基于 TPCM 可信根的主动免疫控制系统防护设计*

孙 瑜,洪 宇,王炎玲

(北京可信华泰信息技术有限公司,北京 100195)

摘 要: 目前针对工业控制系统的安全风险与日俱增,传统"封堵查杀"的防护技术难以有效应对当前所面临的安全威胁,急需一套更适合工控系统环境的安全解决方案。结合我国自主创新的可信计算 3.0 关键技术,提出一种基于 TPCM 可信根的适用于工业控制系统的主动免疫防护方案,通过对关键节点的可信构建使工业控制系统防护更加透彻,安全处理融洽一致,为工业控制系统构建主动免疫防御能力,使之能够有效识别和防御未知威胁。

关键词: 可信计算 3.0;可信平台控制模块;PLC;工业控制系统;主动免疫

中图分类号: TP393.08 **文献标识码:** A **DOI:** 10.19358/j.issn.2096-5133.2021.03.003

引用格式: 孙瑜,洪宇,王炎玲. 基于 TPCM 可信根的主动免疫控制系统防护设计[J].信息技术与网络安全,2021,40(3):14-18.

An active immune protection design for industrial control system based on trust root of TPCM

Sun Yu, Hong Yu, Wang Yanling

(Beijing Huatech Trusted Computing Information Technology Co., Ltd., Beijing 100195, China)

Abstract: With the rapid development and application of industrial information, cybersecurity risks are increasing. The traditional "blocking and killing" protection technology is difficult to deal with the current security threats. There is an urgent need for a more suitable industrial control system environmental security solution. This paper combined with our country's independent innovation of trusted computing 3.0 key technology, and proposed an active immune protection scheme based on the root of trust of Trusted Platform Control Module(TPCM) for industrial control systems. By constructing key trust nodes, it enhances the protection capabilities of industrial control systems, and handles security incidents in a harmonious and consistent manner, which builds active immune defense capabilities for industrial control systems, and can effectively identify and defend against unknown threats.

Key words: trusted computing 3.0; trusted platform control module; PLC; industrial control system; active immune defense

0 引言

目前,随着网络空间成为继陆、海、空、天之后的第五维空间,我国网络安全形势面临着严峻的挑战。网络安全的首要问题是解决核心技术受制于人的问题,亟需建立创新发展的主动免疫可信防护体系[1]。我国的国家关键基础设施运行往往是由工业控制系统的生产系统来实现的,数字化控制系统已成为工业控制系统的普遍趋势。数字化控制系统是国家关键信息基础设施的重要组成部分,一旦遭到破坏、丧失功能或者数据泄露,将会给国家安全、国计民生、公共利益带来严重危害。因此数字化控制系统往往成为网络战的第一目标,针对工业控制系统的攻击通常具有极强的针对性和隐蔽性,能够突破以隔离为主的安全防护体系,使现有安全防护失效。

《中华人民共和国网络安全法》第三十一条规定:"关键信息基础设施在网络安全等级保护制度的基础上,实行重点保护"。国家网络安全等级保护 2.0 核心标准《GBT22239-2019 信息安全技术网络安全等级保护基本要求》、《GBT25070-2019 信息

* 基金项目:国家重点研发计划(2018YFB0803502)

安全技术 网络安全等级保护安全设计技术要求》、《GB/T 28448-2019 信息安全技术网络安全等级保护测评要求》于 2019 年 12 月正式实施，在等级保护 2.0 基本要求及设计要求中强调了基于可信根的可信验证在整个信息系统防护中的重要地位。一方面可信验证是通用要求，是所有系统的基础性安全要求；另一方面在基本要求中对信息系统进行分类，在扩展要求中对工业控制系统也提出了更具针对性的安全防护要求[2-4]。

综上，设计具有可信根和可信验证功能的工业控制系统，对我国生产制造业和国家关键信息基础设施的发展有着重要的意义。

1 工业控制系统的安全分析

随着信息化技术在工业控制领域的快速发展，工业互联网、智能制造等技术的应用推广，控制系统的物理隔离被打破，孤岛现象逐步消失，其开放性带来便利的同时也扩大了安全暴露面，安全风险也与日俱增。对于企业而言，工业控制系统与 IT 的集成和融合不可避免，由此会面临愈加复杂的安全风险，如何进行工业控制系统安全防护建设，已经成为一个制约企业发展的重要问题。卡巴斯基 Kaspersky 早在 2016 年曾对 188 019 套工业控制系统所面临的威胁进行调查研究，发现超过 91%的工业控制系统存在安全漏洞，所有安全漏洞均可能被非法远控和利用，绝大部分组织或企业的工控系统都面临网络威胁。

