工业控制系统的信息安全问题研究*

Research of Industrial Control System Security

何之栋[1] 裘 坤[2] 钟 晨[2] 王海凤[1]
(1 浙江大学智能系统与控制研究所工业控制技术国家重点实验室,浙江 杭州 310027;
2 浙江中控技术股份有限公司,浙江 杭州 310027)

摘 要

分析了工业控制系统的安全要求、典型的威胁与攻击形式,阐释了工业控制系统信息安全与传统 IT 信息安全的区别;分析了现有的控制系统信息安全的解决思路,结合 SP800-82 工业控制系统(ICS)安全指南,介绍了控制系统网络防护的主要措施;总结了热点研究趋势,包括安全通讯协议和安全控制器的设计。

关键词:工业控制系统,信息安全,网络防御,安全协议,安全控制器

Abstract

The operation requirements of industrial control systems are researched.Next,additional security challenges with typical threats and attacks created by the characteristics of ICS are analyzed.Especially,the differences between ICS and traditional IT information security are described.Based on SP800-82 ICS security guidance,this paper presents the main solutions and research trends,including network defense solutions,secured communication protocols,and the design of a secure controller.

Keywords:industrial control systems,security,network defense,secured protocols,secure control

工业控制系统在过程生产、电力设施、水力油气和运输等领域有着广泛的应用[1]。传统控制系统的安全性主要依赖于其技术的隐秘性,几乎未采取任何安全措施[2]。随着企业管理层对生产过程数据的日益关注,工业控制系统越来越多地采用开放 Internet 技术实现与企业网的互连。目前,大多数工业通信系统在商用操作系统的基础上开发协议,通信应用中存在很多漏洞[3]。在工业控制系统与 Internet 或其他公共网络互连时,这些漏洞将会暴露给潜在攻击者。此外,工业控制系统多用于控制关键基础措施,攻击者出于政治目的或经济目的会主动向其发起攻击,以期造成严重后果。例如,2010 年,“震网”病毒席卷全球,伊朗布什尔核电站因遭此攻击延期运行[4]。因此,近年来,工业控制系统的信息安全问题成为一个广泛关注的热点问题。

本文主要首先结合工业控制系统的特点,分析控制系统的要求及其面临的威胁和攻击,其次结合相关标准,从网络防护角度介绍了目前的信息安全解决思路,并介绍了相关的研究趋势,包括安全通信协议和安全控制器。

1 工业控制系统的信息安全分析

1.1 工业控制系统概述

工业控制系统是以计算机为基本组件,用于监测和控制物理过程的系统。这类系统包含了大部分网络系统与物理系统连接的网络化系统。根据其应用范围,控制系统又可分为过程控制系统(PCS),监控和数据采集系统(SCADA),或网络-物理系统(CPS)[5]。

控制系统通常由一系列网络设备构成,包括:传感器、执行器、过程控制单元和通信设备。控制系统通常采用分层结构,典型的控制系统网络结构如图 1 所示,第一层为安装有传感器和执行器等现场设备的物理设施,现场设备通过现场总线网络与可编程逻辑控制器(PLC)或远程终端设备(RTU)连接,PLC 或 RTU 设备负责实现局域控制功能。第二层为控制网络,主要负责过程控制器和操作员站之间的实时数据传输。操作员站用于区域监控和设置物理设施的设定值。第三层为企业网,企业工作站负责生产控制,过程优化和过程日志记录。

根据控制系统的应用特性,可以分为安全相关的应用和非安全相关的应用[6]。安全相关的应用一旦失效,可能会造成受控制的物理系统发生不可恢复的破坏。如果这类控制系统遭受破坏,将会对公共健康和安全产生重大影响,并导致经济损失。

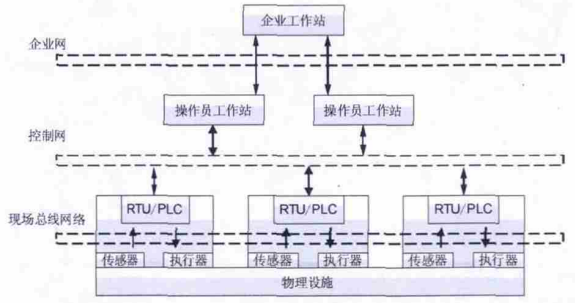

图 1 典型控制系统的架构

1.2 工业控制系统的安全要求

传统 IT 信息安全的技术相对成熟,但由于其应用场景与控制系统存在许多不同之处,因此,不能直接应用于控制系统的信息安全保护[1]。本节主要针对控制系统与传统 IT 信息安全的区别,分析控制系统信息安全的特有属性,并提出控制系统面临的新的挑战。

