工作时间。所记录的累计无故障工作时间均低于评定指标的 MTBF 值。

评定指标规定 C³I 系统 MTTR≤0.5h。目前该 C³I 系统中仅有投影仪、图形控制器和投影信源工控机发生过影响系统正常运行的故障，其 MTTR 量值均达不到指标要求，其中投影仪的故障排除因依

赖于异地的厂家专业人员，其 MTTR 远超出指标要求。

该 C³I 系统发生故障的设备主要包括投影仪灯箱、图形控制器、投影控制微机、接口微机、地勤服务器等。其故障主要由项目没有按照总体技术方案实施、产品达到使用寿命、软件缺陷等引起的。投影仪灯箱具有一定的使用寿命。

该 C³I 系统中的薄弱环节包括图形控制器、投影控制微机、接口微机、地勤服务器软件等。拟采取以下改进措施：增加 4 台投影控制微机和 1 台备份微机，增加 4 台接口微机和 1 台备份微机，对地勤服务器软件进行改造，该 C³I 系统将满足任务对 C³I 系统的可靠性要求。

需要说明的是，虽然我们开展了各发射场 C³I 系统可靠性数据收集工作，但是可靠性数据的主要来源是原先记录的故障数据。当时作记录并非为了可靠性分析目的，故所获得的可靠性数据可能是不完全、不准确的。并且由于可靠性数据较少，无法准确推算 C³I 系统各设备的故障分布。

4 C³I 系统可靠性下降原因分析与工作建议

4.1 C³I 系统可靠性下降原因分析

经过对各发射场目前正在使用的 C³I 系统进行分析，我们认为，造成 C³I 系统可靠性下降的原因有以下几个方面：

（1）项目实施时没有依据总体技术方案。例如，一个总体技术方案中采用 5 台微机分别控制 5 台投影仪，而在项目实施时只利用一台微机加装多屏显卡集中控制，导致这台投影控制微机负担过重。

（2）项目实施时设备选型不当。例如，一个图像处理器由于选型不当，造成边缘不融合以及输出黑屏。

（3）项目实施时考虑不周，散热处理不好。例如，一个 LED 屏局部过热，出现大片闪烁。

（4）设备正常使用过程中的损耗、性能下降。例如，一个 2 台 64 英寸投影电视工作不稳定；部分微机显示器颜色失真；LED 屏“坏点”逐年增多。

4.2 C³I系统可靠性工作建议

针对对各发射场目前正在使用的 C³I 系统存在的薄弱环节和可靠性下降原因，我们提出以下建议：

（1）加强网络交换机的备份。一个指挥显示网交换机和接口网交换机构成了互为热备份的关系，即测发服务器、指挥员微机、专家微机、D/V 转换微机、关键参数显示微机、接口微机等同时挂接在两台交换机上。

（2）加强服务器备份。一个两台测发服务器成了互为热备份的关系，并由专门研制的双工控制台负责它们之间的切换。目前有的发射场服务器没有备份。

（3）加强项目实施过程的监督、管理项目实施时必须依据总体技术方案，不得擅自变更 C³I 系统结构。

（4）加强项目实施过程的设备选型，尽量选择高质量的网络交换机、服务器、图像处理器、微机、投影仪等产品，提高系统的可靠性。

（5）加强系统使用过程中的维护、保养、管理，定期进行检修、检测，使设备保持在良好的状态，尽早发现存在的故障和隐患，并及时排除，预防可靠性下降。

（6）加强软件可靠性设计研究。目前各发射场大部分 C³I 系统中，两台互为热备份的服务器上安装、运行的是同一套应用软件，主要能适应服务器的硬件故障。一旦服务器应用软件出现故障，则在两台服务器上都会出现故障，两台服务器起不到冗余备份作用。由两支不同的开发队伍为一个两台互为热备份的服务器分别设计了两套功能相同的应用软件，才能充分体现软件高可靠性冗余设计思想。

5 结束语

C³I 系统在发射场中发挥着重要作用。人们对其可靠性提出了很高的要求。本文对 C³I 系统的可靠性分析方法进行研究，提出 C³I 系统的可靠性评定指标，收集 C³I 系统可靠性数据，对 C³I 系统可靠性进行分析，查找 C³I 系统中存在的薄弱环节，分析造成其可靠性下降的原因，并提出可靠性工作建议。在今后的工作中，我们将进一步完善所提出的 C³I 系统可靠性分析方法。

进一步的工作还包括加强可靠性基础数据的收集。可靠性数据收集是发射场 C³I 系统可靠性建设的重要内容，借助有计划、有目的的收集发射场 C³I 系统寿命周期各阶段的数据，经过分析，发现 C³I 系统可靠性薄弱环节，从而改进设计，有利于不断提高 C³I 系统可靠性水平。

今后我们还将加强软件可靠性研究。软件在 C^3I 系统中发挥着不可替代的重要作用。在软件可靠性理论方面，软件可靠性概念提出时间较晚，由于软件自身的特性，其在可靠性模型、指标分配与预计、高可靠性设计、可靠性测试与评估等方面都与硬件存在着显著的差异，有很多理论问题都有待深入研究。 ◇

参 考 文 献

[1] 徐克俊主编. 发射工程学概论. 北京: 国防工业出版社, 2003.
[2] 刘松林, 刘 阳, 刘 晗, 谭云涛. 我国未来发射场可靠性设计思路研究. 导弹与航天运载器技术, 2008(6): 36–40.
[3] 孙雅度, 刘松林, 肖力田, 周 旭, 张永华. 921 航天发射场地面设施设备安全性可靠性复核思路研究. 靶场试验与管理, 2008(2): 6–11, 22.
[4] 徐克俊, 金星, 郑永煌. 航天发射场可靠性安全性评估与分析技术. 北京: 国防工业出版社, 2006.
[5] 国防科学技术工业委员会. 中华人民共和国国家军用标准 GJB/Z 102–1997 软件可靠性和安全性设计准则, 1997.
[6] 中国人民解放军总装备部司令部. 总装备部软件工程规范. 2008.
[7] 卢明银, 徐人平主编. 系统可靠性. 北京: 机械出版社, 2008.

Analysis on the Reliability of Command, Monitor and Control System for Testing and Launching

SHAN Jinhui　CAO Zongsheng　ZHANG Ailiang　NIU Shengfen
(Beijing Special Engineering Design and Research Institute)

Abstract: Command, monitor and control system for testing and launching (abbreviated as C^3I System) plays an important part in the launching site due to the requirements for high reliability. In this paper, the analyzing methods of reliability of C^3I System are studied, the assessment index of the reliability of C^3I System is proposed, and the reliability data of C^3I System are collected. Then the reliability of the C^3I System is analyzed to look for the existing weak link and the cause of decline of reliability. Finally, some suggestions are proposed for the reliability work of C^3I System.

Keywords: Command; Monitor; and Control System for Testing and Launching; C^3I System; Reliability; Analysis.

(上接第 30 页)

The Collision Detection and Automatic Amendment in the TT&C Plan

HUAN Pei　LIU Chengjun
(Beijing Aerospace Control Center)

Abstract: There are various contradictions and collisions in the process of the plan generation. The plan including the contradictions and collisions can not be carried into execution without making improvements and optimization. On the basis of summarizing the collision detection methods in the existing plan software, the concept of automatic amendment is introduced into the plan software, the basic principles of the collision detection and the algorithm of automatic amendment are discussed.

Key Words: TT&C plan; Collision; Collision Detection; Automatic Amendment