# 关键基础设施及其安全管理①

刘 晓[1,4], 张隆飙[2], ZhangW J[3], Tu Y L[4]
(1. 上海交通大学机械与动力学院, 上海 200240; 2 东北大学工商管理学院, 沈阳 110004;
3. 萨斯客彻温省大学机械工程学院, 加拿大; 4. 卡尔加里大学机械与制造工程学院, 加拿大)

摘要: 关键基础设施(CI)系统是复杂的、高度相互依存的、网络化的社会—技术系统, 一旦系统被中断或者被破坏, 将会对国民健康、国土安全、经济稳定以及政府的正常运转等产生重大的影响. 主要研究关键基础设施及其安全管理过程中的若干问题, 对 CI的特点进行了分析和总结, 建立了网络化 CI系统的体系结构, 并利用视图模型来描述系统, 同时还给出了灾难处理的一般过程. 最后, 进一步探讨了如何使用系统工程的方法来分析和模拟网络化 CI系统的运行方式、潜在的薄弱环节以及改进这些薄弱环节的实施方法.

关键词: 关键基础设施; 社会–技术系统; 建模; 体系结构
中图分类号: N949 文献标识码: A 文章编号: 1007–9807(2009)06–0107–09

## 0 引 言

近年来, 灾难事件在世界范围内频频发生, 如中国的 SARS, 欧洲的疯牛病、美国的 911袭击、印度洋海啸、美国和加拿大大停电、英国的地铁爆炸事件, 法国的机场坍塌事件, 加拿大的安大略洪水灾难等等. 同样, 我国对灾难的预防及应急处理技术也存在很大的需求, 很多地方都可以看到由灾难事故及其引发的链锁式反应造成的严重后果. 比如, 广东江门某油库在施工过程中, 电焊产生的火花使一座存有少量废油的油罐发生爆炸, 导致周边数万人被疏散. 另一个案例更加触目惊心, 1989年 8月 12日中国石油天然气总公司管道局胜利油田输油公司黄岛油库的特大火灾, 造成 19人死亡, 100多人受伤, 烧掉原油 4万多立方米, 大约 600吨石油在胶州湾海面形成几条 10多海里长、几百米宽的污染带, 另外还烧毁消防车 10辆, 直接经济损失达 3 540万元. 这一系列的灾难严重影响到人们的正常生活, 它不仅对人的生命造成威胁, 而且在心理上也会产生巨大的负面影响. 因此该领域的研究工作受到国内外政府及学者越来越多的重视.

灾难事件的诱因主要可以分为以下几类: (1)自然灾害, 例如飓风、地震、大范围发生的传染病等; (2)人为事故, 主要是由人的误操作引起的事故; (3)技术问题, 主要是由设备可靠性问题引发的事故; (4)恐怖袭击, 主要是人为的故意破坏. 尽管各国政府也都对上述各类事件都做出了积极的反应, 但由于灾难事件管理是巨大的社会—技术复杂系统, 尚缺乏行之有效的管理理论或者实践经验[1,2]. 这就要求人们对那些一旦收到破坏就会对直接威胁到国民健康、社会安定、经济稳定, 甚至导致整个社会体系崩溃的特殊基础设施, 即关键基础设施事先考虑其发生灾难的风险, 并作好应对措施.

所谓关键基础设施(critical infrastructures, CI)是指能够为国土防御、经济安全以及国民健康、福利事业持续提供产品或服务的行业、公共机构和传播媒介[1]. 它主要包括: 公共事业、电信设

① 收稿日期: 2006–11–13; 修订日期: 2008–03–17.
基金项目: 国家自然科学基金资助项目(70571077).
作者简介: 刘 晓(1967—), 女, 吉林人, 博士, 副教授. Email: xliu@mail.neu.edu.cn

施、能源、金融、物流 5个重要部门. 其中, 公共事业部门又包括水、食品、执法机构和公共卫生设施等众多的子部门, 所有这些部门构成了为国民生存提供必备的物资和服务的复杂网络; 电信设施和能源部门 (如电力、石油、天然气 )的可靠安全运行是其它关键基础设施正常运转的基本保证, 在 CI系统中起着非常重要的作用; 金融、物流 (机场、港口、地铁、高速公路、铁路、邮政服务和航运 )是人们日常生活的重要组成部分, 同时也是其它基础设施高度依赖的两个关键部门.

## 1　CI系统的特点

### 1.1　依赖性和内部依赖性

综合 Health Canada[1], Kuban[3], Rinaldi[4]以及 Thissen和 Herder[5]等的论述, 复杂的 CI系统具有相互依赖和内部依赖的关系, 如图 1所示. 这些依赖关系可以分为物质流依赖关系和非物质流依赖关系[6], 二者的区别在于是否存在物质的流动. 物质又包括: 1)材料; 2)能源; 3)信息; 4)人. CI系统的物质流关系是显而易见的, 并且在作应急预案的时候也得到了考虑, 然而对于非物质流关系来说, 却很少得到关注. 例如对于在同一地区提供医疗服务的两家医院来说, 尽管两个 CI之间没有任何物质的流动, 但它们却是相关的, 因为它们都要对伤员进行处理. 如果一家医院收到了破坏, 那么另一家医院就必须接待更多的患者. 鉴于 CI系统复杂的相互依赖及内部依赖关系, 本文将称之为“网络化 CI系统”.