控制系统的特点之一在于对可用性的要求[1]。因此,传统信息安全的软件补丁方式和系统更新频率对于控制系统不再适用[7]。例如,控制系统的系统升级需要提前几个月进行计划,并且更新

* 国家 863 计划项目(2012AA041105)资助

时需要将系统设为离线状态。而且,在工业应用环境下,停机更新系统的经济成本很高。此外,有些系统补丁还可能违反控制系统的规则设定。例如,2008 年 3 月 7 日,某核电站突然停机,原因是系统中的一台监视工厂数据的计算机在软件更新后重启。计算机重启后将控制系统中的数据重置为默认值,导致安全系统认为用于给核燃料棒降温的水温下降[8]。

控制系统的另一个特点在于对实时性的要求[1]。控制系统的主要任务是对生产过程自动做出实时的判断与决策。尽管传统信息安全对可用性的研究很多,但实时可用性需要提供更为严格的操作环境。例如,传统 IT 系统中经常采用握手协议和加密等措施增强安全性,而在控制系统中,增加安全措施可能会严重影响系统的响应能力,因此不能将传统信息安全技术直接应用于控制系统中。为了保证控制系统具备更强的安全性,控制网络需要实现相关安全机制和标准,这就要求网络满足一定的性能要求。

除了以上两个特点,控制系统与传统 IT 信息系统的最大区别在于控制系统与物理世界存在交互关系。总的说来,信息安全中的许多技术措施和设计准则相对成熟,如认证,访问控制,消息完整性,最小权限等。利用这些成熟的技术可以帮助我们防御针对控制系统的攻击。但是,计算机安全主要考虑信息的保护,对于攻击如何影响物理世界并没有研究。而且,工业控制系统的资源有限,生命周期长,不能直接移植传统 IT 的信息安全技术。因此,虽然目前的信息安全工具可以为控制系统提供必要的防御机制,但仅仅依靠这些机制,无法为控制系统提供充分的深度保护。

当然,与传统 IT 系统相比,控制系统也存在更易操作的特点,为设计系统安全机制提供了便利。控制系统的网络动态特性更为简单,具有服务器变动少、网络拓扑固定、用户人群固定、通信类型固定、使用的通信协议少等特点[9]。

1.3 工业控制系统的威胁

工业控制系统面临的威胁可以分为两种:系统相关的威胁和过程相关的威胁[3]。典型的系统相关威胁和过程相关威胁如表 1 所示。

表 1 工业控制系统的威胁

威胁类型	举例
系统相关的威胁	攻击者使用 Windows 服务漏洞传播恶意代码; 攻击者使得系统栈溢出
过程相关的威胁	攻击者强行插入错误指令,导致过程失效; 攻击者改变报警设定值,使报警失效

系统相关的威胁是指由于软件漏洞所造成的威胁。控制系统从广义上是一种信息系统,会受到系统相关的威胁,如协议实现漏洞、操作系统漏洞等。在控制系统安全项目 CCSP2009[10]报告中,通过 CSSP 安全评估,将一般控制系统的系统相关威胁分为九种类型。表 2 列举了这九种安全问题。

表 2 控制系统漏洞分析

九种漏洞类型	代码质量差
	使用易受攻击的 Web 服务
	网络协议实现的安全功能少
	补丁管理方式薄弱
	认证方式薄弱
	违反最小用户权限原则
	信息泄露
	网络设计漏洞
	网络设备配置漏洞

过程相关的威胁是指工业控制系统在生产过程遭受的攻击。这种攻击利用过程控制的特点,攻击者非法获取用户访问权限后,发布合法的工业控制系统命令,导致工业过程的故障。基于工业控制系统用户与工业过程的交互点,可以将过程相关的威胁分为两类:①影响现场设备的访问控制的威胁;②影响中央控制台的威胁。前者通常发送错误的现场数据到控制系统状态监测中心,从而导致系统状态分析出现错误。后者通常在中央控制台执行合法的命令,但该命令对生产过程而言不合理,将对生产或设备产生负面影响。