目前工业控制系统的安全防护主要依靠防火墙、网闸、漏洞扫描、主机加固、防病毒软件、USB 禁用等手段。然而，网络空间安全主要是攻防双方的安全博弈，由于双方的不对称性使以上防护手段不能有效地发挥作用。如在工业控制系统领域，防病毒软件病毒库往往不能够及时更新，因为每一次更新变化都可能对工业系统运行带来不良影响，未实时更新的病毒库不能有效防御新出现的病毒。另外，即使实时更新的病毒库也不能有效应对未知病毒，例如 Stuxnet 病毒作为一种新病毒，在其攻击系统前，防病毒软件由于病毒库中没有该病毒特征值而无法予以发现和识别。再如漏扫机制，在其连接敏感设备并进行漏洞数据收集时，可能给系统带来无法接受的生产中断，对生产造成极大的损失[5-7]。

较一般信息系统而言，工业控制系统具备其特殊的特点及要求，如强实时性通信、通信协议丰富多样、系统不允许重启、人和控制过程安全、加入安全功能及机制后不影响控制流程、设备不易更换且设备生命周期较长等。鉴于工业系统自身特点及对安全的特殊要求及限制，传统的“封堵查杀”安全防护技术多是基于特征匹配的方法，无法解决利用未知漏洞的攻击，难以有效解决工业控制系统的安全问题。无论是外部攻击还是内部恶意行为(如病毒感染、员工失误、员工/服务商人员恶意修改等)，最终都是通过改变控制系统的程序组态实现对工业控制系统的攻击，或者直接取得对控制系统的操控权。

可信计算 3.0 技术将控制系统计算节点构建为工业生产过程控制的可信计算环境，能够保障业务逻辑不被篡改，可对业务环境和使用者进行有效鉴别验证，通过安全管理中心支撑下的计算环境安全、区域边界安全、通信网络安全组成三重防护体系结构，构建纵深防御、主动免疫的防护能力，从而解决工业系统当前面临的安全风险，并同时满足国家等级保护标准要求[8-12]。

2 控制系统的可信防护设计

2.1 我国可信计算发展现状

相比于国外可信计算技术，我国在可信计算方面的研究起步较早，于 1992 年发明了微机保护卡，通过密码技术为 DOS 运行环境中的 PC 实施安全保护，达到了无病毒、自我免疫的效果。历经二十多年的发展，我国可信计算技术已经拥有了完整的技术理论、逐步完善丰富的标准体系[13-21]和产品应用。

我国自主创新的可信计算 3.0 技术是以 TPCM 为技术路线，核心的主动免疫双体系架构是基于自主创新的对称与非对称结合的密码体制，将其作为主动免疫基因；在系统设备硬件层通过植入 TPCM 可信控制模块作为可信根，内置 TCM 模块具备可信控制功能，将密码与控制相结合，构建计算与防护并行的可信计算节点，由信任根实现对可信计算平台的主动控制；在设备软件层通过部署可信软件基软件，实现宿主机操作系统和可信软件基的双重系统核心，无需改变应用层软件即可实现对系统的执行环境及进程行为的主动可信度量，为系统构建主动免疫防御能力；在系统网络层，通过可信连接技术实现对接入网络源、目标平台的可信验证和控制，确保网络连接的可信性，将可信由单点拓

展至整个网络[9]。

随着可信计算体系标准的逐渐丰富和完善,越来越多的企业开始对可信计算进行研究,目前市场上已有几十家企业推出了可信计算产品,可信计算产品已具备完整的产品体系,目前已覆盖芯片、固件、板卡、软件、整机、网络、外设、专用设备等。可信计算产品最核心的可信模块包括 TPCM 可信根硬件和配套可信软件基软件体系,TPCM 可信根实现方式主要包括 CPU 内置和外置插卡/板载芯片。

2.2 可信 PLC 构建

PLC 作为 SCADA 和 DCS 等主要工控系统中的现场控制组件,通常应用于工业过程控制领域。对 PLC 的编程控制和诊断,一般通过常见的 Unity Pro、WINCC 等下位机软件来实现。

可信 PLC 的构建基于可信计算 3.0 技术,采用“计算+防护”并行的双体系架构,通过在 PLC 硬件层植入主动度量控制芯片 TPCM 构建可信根,实现计算和可信的融合。具体构建方式如下:

