

石化行业网络系统的安全分析与对策

刘 强

(广东财经大学, 广州 510320)

摘 要 随着两化融合的逐步发展,石化行业工业控制系统的信息化管理水平不断提高,石化生产及管理效率也显著提升。然而其网络系统的信息安全技术水平较低,服务器系统应对物理损伤、自然灾害、网络攻击的容灾容错能力薄弱。为此,提出一种针对服务器实时安全备份及应急接管的技术方案,以期有效地解决石化行业网络系统信息安全的问题。

关键词 石化行业,信息安全,工业控制系统,服务器,网络系统

Security analysis and countermeasure of network system in petrochemical enterprises

Liu Qiang

(Guangdong University of Finance & Economics, Guangzhou 510320)

Abstract With the gradual development of the integration of informatization and industrialization, the level of information management of industrial control systems in the petrochemical industry continues to improve. Petrochemical production and management efficiency have also been improved significantly. However, its network system has a low level of information security technology. The server system was weak in fault tolerance for physical damage, natural disasters, and network attacks. Therefore, a technical solution for real-time secure backup and emergency takeover of servers was proposed, which can effectively solve the problem of information security in the petrochemical industry network system.

Key words petrochemical industry, information security, industrial control system, server, network system

石化行业是国家重要的支柱产业,广泛涵盖到石油、石化、化工等方面,具有高温、高压,易燃、易爆和易腐蚀性的特点^[1]。石化行业的特殊性,决定了其生产安全的重要性,一旦生产系统出现崩溃或者局部故障,可能引起生命安全和环境污染等严重后果^[2]。随着物联网、云计算、人工智能等新技术的飞速发展,石化行业的两化融合正向纵深发展^[3]。未来以技术促安全,不断提高工业控制系统的自动化水平和信息化管理水平是石化行业的发展趋势。

纵观当前工业控制系统,一般可分为 3 个层次^[4-5]: (1) 过程级,指现场控制网络,包括现场的执行器、传感器、仪表等设备; (2) 操作级,指过程控制网络,包括服务器系统硬件设备、数据库等应用软件及防火墙等安全软件; (3) 管理级,指企业信息网络,包括企业工作站、应用工作站等信息管理层面的业务。

信息安全是工业控制系统的重要保障,诸多安全技术比如:安全认证、数据加密和防火墙等技术已

经得到广泛应用^[6-8]。然而服务器作为网络系统的核心设备,其应对物理损伤、自然灾害、网络攻击的容灾容错能力仍然相当薄弱。当前由网络攻击引起服务器瘫痪或者故障的信息安全问题最为常见^[9-10],其次是自然灾害引起的物理损坏,或者管理员误操作引起的软硬件错误。其后果是数据备份耗费时间成本大,同时带来业务中断的后果。对于石化行业而言,工业控制系统中枢暂停工作可能导致致命的影响。

为此,针对服务器系统容灾容错需求,提出了实时安全备份及应急接管的技术方案,能够在服务器发生大面积崩溃,或者局部故障的情况下,实现快速无缝接管,在不中断企业信息网络和现场控制网络的前提下,保障服务器系统正常工作。