控制系统的漏洞一旦被攻击者利用,会遭受不同类型的攻击,具体的攻击形式可以分为:

1)欺骗攻击:在通信过程中伪装成某个合法设备。例如,使用一个伪造的网络源地址。

2)拒绝式服务攻击[11]:系统中任意资源的不可用。例如,设备因忙于应答大量的恶意流量而无法响应其他消息等。

3)中间人攻击[19]:攻击者从通信的一端拦截所有消息,修改消息后再转发到终端接收设备。

4)重播攻击[12]:重复发送某个过时的消息,如用户认证或命令等。

2 工业控制系统的信息安全解决思路

为了防止工业控制系统在通信过程中遭受上述各种威胁与攻击,需要使用多层安全措施完成对系统的保护。本文将以现有的研究成果为基础,从网络边界防护、安全协议和安全控制器方面,介绍控制系统信息安全解决思路。

2.1 网络边界防护

上文所述工业控制系统的系统威胁,一方面是由于系统采用传统 IT 技术,如操作系统、Web 服务器、邮箱的漏洞等造成,另一方面控制系统与企业网实现互连,暴露于公共网络之中,面临更多的攻击。因此,为了保证工业控制系统的安全性,首先需要增强网络边界的防护,以降低由企业网引入的威胁风险。标准 SP800-82《工业控制系统(ICS)安全指南》[13]指出,在处理工业控制系统网络与其他应用网络的连接问题时,需要按照最小访问原则设计,具体分为两点建议:

1)工业控制系统部署网络时,建议隔离工业控制系统与其他企业网络。通常这两类网络的流量不同,且企业网对网络设备变更没有指定严格的控制规程;如果工业控制系统网络流量存在于企业网上,可能会遭受拒绝服务式攻击。网络隔离可以通过采用防火墙等技术实现。

2)如果工业控制系统网络与企业网之间必须建立连接,尽可能地只允许建立一个连接,且连接通过防火墙或非军事区实现。

在具体的技术措施上,SP800-82 从身份认证、访问控制、审计与核查、系统与通信保护等方面详细介绍了可用的技术措施。

(1)身份认证

通过 PIN 码或密码验证申请访问的设备或人员。在网络上传输密码时需要对密码进行加密,通过选取合适的加密哈希函数,可以阻止重播攻击。密码认证还可以辅以其他认证措施,如询问/应答或使用生物令牌或物理令牌。紧急情况下,工业控制系统使用密码和生物认证都存在一定危险。因此在不适合使用密码的情况下,可以采用严密的物理安全控制作为替代。

(2)访问控制

基于角色的访问控制(RBAC)可以用于限制用户的权限,使其能以最小的权限完成任务。系统管理员的通讯需要加以认证,并对其保密性和完整性加以保护,如使用 SSHv2 和 HTTPS 协议。这两个协议都使用公钥/私钥对进行用户认证。通信双方产生并使用对称密钥加密数据交互过程。

RADIUS 远程认证拨号用户服务式目前使用最多的认证和授权服务。它使用 IEEE802.1x 和 EAP 协议,可以在网络的各个层实现用户认证。例如,防火墙和接入路由可以作为认证代理。当无线设备或中断用户设备需要与其连接时,认证代理向设备

发出询问,设备通过认证服务器返回认证信息,从而获得授权和接入许可。

调制解调器经常用于提供备份连接。回叫系统通过存储于数据库中的回叫号码,确认拨号者是否为合法用户。远程控制软件需要使用唯一的用户名和密码,加密和审计日志。链路层的邻居认证需要使用 CHAP 协议等实现。

无线用户接入和网络设备间的链接可以使用多种方式实现,如 IEEE 802.11b/g 的网络接入点方式。所有的无线通信需要使用强加密,如 IEEE802.11i 中的 AEP 加密。无线接入需要使用 IEEE802.1x 认证客户。

(3)审计与核查

工业控制系统需要进行周期性的审计,验证内容包括:测试阶段的安全控制措施在生产系统中仍安装使用;生产系统不受安全破坏,如果受到安全破坏则提供攻击的信息;改动项目需要为所有的变动建立审查和批准的记录。