构建可信 PLC,即在原有的 PLC 基础上融合可信芯片,同时在 PLC 的操作系统中内置预装可信功能模块,从而构建可信 PLC 环境。在可信 PLC 启动时,可信机制首先进行自身安全诊断,然后进行 PLC 的计算环境检测,并对 PLC 的业务模块进行检测,当通过上位机软件对 PLC 进行编程控制和诊断时,可信机制能够度量和执行验证代理,并对 PLC 的操作系统进行完整性度量、验证和存储,对上位机软件进行可信验证,PLC 根据上位机软件的指令开始运行。

可信 PLC 的功能除了包括 PLC 本身带有的处理、通信、输入输出等核心功能外,还包括 TPCM。作为可信计算模块, TPCM 是可信功能结构的核心,主要发挥存储信任根、报告信任根和计算信任根的作用,并为工控系统其他组件提供基本的存储保护功能及 PCR 和签名密钥等可信资源。其结构如图 1 所示。

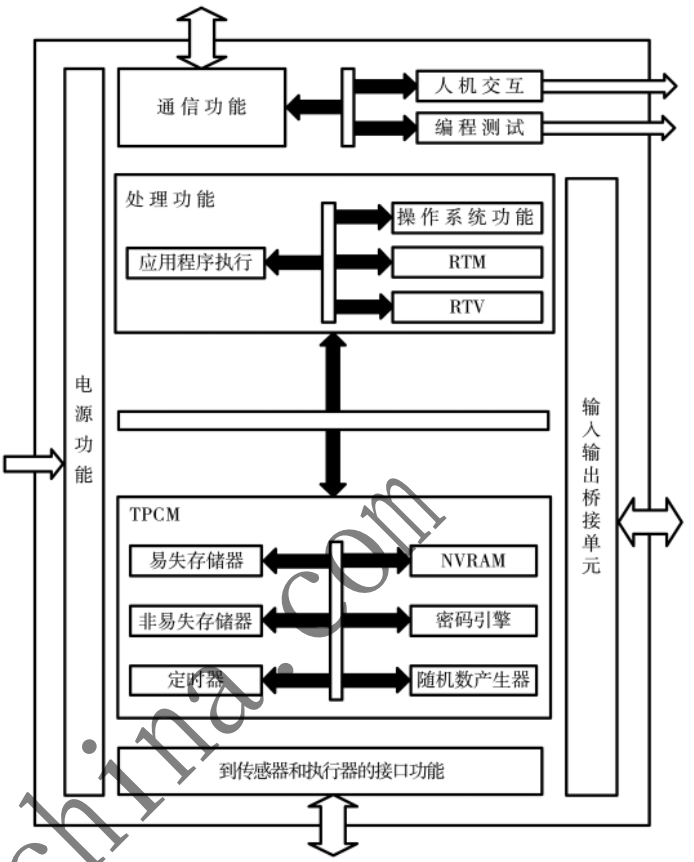

图 1 可信 PLC 的功能结构图

从整机设备体系结构上看,最关键的设计就是如何将可信根接入 PLC 整机。可信根是整体可信保障体系的核心。针对工控 PLC,一种典型的信任链构建及传递过程为:在 PLC 设备上电以后,TPCM 模块有优先执行权,对初始化的固件镜像进行可信度量验证,待验证通过后,执行权再由 TPCM 模块交给初始化固件,PLC 主控 CPU 读取验证过的固件镜像并执行,从而完成 PLC 设备初始化工作。在产品实现上,TPCM 可由独立芯片进行整机构建,再配合修改启动时序电路、独立存储资源从而实现可信 PLC;或者利用 PLC 主控 CPU 内部安全芯片或IP 核实现 TPCM 功能,例如我国飞腾 CPU 基于 AMAB 总线 AXI 扩展接口能够实现安全 IP 核的资源隔离,可用该安全 IP 核实现 TPCM,构建可信 PLC 从而节省了 PLC 整机硬件设计修改工作。

采用飞腾 2000/4 型号 CPU 作为 PLC 的主控 CPU 实现信任链启动。飞腾 2000/4 型号 CPU 是 ARMV8 架构支持可信,可以完整运行 Linux、嵌入式 Linux 之类操作系统,并且内部已经集成 SM2、SM3、SM4 国密算法引擎和真随机数生成器,具备实现可信根的密码资源和计算资源。在整机上电后飞腾 CPU 首先加载飞腾 PBF 固件初始化 CPU, 同时将 CPU 中的四个核中的一个作为可信核以实现 TPCM 功能,另外三个核作为计算核以实现 PLC 原有的业务逻辑。用飞腾 CPU 分核实现安全和计算,这种设