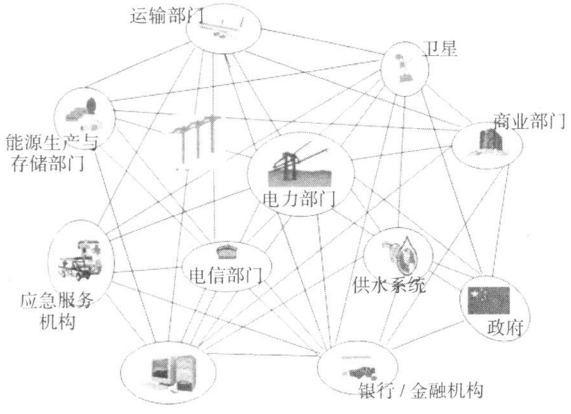


图 1　网络化 CI系统示例[7]

Fig. 1 An example of the networked CI system

### 1.2　开放性和拓扑结构可变性

由于系统边界的开放性和拓扑结构的可变性, 网络化 CI系统变得非常复杂. 当灾难发生时, 现有的 CI系统可能会因为资源耗尽而变成孤立系统, 与此同时还可能涉及到管理团队的变动 (如成员的增减 ). 例如在经历灾难之后, 运输系统可能由于种种原因而遭到破坏, 此时它便会脱离原来的 CI系统, 同时也要求对该运输系统的管理团队进行裁减. 网络化 CI系统对于这种增加或裁减也是开放的. 由于 CI系统的这种开放性特点, 如果增加新的 CI, 那么新增的 CI将与现有的 CI建立新的联系; 相反, 如果某些现有 CI被裁减, 那么这些 CI将与现有的 CI脱离原有的联系, 导致原来 CI系统的连通性发生变化. 这就表明灾难中的网络化 CI系统具有可变的拓扑结构.

### 1.3　自治性

每个 CI本身就是一个高度自治的系统 (比如核电站 ), 它具有自己的灾难管理系统. 当某一 CI发生灾难时, 其灾难管理系统就会首先被触发. 在这一问题上, Ibarra等[8]讨论了运输系统的灾难管理, Houck等[9]讨论了电信系统的灾难管理. 如果灾难和灾难管理的影响范围超出了特定的 CI系统, 那么该 CI系统的灾难管理水平将会得到增强, 进而影响其他的 CI系统.

### 1.4　地理位置动态性

CI系统的地理位置在灾难状态下可能发生变化 (例如移动发电站可以从一个地方转移到另一个地方 ), 然而这种变化可能会影响到它的功能. 因为对于一个特定的 CI系统来说, 其运行条件会随位置的改变而改变. 或者说, 每个 CI都运行于特定的外部条件下. 一些 CI系统 (例如动力系统、电信系统 )可能包含分布式的子单元, 而这些子单元位于不同的地理位置. 如果这些子单元的地理位置发生了改变, 那么 CI系统的地理位置也将随之相应地改变.

### 1.5　系统中人的因素

网络化 CI系统不仅包括技术系统, 而且还包括社会系统. 例如发电厂必须由人来进行操纵和监督. 任何灾难的影响都将最终作用于人, 同时灾难中的受害者又会作为反馈的一部分作用于灾难

管理系统, 如图 2所示. 从图中可以看到, 受害者的状态作为灾难管理系统输出的一部分, 而这些输出会被进一步反馈到灾难管理系统来调整它的管理决策或者制定新的决策. 但需要注意的是, 由于环境和人的双重不确定性, 受害者的状态也在随时间而改变. 因此可以看出, 灾难管理是具有不确定输出的复杂的控制问题.

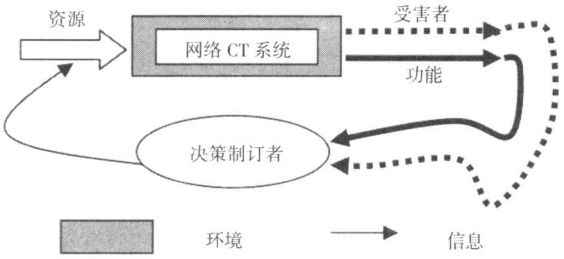


图 2　灾难管理的双重目的

Fig. 2 The dual goal in disaster management

总之, 网络化 CI系统具有如下特点: 1) 开放性 (C1); 2)拓扑结构可变性 (C2); 3)社会—技术以及人—机之间的交互性 (C3); 4)动态演变性 (C4); 5)地理位置动态性 (C5); 6)自治性 (C6). 这些特点描述了网络化 CI系统的静态特性. 然而当 CI系统运行时, 其动态特性又包括极其复杂的过程, 这些过程具有以下特征: (i)并发性, (ii)异步性, (iii)分布式, (iv)并行性, (v)随机性[6].