周期性的审计结果用一定的度量表示,用于显示安全性能和安全趋势。审计需要使用特定工具进行记录维护,需要工业控制系统中的组件支持。审计有利于维护工业控制系统在系统生命周期内的完整性。工业控制系统需要为审计工具提供可靠的同步时间戳。工业控制系统应用中维护的日志可以存储于多个地点,加密或不加密都是可以的。

(4)系统与通信保护

系统与通信的保护可以通过网络防护措施,如防火墙和入侵检测系统等,以及数据加密,如 VPN 等实现。

网络防火墙控制不同安全等级的网络区域间的数据流量。NIST SP 800-41 为防火墙的选择和防火墙策略提供了指导。在工业控制系统环境下,需要在控制网和企业网之间部署防火墙。防火墙包含的特征功能包括:事件记录,入侵检测系统,基于非军事区的路由,访问列表等。

当系统被嗅探或攻击时,入侵检测系统发出警报。入侵检测系统通过在网络的各个关键点收集信息,分析数据包内容发现恶意流量,并发出警报、废弃无效数据、记录事件和活动并触发其他安全响应。对于多种工业控制系统中的应用协议所受到的攻击,如 DNP 和 ICCP,入侵检测系统也会增加相应的攻击特征。

基于 IPsec 的 VPN 可以为网络边界的通信提供安全隧道,通常在相应的防火墙上执行。IPsec 可以保证完整性、认证和数据保密性。在隧道入口处,IP 包外增加额外的数据包头,路由器使用新的包头信息转发数据,到达隧道出口时,将原始 IP 包提取出来。在用户认证过程中,IPsec 通常使用私钥和 RSA 签名。在消息认证和完整性保护时,使用 MD5 或 SHA 哈希函数。在数据加密时,使用 AES 或 3DES。IPsec 还使用 Diffie-Hellman 作为对称密钥推导。IPsec 设备使用 IKE 协议认证其他设备、协商和分配对称加密密钥以及建立 IPsec 安全连接。

控制系统的安全管理包括检测、分析、提供安全和事件响应。具体内容包括动态调整安全要求,安全漏洞的优先级排序,以及安全要求到安全管理的映射;认证和授权服务器,安全密钥,流量过滤,IDS,登录等。SNMP 用于管理 IP 网络资源,如路由,防火墙和服务器等。SNMP 也可用于提供控制系统网络的集中管理。SNMPv3 包括的安全特性有消息完整性,认证和加密。SNMPv3 使用 MD5 和 SHA 哈希算法和 DES 以及 AES 加密算法。

(5)其他措施

为了保证网络操作的可靠性,工业控制系统需要设置冗余拓扑和功能。工业控制系统中大多使用以太网和 IP 网络作为通信协议。以太网层的冗余可以通过在局域网内使用 RSTP 协议中的网格拓扑而实现。IP 层的冗余通过路由间的备份链接,如 OSPF 动态路由协议,和 IP 网络冗余接入,如 VRRP 协议等。MPLS 可以为 IP 网络中的虚拟任意协议数据提供可靠的数据传输。隧道如 L2TP 协议等也可以为 IP 网络中的数据提供可靠传输。

在控制系统中的时钟和网络设备需要精确同步,事件日志记录时也需要记录下准确的时间。NTP 协议和 IEEE1588 协议可以用于时间同步。NTP 协议在因特网中广泛使用,IEEE1588 协议则主要满足控制系统对于时钟同步的要求。这两种协议均可由独立设备提供服务,或者有其他网络设备的组件提供服务。

2.2 协议安全性

工业通讯协议,如 MODBUS 协议等,协议设计时未采取安全措施。然而随着控制系统与外部网络的连接增多,需要增加通信双方的认证过程。协议的安全性可以通过两种方式提高,一是直接修改协议,增加认证功能;二是在不修改现有协议的基础上,增加信息安全层。

文献[14]设计了一种认证型 Modbus 协议,该协议通过对消息使用加密函数和哈希链,增强 Modbus 协议的认证功能,从而使攻击者无法伪装成主机。同时利用一个压缩函数,减少数据存储大小。这种方式可以增加协议对于通信双方的认证过程,但同时也会增加通讯负担,即每次通话传输的消息都需要经过加密认证,不一定能满足控制系统对于实时性的要求。因此在设计时需要同时考虑计算效率与计算消耗。