计不仅节省了传统方案中两个分立芯片的开销，并且利用 CPU 内部的高精度实现，达到安全业务和计算业务之间的高带宽低延时的连接效果。同时它又发挥出计算和安全由一个芯片实现带来的诸多优势，如：物理尺寸减小，整体开销、费用降低，无需因为安全额外修改 PLC 主板电路等。在 PBF 初始化后，可信核也就是 TPCM 首先开启度量工作，度量 PLC 的 Boot.bin 引导文件、内核镜像、设备树文件等，可信核通过总线获取存储于 Flash 芯片上的数据文件并通过 SM3 计算出哈希值，与内部存储的Boot.bin 引导文件、内核镜像、设备树文件预期值进行比对；当可信验证通过后可信核发出信号，计算核开始工作加载 Boot.bin 引导文件、内核镜像、设备树文件等，PLC 进入工作状态实现可信启动。当 PLC 进入工作状态后，位于 PLC 操作系统的可信软件基依据策略周期性度量操作系统的关键数据结构（例如系统调用表、内核代码段、关键驱动等），以确保 PLC 在可信安全的运行空间中执行工业控制任务。

3 安全管理中心支撑下的工业控制系统防护

可信 PLC 同时结合可信上位机和可信服务器，可逐步构建出工业控制系统的可信计算环境。可信上位机的安全防护主要利用可信根、可信软件基提供的基础安全保障，做好对组态的管理和对非法组态修改的识别。系统组态的改变主要包括由病毒感染引起的修改、黑客入侵修改、未经批准的恶意修改、经批准但因工作疏忽造成的错误修改。无论哪种情况都可以利用可信计算的防护机制进行阻断修改。即需要做好对组态的基准值管理，建立操作系统和工业控制软件的基准值采集和管理机制。

在工业控制系统内包括并涉及大量设备，对多源异构设备的集中安全管理是一个难点，可信安全管理中心可实现对系统内众多设备的统一管理，确保安全策略的有效一致性，同时便于安全管理和监测。工业控制系统的另一个难点就是 OT 和 IT 的结合问题，传统网络安全防御的处理机制并不适用于工业控制系统，例如在典型车间，当报警值高于联锁值，则容易造成非计划停车，即在没有对报警处理的情况下出现停车，从而造成重大的经济损失。因此工业控制系统安全在定义策略时要考虑到安全阻断行为会触发怎样工业行为，管理中心就是统一制定安全策略的平台，安全管理员通过管理中心进行安全策略的制定和预演，依据工业系统的应急措施和处理逻辑制定出符合现场的安全防护策略。

4 结论

当前工业控制系统“封堵查杀”的防护技术难以应对当前所面临的安全威胁，本文基于我国自主创新的可信计算 3.0 技术，针对工业控制系统 PLC，提出了主动免疫的计算和防护并行双体系架构，并以此实现 PLC 节点从启动到运行的信任链建立和传递，同时构建了工业控制系统关键计算节点可信 PLC、上位机和服务器，克服了工业控制系统被动防护的现状，使工业控制系统在计算运算的同时实现安全防护，保障工业系统逻辑计算全程可测可控，不被干扰，确保计算结果与预期结果的一致性，为工业系统的安全运行提供安全支撑。

参考文献

[1] 沈昌祥.用可信计算 3.0 筑牢网络安全防线[J].信息安全研究，2017，3(4)：290－298.

[2] 国家市场监督管理总局，中国国家标准化管理委员会.GB/T 22239－2019 信息安全技术 网络安全等级保护基本要求[S].北京：中国标准出版社，2019.

[3] 国家市场监督管理总局，中国国家标准化管理委员会.GB/T 25070－2019 信息安全技术 网络安全等级保护安全设计技术要求[S].2019.

[4] 国家市场监督管理总局，中国国家标准化管理委员会.GB/T 28448－2019 信息安全技术 网络安全等级保护测评要求[S].2019.

[5] 王晔，靳方略，吕铭心.油田工业控制系统网络安全解决方案研究[J].信息技术与网络安全，2020，39(10)：38－43.

[6] 赵国玺.工业控制系统的完整性与运行安全[J].流程工业，2020(9)：25－30.

[7] 李占英.分散控制系统(DCS)和现场总线控制系统(FCS)及其工程设计[M].北京：电子工业出版社，2015.

[8] 陈卫平.可信计算 3.0 在等级保护 2.0 标准体系等中的作用[J].信息安全研究，2018，4(7)：633－638.