综上所述, CI系统是个复杂的、网络化的、"社会—技术"以及"人—机"交互系统. 而人–机交互的本质意味着每一个 CI系统都与人自身休戚相关. 许多众所周知的灾难性事件就是由于人为因素造成的, 比如三里岛事件. 这些事件对管理能力提出了新的挑战, 即如何对网络化 CI系统在正常工作条件下或是在有意外事件发生的情况下进行有效地控制与管理. 目前, 在国内外的研究中主要存在两个与网络化 CI系统相联系的基本问题: 灾难预警和灾难处理. 其中, 灾难预警的关键问题是如何确定网络化 CI系统中的薄弱环节; 灾难处理的关键问题是如何使损失最小化并使系统功能得到迅速恢复. 本文侧重于灾难处理 (或称应急处理)的研究.

## 2　FEBPSS框架

系统是由一系列相互关联的元素或实体构成的. 本文将其描述为"功能 – 效果 – 行为 – 规则 – 结构 – 状态" (function-effect-behavior-principle-structure-state, FEBPSS)框架[10]. FEBPSS框架的核心概念包括: 1)结构、状态和状态变量; 2)行为; 3)规则; 4)功能和效果; 5)系统分解.

上述概念之间的关系如图 3所示. 从图中可以看出结构位于整个体系的最低层, 继而依次是状态、行为和功能. 规则处于状态和行为之间, 用于支配或者解释行为. 效果位于行为和功能之间, 它给出了从行为到功能的基本准则. 此外, FEBPSS框架沿两个维度安排这些概念: 1)聚合维 (结构→状态→行为→功能); 2)控制维 (规则和效果).

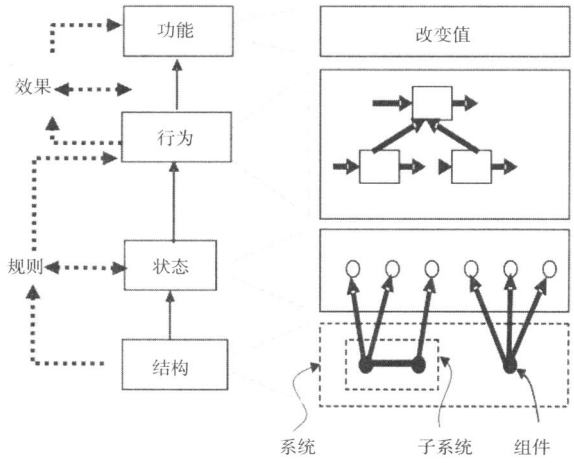


图 3　FEBPSS框架

Fig. 3 The FEBPSS framework

另外, 图 3的右下部分体现了系统分解的思想. 对于一个系统来说, 不仅其本身可以被分解成多个子系统和组件, 而且其结构、行为、规则、效果和功能也都是可以再分解的. 这说明研究组件、子系统、系统的行为 (功能、规则、效果)是必要的. 同时可以清楚地看出, 系统分解和 FEBPSS是正交的.

## 3　网络化 CI系统的建模方法

### 3.1　网络化 CI系统及其灾难管理的控制系统视图

前面的讨论表明灾难管理实质上是决策问题或者控制问题. 因此, 可以从控制系统的角度来研

究网络化 CI系统的灾难管理过程, 从而可以得到具有控制系统的网络化 CI系统的概念模型 (参见图 4).

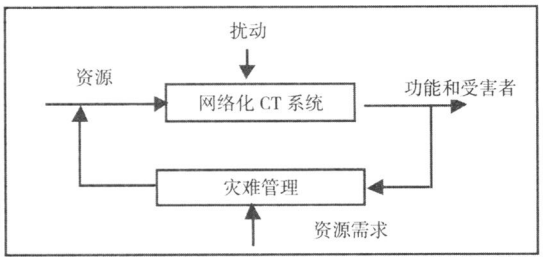


图 4 灾难管理的控制系统视图

Fig. 4 Control system view of disaster management

控制系统通常有目标导向和任务导向两种类型的工作. 在目标导向型的控制工作中, 通常会有一个明确定义的目标. 而对于任务导向型的工作来说, 工作不能通过预定义的方式进行描述, 比如在人员的搜救工作中, 救援队对是否有人员的伤亡, 具体的伤亡数目, 或者是他们处于什么状态并不知道. 为了量化问题, 不得不将面向任务的工作分解成一系列在某一时间段内面向目标的工作. 网络化 CI系统中的灾难管理便是任务导向型的工作, 它的首要任务就是在限定的时间内恢复处于灾难状态下的 CI系统. 这一任务可以被分解成多个子任务, 例如在 10小时内用地面运输系统将伤员从 A 地运送到 B地, 把他们送到最近的医院等等. 与此同时, 控制、管理和协调将会起到应有的作用.