文献[15]借鉴功能安全的概念,提出了一种在通信系统之上增加信息安全模块的方法。控制系统的功能安全在传输系统的基础上增加功能安全层,无需改变底层传输系统,即可实现系统的故障安全。类似地,文献[15]设计一种信息安全模块,用于保护端到端通信的认证、完整性和保密性。所谓的安全模块不是指简单的物理模块,而是与 PROFINET IO 中的设备模型相对应,是一个软件实现。如图 2 所示,安全模块从应用层中获取过程数据,通过加密算法加密过程数据,利用 MD5 算法计算消息完整性编码,状态字节用于表示消息完整性和超时。安全模块通过参数化,可以适应不同的安全需求和不同的计算能力。消息完整性编码可以防止中间人攻击,例如,攻击者截取发送的消息并篡改过程数据,由于没有密钥,无法计算出准确的消息完整性编码,接受者在接收到消息后对 MAC 进行验证,如果无法验证其正确性,则会修改状态字节,用以汇报受攻击状态。

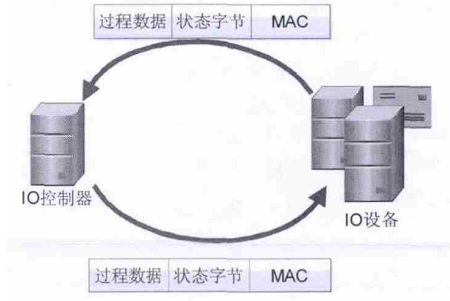

图 2 安全数据传输示意图

安全模块是置于 PROFINET IO 之上的软件层,只能用于防御基于网络的攻击,而不能保证设备安全。如果攻击者获取了设备的控制权,那么数据会被操控,而安全模块将无法产生作用。因此,可以将安全模块可以与设备安全措施相结合,解决设备和网络安全。

协议安全性主要是体现在对传输数据进行加密处理,保证消息的完整性和保密性,并实现对设备的安全认证。在实际应用

中，需要考虑两个影响因素，一方面，由于加密措施的计算量大，对通信实时性和系统的可用资源都会产生影响，二是需要设计合理有效的密钥管理方法。

2.3 控制器设计

以上从网络防护和通讯协议的角度介绍了两种安全问题解决思路，但其本质上都是对信息的保护。无论是何种攻击，其最终的目的都是实现对物理设施的破坏，因此，需要研究攻击对于系统的状态预测和控制算法的影响，从物理系统的角度设计防御措施。

为了理解控制系统与物理世界的交互过程，首先需要分析攻击对于物理系统的影响；其次基于控制命令和传感器的测量值，预测物理系统应有的现象，从而判断是否受到攻击者的影响；最终在控制器算法设计时将攻击因素考虑在内，设计出一种可以抵御攻击的控制算法。

文献[16]和文献[17]分别对重播攻击和完整性攻击进行分析，采用卡尔曼滤波和 $\chi 2$ 故障检验法检测系统是否受到攻击。这种检测方法基于物理模型，可以作为基于网络和计算机系统模型的入侵检测的补充。在设计检测算法时，需要考虑实时性和嵌入式平台的计算能力限制。

文献[18]首先建立物理系统的典型模型，将物理系统简化为一个线性系统。其次，针对 DOS 攻击和欺骗攻击，在原有线性系统模型基础上增加攻击因素。如图 3 所示，攻击因素可能分布在闭环控制回路的不同部分，传感器部分、执行器部分和设备部分。基于不同的攻击因素，设计带状态监测器的控制算法，用以检测系统的运行状态。该算法可以使系统在受到拒绝时服务攻击时，仍然处于安全状态；在受到欺骗攻击时，可以检测出攻击。

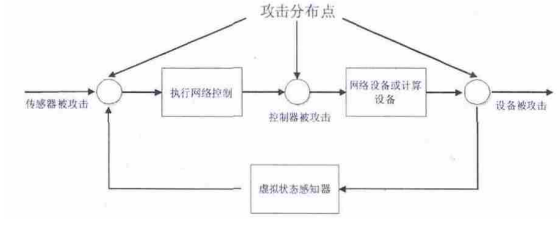

图 3 闭环系统攻击示意图

安全控制器的设计目前仅限于学术领域的研究，在实际系统中的应用尚未成熟。这是由于设计控制器需要建立相对精确的物理模型，普适性不高。可能的解决思路是在控制器的硬件设计时采用主控制器和安全控制器的模式，利用旁道信息，如程序执行时间、代码执行顺序等，如果主控制器与安全控制器的旁道信息不一致，则采取安全措施。