[9] 沈昌祥.用主动免疫可信计算 3.0 筑牢网络安全防线营造清朗的网络空间[J].信息安全研究，2018，4(4)：282－302.

[10] 沈昌祥，左晓栋.网络空间安全导论[M].北京：电子工业出版社，2018.

[11] 沈昌祥，田楠.按“等保 2.0”用主动免疫可信计算筑牢“新基建”网络安全防线[J].信息安全与通信保密，2020(10)：2－9.

[12] 沈昌祥.离开“封堵查杀”,怎样确保网络安全?[J].信息安全与通信保密,2018(11):13-15.
[13] 国家质量监督检验检疫总局,中国国家标准化管理委员会.GB/T 29827-2013 信息安全技术 可信计算规范 可信平台主板功能接口[S].北京:中国标准出版社,2014.
[14] 国家质量监督检验检疫总局,中国国家标准化管理委员会.GB/T 29829-2013 信息安全技术 可信计算密码支撑平台功能与接口规范[S].2013.
[15] GB/T 37935-2019 信息安全技术 可信计算规范 可信软件基[S].2019.
[16] GB/T 38638-2020 信息安全技术 可信计算 可信计算体系结构[S].2020.
[17] GB/T 39935-2019 信息安全技术 可信计算规范 可信软件基[S].2019.
[18] GB/T 29828-2013 信息安全技术 可信计算规范 可信连接架构[S].2013.
[19] 国家密码管理局.GM/T 0011-2012 可信计算 可信密码支撑平台功能与接口规范[S].2012.
[20] 国家密码管理局.GM/T 0012-2012 可信计算 可信密码模块接口规范[S].2012.
[21] 国家密码管理局.GM/T 0013-2012 可信计算 可信密码模块符合性检测规范[S].2012.

(收稿日期:2020-11-26)

作者简介:

孙瑜(1977-),男,博士,正高级工程师,主要研究方向:可信计算、网络安全、等级保护。

洪宇(1986-),男,硕士,高级工程师,主要研究方向:可信计算、等级保护。

王炎玲(1986-),通信作者,女,硕士,高级工程师,主要研究方向:可信计算、网络安全。E-mail:wangyanling@httc.com.cn。

“区块链安全技术研究”主题征文

区块链技术作为新一代信息技术的底层技术,以其可信任性、安全性和不可篡改性,让更多数据被解放出来,推进了数据的合理利用,在数字资产管理、社会治理、商业交易、物联网、知识产权保护乃至智能制造等领域拥有广阔的应用前景。同其它新技术一样,区块链技术发展也面临新的安全问题,如区块链中的共识算法会随着密码学和计算技术的发展而变得越来越脆弱,对计算资源的掌控可能导致系统混乱,区块链隐私保护与匿名追溯难等问题。开展区块链安全技术研究,对解决行业应用痛点,推进传统产业数字化转型,提高数字经济发展效率和质量具有重要现实意义。

《信息技术与网络安全》期刊服务中国电子“打造国家网信产业核心力量和组织平台”的使命,追踪前沿技术发展动向,现诚挚邀请业内专家学者就区块链安全问题开展深入研究和探索,优秀征文将刊发在《信息技术与网络安全》期刊(2021 年第 5 期)主题专栏。征文主题及方向如下:

一、征文主题:区块链安全技术研究

分主题方向包括但不限于如下范围:

(1)区块链技术 6G 网络应用;(2)智能合约安全性分析及标准;(3)区块链安全前沿技术发展现状;(4)区块链隐私保护前沿技术;(5)区块链技术安全与形式化验证;(6)区块链技术与关键基础设施安全。

二、稿件要求

论文要求观点鲜明、逻辑严谨,论据充分、方法合理、数据翔实,能够反映区块链安全领域的最新研究成果。投稿文章须未在其他期刊或者出版正式论文集的会议上刊登过,且不在其他刊物或会议的审稿过程中,不存在一稿多投现象;保证文章的合法性(无抄袭、剽窃、侵权、虚假引用等不良学术行为),字数 4000-6000 字左右。稿件经录用后,在《信息技术与网络安全》(正刊)上以技术专栏形式发表。

三、投稿方式

官方投稿网站(http://www.pcachina.com)注册、投稿。注册后请投稿在“区块链”栏目。

四、时间安排

截稿日期:2021 年 4 月 10 日;出版日期:2021 年 5 月 10 日。

特约主编及联系方式:

盖珂珂,北京理工大学,gaikeke@bit.edu.cn。

关志涛,华北电力大学,guan@ncepu.edu.cn。