### 3.2 建模策略的选择

按照控制论的观点, 为了有效的控制和管理一个工厂, 需要建立使工厂与其输入、输出关联的模型. 建立此模型有两种策略, 第 1种是从工厂的结构开始建模, 第 2种是从工厂的行为开始建模. 对于网络化的 CI系统来说, 第 2种策略并不合适, 因为要了解网络化 CI系统的行为并非易事 (要了解其行为要求灾难发生在一个特定的网络 CI系统中, 而这是不现实的 ). 因此本文采用第 1种建模策略, 即利用 FEBPSS框架来建立模型 (见图 5). 在图 5中, 对每一个 CI系统, 甚至网络化 CI系统整体都利用 FEBPSS框架进行建模. 这种方法符合第 2部分提到的 FEBPSS 体系结构与系统分解相互正交的建模原则.

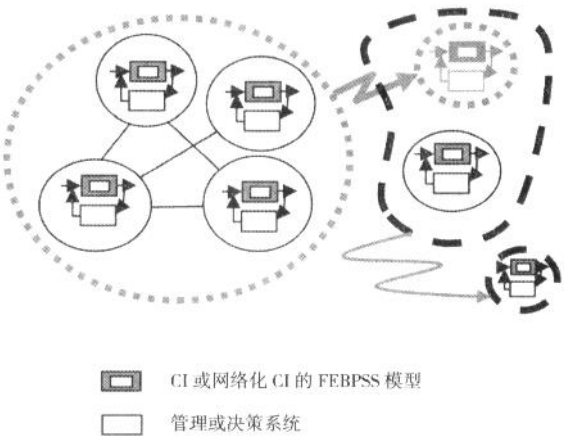


图 5 FEBPSS框架在网络 CI系统中的应用

Fig. 5 Application of the FEBPSS framework to the networked CI system

### 3.3 网络化 CI系统的体系结构

系统的体系结构包括系统的组成元素和它们之间的功能性关系. 在本文中, 提出了网络化 CI系统体系结构的通用模型 GANetCI( generic architecture of the networked CI system). 为了使 GANetCI具有前述网络化 CI系统的所有特征, 需要首先做一些假定, 以使该体系结构能够利用 FEBPSS框架来进行建模.

将网络化 CI系统中的每个 CI都看作是拥有 FEBPSS框架的智能体. 为具有 CI系统的开放性特点 ( C1), 假定智能体的数量是可变的. 为了具有拓扑结构可变的特点 ( C2), 假定 CI之间联系的数量是开放的. 为具有自治性特点 ( C6), 假定每个 CI系统都具有灾难管理系统 (见图 5); 同时假定同一层次的所有 CI系统构成的聚合体也具有灾难管理系统 (见图 5). 为了具有动态演变性和地理位置动态性的特点 ( C4, C5), 认为网络化 CI系统的所有状态都是时间和位置的函数.

在研究包含多种上述关系的复杂性动态系统时, 视图模型被认为是最有效的方法 [10]. 每种视图都从一个特定的角度对系统进行描述, 并且都可以视为系统的简化版本. 视图模型所隐含的哲学思想是: 系统的复杂性可利用“分而治之”的方法来处理. 实际上, 可以将视图看成是对系统的抽象, 例如 X 的视图是忽略除 X 之外的所有其它东西之后得到的[11].

利用视图模型方法, 可以为网络化 CI系统定义下列视图: 1)功能视图, 2)过程 (或行为 )视图, 3)结构视图, 4)人类组织视图, 5)资源视图, 6)灾

难视图. 前 3种视图直接与 FEBPSS框架相联系, 第 4种视图与具有特性 C3的社会系统相关联, 最后两种视图与灾难和灾难管理相关联. 下一部分将对这些视图模型进行详细的讨论.

## 4　网络化 CI系统的视图

众所周知, 视图和视图模型是不同的. 视图描述的是系统的语义, 而视图模型是对使用形式语言的视图的描述. 下面将对网络化 CI系统的视图逐一进行研究.

### 4 1　功能视图

功能视图着眼于在网络化 CI系统中探索 CI系统的功能以及它们之间的关系. CI系统功能之间的关系并不包括物质的流动. 关系的种类可以利用数据抽象的方法来分类, 而数据抽象又包括普遍化 /特殊化 ( generalization / specialization, G/S)和聚合 /分解 ( aggregation / decomposition, A/D)两种形式. 如图 6, 灾难管理系统中共有 3家医院, 其作用是为灾难中的受伤人员提供医疗服务. 图 6a是伤员医疗服务的局部模型, 图中同时显示了利用 A /D数据抽取方法处理这类问题的具体做法. 在本例中, 还需要利用运输系统把伤员从一个地方送到另外一个地方. 图 6b为包含运输系统的功能视图, 图中同时显示了利用 A /D数据抽取方法处理这类问题的具体做法. 另外, 需要指出的是, 在网络化 CI系统中, 可能有些系统并不是关键的, 但是为了保持网络化 CI系统功能的完整性, 这些辅助系统的存在是必要的, 例如污水排放系统, 临时居住点等. 由于它们并不是关键因素, 因此假定辅助系统的容量是无限的. 同样需要注意的是, 容量限制也是功能视图的一部分.