3 结束语

本文首先研究了工业控制系统的行业特点和需求，并分析了工业控制系统面临的威胁，其次在深入了解相关行业信息安全保障应用行规之后，介绍了适用于工业控制系统的信息安全现状，从网络防护、协议安全性和控制器设计这三个角度分析了目前的研究思路，具有一定的借鉴意义。

参考文献

[1]Dacfey Dzung, Martin Naedele, et al. Security for Industrial Communication Systems. Power Delivery, IEEE Transactions on 23.4 (2008): 2628–2629

[2]Stamp, Jason, et al. Common vulnerabilities in critical infrastructure control systems.SAND2003–1772C. Sandia National Laboratories (2003)

[3]Ten, Chee–Wooi, Govindarasu Manimaran, and Chen–Ching Liu. Cybersecurity for critical infrastructures: attack and defense modeling. Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on 40.4 (2010): 853–865

[4]Cárdenas, Alvaro A., et al.Attacks against process control systems: risk assessment, detection, and response.Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security. ACM, 2011

[5]Hadziosmanovic, Dina, et al.Challenges and opportunities in securing industrial control systems.Complexity in Engineering (COMPENG), 2012. IEEE, 2012

[6]Yan, Ye,et al.A survey on cyber security for smart grid communications.(2012): 1–13

[7]杨建军，唐一鸿.工业控制系统信息安全标准化[J].信息技术与标准化，2012(3)：20–23

[8]Amanullah, M. T. O., A. Kalam, and A. Zayegh.Network security vulnerabilities in SCADA and EMS.Transmission and Distribution Conference and Exhibition: Asia and Pacific, 2005 IEEE/PES. IEEE, 2005

[9]刘威，李冬，孙波.工业控制系统安全分析[C]//中国计算机学会计算机安全专业委员会. 第 27 次全国计算机安全学术交流会论文集. 中国计算机学会计算机安全专业委员会，2012：3

[10]Gupta, Rachana Ashok,and Mo–Yuen Chow.Networked control system: Overview and research trends.Industrial Electronics, IEEE Transactions on57.7 (2010): 2527–2535

[11]Amin,Saurabh,Alvaro Cardenas,and S.Sastry.Safe and secure networked control systems under denial–of–service attacks. Hybrid Systems: Computation and Control (2009): 31–45

[12]Mo, Yilin, and Bruno Sinopoli.Secure control against replay attacks.Communication, Control, and Computing, 2009. Allerton 2009. 47th Annual Allerton Conference on. IEEE, 2009

[13]唐一鸿，杨建军，王惠莅.SP800–82《工业控制系统(ICS)安全指南》研究[J].信息技术与标准化，2012，Z1:44–47

[14]Liao, Gen–Yih, et al.Toward authenticating the master in the modbus protocol.Power Delivery,IEEE Transactions on 23.4 (2008): 2628–2629

[15]Akerberg, Johan, and Mats Bjorkman.Exploring security in profinet io.Computer Software and Applications Conference, 2009. COMPSAC´09. 33rd Annual IEEE International. Vol. 1. IEEE, 2009

[16]Mo, Yilin, and Bruno Sinopoli.Integrity attacks on cyber–physical systems.Proceedings of the 1st international conference on High Confidence Networked Systems. ACM, 2012

[17]Mo, Yilin, and Bruno Sinopoli.Secure control against replay attacks.Communication, Control, and Computing, 2009. Allerton 2009. 47th Annual Allerton Conference on. IEEE, 2009

[18]Cárdenas, Alvaro A., Saurabh Amin, and Shankar Sastry. Research challenges for the security of control systems.Proceedings of the 3rd conference on Hot topics in security. USENIX Association, 2008

[19]Wei, Dong, et al. An integrated security system of protecting smart grid against cyber attacks.Innovative Smart Grid Technologies (ISGT), 2010. IEEE, 2010

[收稿日期：2013.7.10]