1 石化工业控制系统的架构

石化工业控制系统一般可分为 3 个层次,其架构原理见图 1。

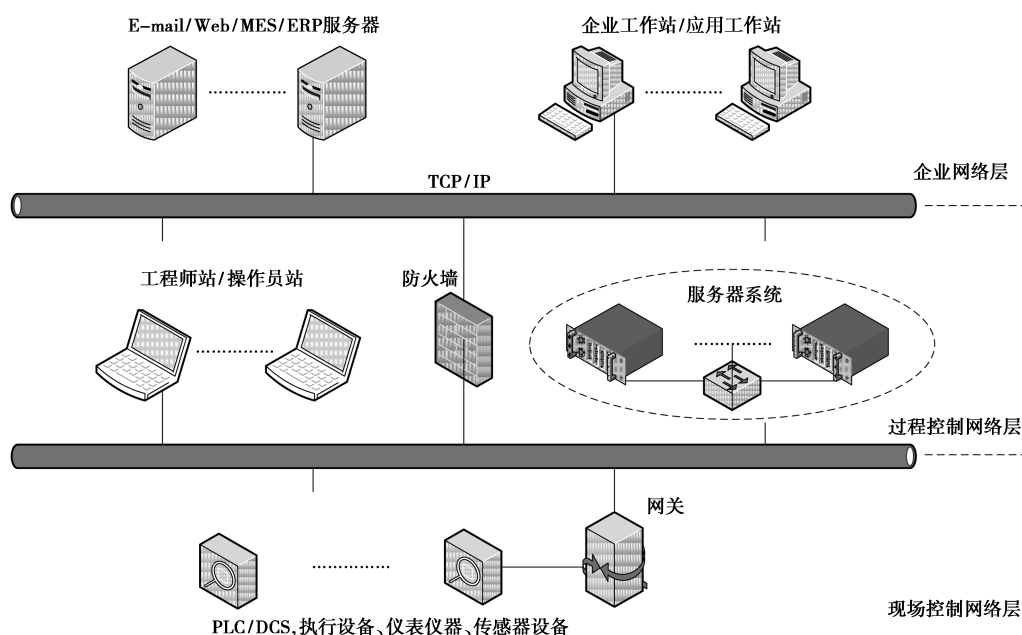


图 1 石化行业工业控制系统的架构原理图

(Web 为网页;MES 为制造执行系统;ERP 为企业资源计划;TCP/IP 为网络通讯协议)

现场控制网络通过可编程逻辑控制器(PLC)和分布式控制器(DCS)实现现场控制,通过执行器完成生产操作,通过现场传感器对各类数据进行实时采集。采集的数据一方面通过现场仪表仪器进行实时显示,同时通过现场网络上传到远程服务器,存储至数据库之中。

企业信息化管理层次通过 Web 服务器、MES 服务器、ERP 服务器、邮件服务器及其他工作站通过人机交互获取远程服务器的数据,根据数据完成相应业务,体现出信息化管理水平。

而过程控制网络中的服务器系统作为工业控制系统的中枢部分,实现了信息化和自动化的交叉融合,是工业控制网络信息存储、处理和传输的重要节

点。服务器系统是网络攻击的重点目标,也是抗灾容错的重点防患部分。服务器信息安全是工业控制系统信息安全的重中之重。

当前工业控制系统普遍存在的问题是缺乏实时安全备份和应急接管能力。传统方式一般只对重要数据进行备份,备份的 PRO 格式文件比较大,且备份的数据难以及时验证,数据正确性验证的时间成本和技术成本较高,数据恢复的时间漫长。同时在服务器出现大面积崩溃,即使是局部故障时,企业管理网络和现场控制网络均会受到不同程度的影响。

2 服务器备份及应急接管技术方案

为了解决工业控制系统服务器存在的问题,提

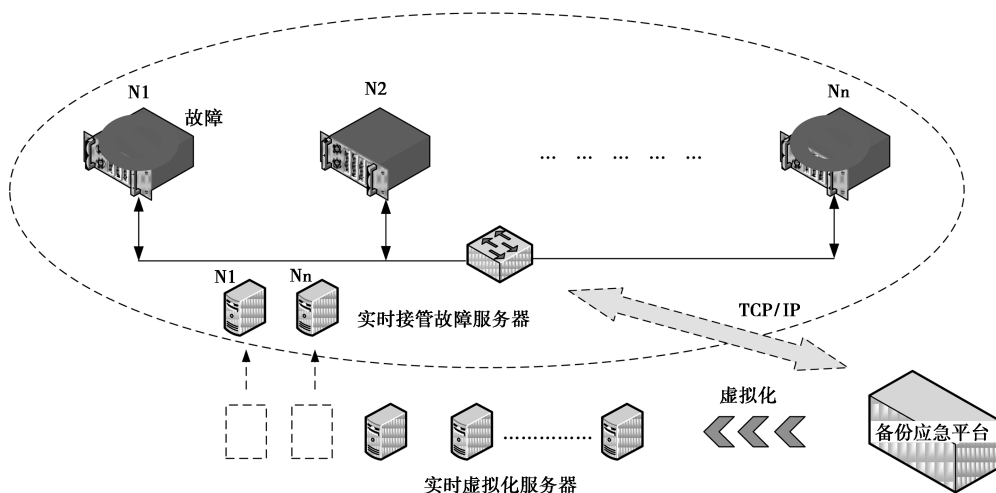


图 2 实时安全备份及应急示意图

出实时安全备份及应急接管的技术方案。针对服务器在软硬件故障、自然灾害和网络攻击的情况下,能够对损坏的服务器进行实时备份和无缝接管,保障服务器系统的正常运维。实时安全备份及应急接管示意图见图 2。