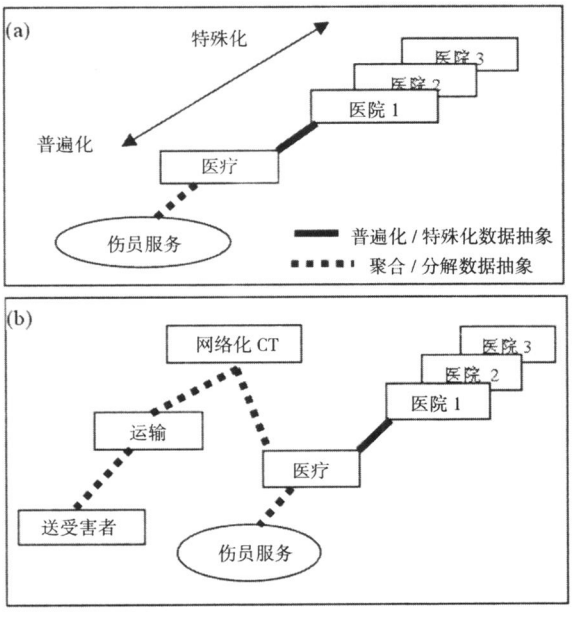


图 6　功能视图

Fig. 6 Function view

### 4 2　过程视图

网络化 CI系统的过程视图对应 FEBPSS框架中的行为的概念. 系统 (或者子系统、部件 )的行为主要是指与系统相关的一系列主动变量和被动变量之间的关系 (见图 7a). 根据 FEBPSS框架的正交性, 本文给出了过程视图 (见图 7). 在此图中, X1, X2(图 7a)两个系统被聚合成一个更高层次的系统 X1X2(图 7b). 系统 X1X2具有自己的包括一个输入和两个输出的行为, 并且通过输入输出进一步和其他系统相联系 (见图 7b). 此外根据在 1. 1节的讨论, 过程中的物质的种类有 4种: 1)材料, 2)能源, 3)信息, 4)人. 复杂的过程可以包括所有这 4种物质. 很明显, 可以在物质分类的基础上对过程视图进行进一步地分解. 例如, 可以将其进一步分解为材料过程视图和信息过程视图. 这两种视图 (确切地说子视图 )是相互联系的.

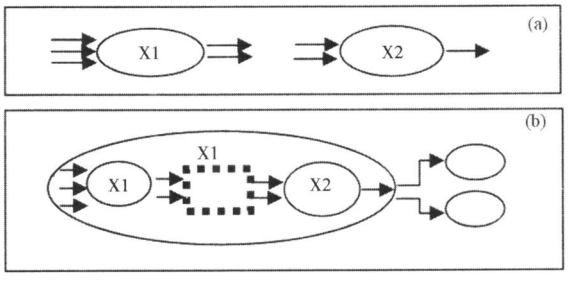


图 7　过程视图

Fig. 7 Process view

### 4 3　结构视图

结构视图通常用于描述 CI系统以及它们之间的联系, 例如医院不仅是一个 CI系统, 同时它又与运输 CI系统和化工厂都有联系 (详见第 5部分的讨论 ). 在结构视图中, 将空间的和时间的信息也包含进来, 以满足第 1部分提到的动态演变性和地理位置动态性的特点 ( C4, C5). 一般来说, 结构视图和功能视图在所包含关系的交叉部分可能会产生混淆. 例如在网络化 CI系统中, 具有层次结构的图 6b对医疗和运输系统的相关性进行了描述, 具有网络化结构的图 8描述了他们之间

的相关性. 但实际上这种混淆是易于解决的, 因为图 6b所描述的关系是当两个 CI都对社会—技术系统的整体功能产生作用时的情况; 而图 8实际上描述了任意两个 CI之间的物质流关系. 这种观点是在产品建模工作中被首先提出的[12].

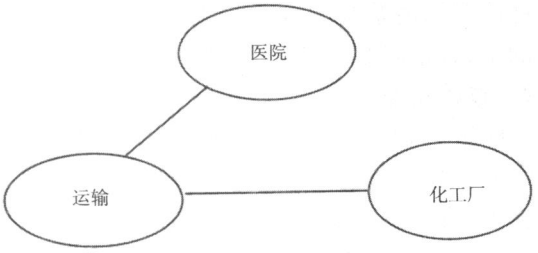


图 8 结构视图

Fig. 8 Structure view

### 4.4 灾难视图

灾难视图是关于以下这些方面的信息: 1)灾难发生的时间 (when) 和地点 (where), 2)灾难的类型, 3)灾难的规模, 4)灾难引起的网络化 CI系统功能的受破坏程度, 5)灾难中生命系统 (包括人、动物、植物) 之间的因果关系. 在具有灾难管理的情况下, 可以在灾难发生前观察到异常的征兆, 这些征兆可能由自然、意外、人为破坏 3个因素中的 1个或者多个所引起[2].

### 4.5 资源视图

系统的过程是指系统的输入与输出之间的关系, 资源就像可以随时取用需求物资的“仓库”, 用以保证“过程”处于稳定的状态. 当有充足的资源投入到过程中时, 过程就会“加速”. 当资源不足时, 物质的流动就会“减速”直至最终“停止”. 值得一提的是, 资源在过程的输出端还起到了“储存”剩余物质的作用. 在灾难管理的情况下, 资源的种类和物质的种类相同, 即材料、能源、信息和人. 其中, 物质材料还包括用于加工物质的工具和设施.

### 4.6 人类组织视图

人类组织视图是从人的角度来看待网络化 CI系统. 本文认为对于技术系统中的每个部件和子系统, 都会有相应的人类组织视图. 这一观点在图 2中已经有所体现, 图中每个 CI都与特定的社会环境相联系, 而社会环境既为技术 CI系统提供约束又为其提供条件. 基于这种考虑, 每个 CI都在双重约束下工作: 1)对其他 CI系统的依赖; 2)对人类组织系统的依赖.

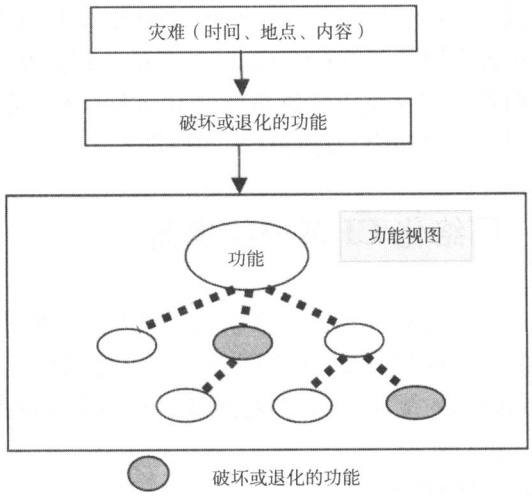


图 9 灾难和功能视图的联系

Fig. 9 The connection between the disaster and function views

上述这些视图之间是相互联系的. 功能、过程和结构视图同属于 FEBPSS体系结构的一部分, 因而是相关的. 资源视图与物质有关, 而物质从过程中流入或流出. 人类组织视图与每个技术 CI系统相联系, 因为每个技术 CI都有其存在的社会环境[9]. 灾难和功能视图之间的联系可以通过图 9进行描述, 从图中可以看出每一个灾难都可能会影响到网络化 CI系统的多种功能. 因此, 我们可以从功能整体的角度对灾难进行预警. 灾难视图通过结构视图进一步和人类组织视图相联系.

## 5 GANetCI有效性演示

目前研究中的关于灾难事故处理的措施与步骤总结如下:

1) 预防 以减小或消除自然灾害和人为灾害带来的影响为目的的一系列措施;

2) 准备 完善应对措施、程序和计划, 从而更加有效地应对紧急事件;

3) 反应 在紧急情况发生时或事后的应对措施;

4) 恢复 事件发生后的重建.

在图 10中, 横坐标代表灾难发生的时间, 纵轴代表各个与灾难相关的决策制定者 (或者说管理者). 同时图 10还进一步说明了图 2中的灾难控制过程 (见图 10的虚线部分).

可以通过对基于 GANetCI的灾难管理通用过程的设计来演示灾难发生后决策制定者应该如何使用 GANetCI来对灾难进行处理. 现在, 以包

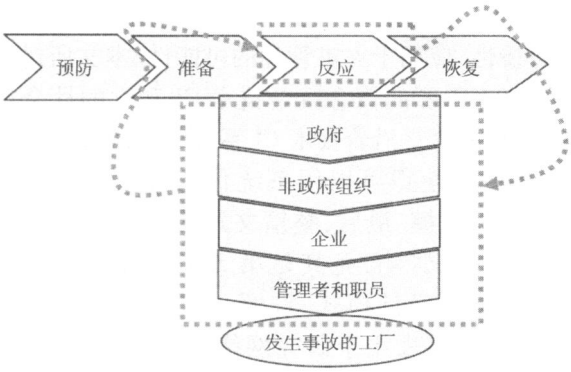


图 **10**　灾难处理流程

Fig 10 Process of disaster management

含医院、运输系统、化工厂 3个 CI的网络化系统为例进行讨论. 假定某化工厂发生了爆炸, 并导致毒气泄露. 同时假定毒气不是被监控装置而是被工厂的工人所发现, 假定毒气在 10小时内就会扩散到附近的居民区.