图 2 中备份应急平台能够在任何一台服务器发

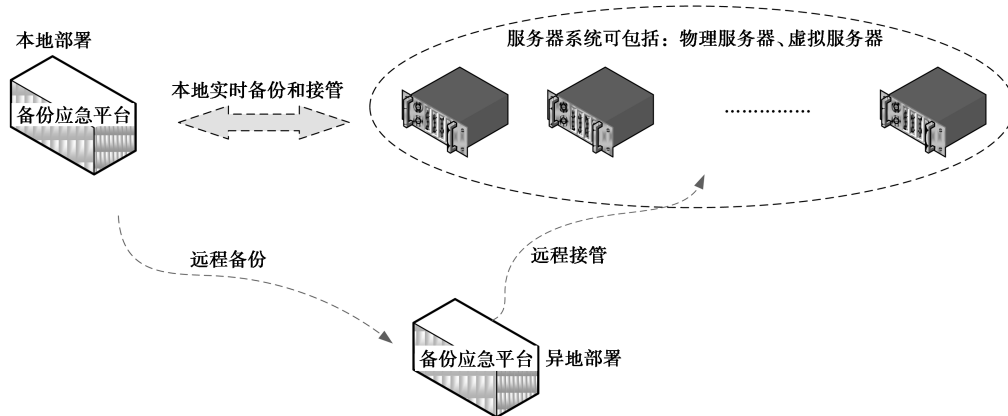


图 3 实时备份及应急接管技术方案原理图

服务器物理平台和虚拟平台的实时备份和应急处理,在单台或多台服务器受到物理损坏、软硬件故障,或者网络攻击时,能够在短短几分钟内进行应急接管。为了防止服务器遭受更大面积的破坏,如自然灾害所导致的服务器系统整体灾难性破坏,在异地部署另一台备份应急平台,提供第二道信息安全屏障。异地备份应急平台保持与本地平台的同步更新,在极端情况下,能够快速无缝接管本地服务器系统,提供对外的正常服务。

3 备份应急平台的关键技术原理

备份应急平台的关键技术在于实时备份及应急接管技术。其技术原理见图 4。

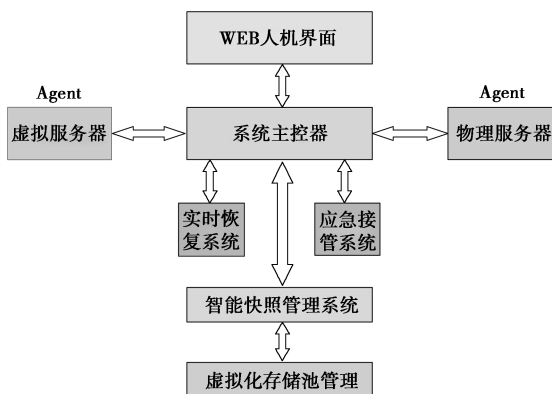


图 4 备份应急平台关键技术原理图

系统主控器是备份应急平台的调度中心,将本地物理服务器和虚拟服务器的镜像数据、以及其他

生软硬件故障或者崩溃的时候,随机接管机房内任何 X86 服务器。通过对多个备份应急平台的集中部署能够实现多达 300 台服务器的应急接管,接管前后保持系统与数据完全一致。实时备份及应急技术方案原理见图 3。

在服务器本地部署备份应急平台,实现对本地

各类实时捕获的数据存入虚拟化存储池之中。除此之外,还将服务器的全部驱动和应用进行实时虚拟化和保存,从而在接管服务器之后能够保持与原系统完全一致无差别化的效果。

虚拟化存储池可为远程异地服务器提供集群管理的虚拟化存储平台,主要存储实时备份的虚拟机文件系统(VMDK)文件,及其他系统驱动和应用的备份文件。

快照管理系统能够管理虚拟化存储池的快照和备份文件,根据系统主控器和应急接管系统的指令快速定位快照和备份文件。

服务器端 Agent 对数据实时变化情况进行跟踪及实时捕获,执行磁盘数据的镜像复制,该功能适用于物理服务器和虚拟服务器。

应急功能系统,当服务器崩溃或者故障后,通过系统主控器调动,从虚拟化存储池中找到相应的快照数据,创建应急的虚拟主机,切换虚拟化路由,并且快速激活虚拟化应急主机接管服务器。

备份应急平台的技术原理决定了该平台能够为多台服务器提供实时备份和快速接管功能,同时具有较高的恢复点目标(RPO)、复原时间目标(RTO)指标。相比传统的以离线备份数据,适用于本地机房定时备份和归档的数据保护方式,备份应急平台提供了更加灵活和有效的保护能力。目前备份应急接管技术在行业领先的有 Novell 公司和上海数腾软件科技股份有限公司。

(下转第 30 页)