每个 CI系统都有自己的 FEBPSS模型 (如图 11所示). 灾难管理有两个目的: 1)恢复遭到破坏的功能, 2)营救受害者. 这些目的可以通过与 GANetCI紧密联系的通用过程来实现, 具体过程如下:

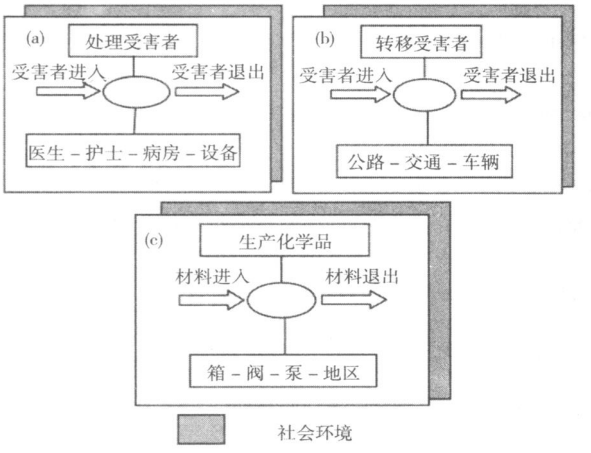


图 **11**　包括 (**a**)医院, (**b**)运输系统, (**c**)化工厂三个 **CI** 系统的简化 **FEBPSS**模型

Fig 11 The simplified FEBPSS model for the three CI systems ((a) hospital, (b) transportation, (c) chemical plant)

第 1步　从灾难视图的角度来描述灾难. 灾难也有其自己的生命周期, 从开始、发展直至结束. 进一步讲, 生命周期还是时间和空间的函数. 对于演示系统, 做如下的假定:

发生爆炸

时间: 上午 10点;

地点: 工厂东部区域 $X_1$, $Y_1$, $Z_1$;

声音: 60分贝;

工人闻到毒气 $H_2S$

爆炸扩散

时间: 上午 11点;

地点: 工厂东部区域 $X_2$, $Y_2$, $Z_2$

第 2步　如果能立即获取灾难的准确数据, 则确定遭到破坏的功能和受害者数量;

第 3步　如果在特定的时间内不能确定灾难的影响情况, 就需要用结构视图来估计遭到破坏的功能和受害者数量. 当得知灾难发生的具体位置之后, 利用结构视图和功能视图之间的联系可以确定遭到破坏的功能. 此外, 可以从人类组织视图和结构视图之间的联系确定受害者的数量;

第 4步　找出功能在正常情况下与遭到破坏的情况下的差异.

第 5步　以功能视图和过程视图之间的联系为基础来确定遭到破坏的过程;

第 6步　找出正常过程和遭到破坏的过程之间的差异, 这将有助于确定需要的资源.

第 7步　比较为恢复遭到破坏的功能所需的资源和基于资源视图的现有资源, 确定尚未满足的资源;

第 8步　对未满足资源的配送过程进行计划和调度.

与上述步骤同样重要的是, 需要营救受害者, 尤其需要完成以下两步:

第 4'步　确定将伤员送往哪些医院 (通过结构视图), 确定受影响区域的居民被安排到哪些地方;

第 5'步　对受害者的运送进行计划和调度. 在这一点上, 10小时的时间限制假定就变得非常重要.

在如上的理论支持下, 本文开发了基于 GIS的 CI决策支持系统, 如图 12所示.

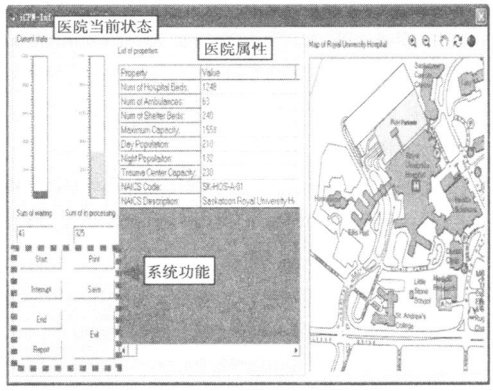


图 **12**　**CI**决策支持系统

Fig 12 CI Decision-making System

## 6 结束语

本文主要讨论了网络化 CI系统的基本概念, 并提出了处于灾难中的网络化 CI系统的结构框图. 所讨论的最重要的概念之一就是网络 CI化系统的控制系统视图, 该视图引出了两个相互分离的概念: 1)网络化 CI系统; 2)灾难管理机制. 这种分离为解决网络化 CI系统的复杂性提供了一个框架. 通过对系统控制和灾难管理的类比进一步提高了将控制系统的丰富理论, 尤其是稳定性和鲁棒性, 应用于灾难管理的可能性. 本文所讨论的另一个重要的概念就是技术 CI和它的社会环境. 这对概念是沿着技术 CI系统分解的阶梯提出的. 此概念使得可以用系统化的方式来对人的因素进行建模. 最后, 整篇文章还受到一般工程设计理论的影响, 尤其是第 5部分提出的通用过程采用了设计模式. 按照一般工程设计的概念, 可以在将来用于研究网络化 CI系统重构的问题.

参 考 文 献:


[1] Food Safety Assessment the Food Emergency Response System of the Canadian Food Inspection Agency[R]. Health Canada, March 1999. http://www.hc-sc.gc.ca/fr-an/alt_formats/hpfb-dgpsa/pdf/securit/fers-siua_e.pdf

[2] Houck D J, Kim E A. Network survivability model for critical national infrastructures[J]. Bell Labs Technical Journal, 2004, 8(4): 153—172.

[3] Kuban R, Mackenzie-Carey H, Gagnon A P. Disaster Response Systems in Canada[Z]. Institute for Catastrophic Loss Reduction, http://www.iclr.org/pdf/research%20paper%2016%20-%20paper%204%20ronf%20kuban.pdf

[4] Rinaldi, Steven M. Modeling and Simulating Critical Infrastructures and Their Interdependencies[C]. Proceedings of the 37th Hawaii International Conference on System Sciences, 2004.

[5] Thissen, Wil A, *et al*. Critical Infrastructures: Challenges for Systems Engineering[C]. The 5th International Conference on Technology, Policy and Innovation, Hague (June), 2001.

[6] Zhang W J. On Modeling and Simulation of Critical Infrastructure Systems[Z]. Presentation at The first annual JIRP symposium, 2005. November 8—10, Ottawa.

[7] Rahman S. Information and Communication Technologies: Powerful Enabler or Weakest Link[Z]. EAPC/PfP Workshop on Critical Infrastructure Protection & Civil Emergency Planning, Switzerland, 2005, http://pforum.isn.ethz.ch/docs/BAA24CA4-65B0-58E9-21A5193021A5E588.pdf

[8] Ibarra G, Stracener J, Szygenda S. Transportation in the Critical Infrastructure: A Holistic Approach Using Systems Engineering Methodologies for Assessing Risk and Cost Impacts due to Highway Disconnects in the Movements of Goods from the Port of Houston[C]. Proceedings CSER 2005, 23—25.

[9] President Critical Foundations: Protecting America's Infrastructures[R]. The President's Commission on Critical Infrastructure Protection (1997), Washington D. C. 1997.

[10] Lin Y, Zhang W J. "Towards a novel interface design framework: Function-behavior-state paradigm," [J]. International Journal of Human Computer Studies, 2004, 61(3): 259—297.

[11] Zhang W J. An Integrated Environment for CAD/CAM of Mechanical Systems[R]. Delft University of Technology, The Netherlands, 1994, 1—263.

[12] Shrikhande, Sachin V. On Effective Information Modeling for Computer-Aided Configuration Management of Complex Products in Manufacturing Environments[D]. Department of Mechanical Engineering, University of Saskatchewan, Canada, 2000.

[13] Longstaff T A, Haimes Y Y. A Holistic Roadmap for Survivable Infrastructure Systems[C]. IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans, 2002, 32(2): 260—268.

[14] Advanced Manufacturing Technology-Systems Architecture-Constructs for Enterprise Modeling[R]. CEN TC 310/WG 1 ENV, 1995, ENV 12 204.

[15] Renaud R, Phillips S. Developping an integrated emergency response programme for facilities: The experience of public

works and government services Canada[J]. Journal of Facilities Management, 2003, 1(4): 347—364.
[16] Radhakrishnan R P, Liu X, *et al* AH and MFM for Interface Design for Complex Work Domain[C]. IEEE Transaction on SMC Part A, 2005 (sulmitted in 2005).
[17]成思危. 复杂科学与系统工程[J]. 管理科学学报, 1999, 2(2): 1—7.
Cheng siwei. Complexity science and systems engineering[J]. Journal of Management Sciences in China, 1999, 2(2): 1—7. (in Chinese)

# Critical infrastructure and its safety management

*LIU Xiao*[1,4], *ZHANG Long-biao*[2], *ZHANG W J*[3], *TU Y L*[4]
1. School of Mechanical Engineering, Shanghai Jiaotong University, Shanghai 200240, China;
2. School of Business Administration, Northeastern University, Shenyang 110004, China;
3. Department of Mechanical Engineering, University of Saskatchewan, Canada;
4. Department of Mechanical and Manufacturing Engineering, University of Calgary, Canada

**Abstract** Critical infrastructure (CI) safety system is a complex and highly inter-dependent and networked social-technical system which, if disrupted or destroyed, would have a serious impact on the health, safety, security, or economic well-being of people and / or the effective functioning of governments. This paper is devoted to the study of the architecture of the CI safety system and problems in its management. We present the architecture of the networked CI system along with its disaster management system, in which the system is described with the notion of view, and the generic process of the disaster management. Also, it discusses how to apply the systems engineering approach to analyze and simulate the networked CI system, and how to find the underlying weak parts and efficient ways to improve them. Finally, we show the usefulness of the architecture by outlining a general procedure for disaster management which is systematic and rational.
**Key words** critical infrastructure; socio-technical systems; modeling; architecture