案例 1

江苏敏捷科技股份有限公司

中车株所工业数据智能安全云平台

引言：

敏捷科技成立于 2008 年，由全球主动信息防护技术原创团队创办，是国内首家原创数据加密软件厂商，专注于为企业、政府及机构解决数据安全及数据管理难题。从 2002 年率先推出填补国内空白的自主知识产权数据加密产品，到全国首发第一套央企商业秘密保护解决方案，再到数据安全卫士系统 DGS 这一整体数据安全与管理解决方案，再到工业数据安全解决方案，敏捷产品始终引领数据安全新趋势，已服务涵盖工业互联网、智能制造、关键基础设施、党政机关等领域上万家知名用户。敏捷科技结合工信部 451 号文、《中国制造 2025》等一系列相关政策和中车株所系统安全防护的具体要求，制定针对性的项目技术路线。

一、项目概况

中车株洲电力机车研究所有限公司（中车株所）始创于 1959 年，前身是铁道部株洲电力机车研究所，现为中国中车股份有限公司一级全资子公司。2016 年，公司销售收入达到 320 亿元，位列湖南企业前 15 强，株洲市第一。中车株所具备强大的自主研发与创新能力，已构建完成在轨道交通装备牵引传动与控制系统

领域的自主创新研发平台，是中国轨道交通电气系统集成解决方案的首选供应商。

在向互联化、智能制造方向发展的过程中，轨道交通产业链重构转型，利益共享、风险同担。轨道交通整车与零部件厂商协作关系越来越趋向合作竞争，在产业链发挥各自的优势；客户多样化需求促使整车制造商与模块供应商在开发、制造、服务方面的紧密合作。产业生态系统互联意味着数据的互通，数据的互通也加剧了泄露风险。近两年，全球针对制造业的数据泄露事件多达 2000 余起。为助力中国制造 2025，提升自身的信息安全水平、促进信息安全技术创新，中车株所决定依托敏捷科技在企业内部建立具有中车株所特色的工业数据智能安全云平台。

1. 项目背景

中车株所具备强大的自主研发与创新能力，从设计到生产制造、检验检测以及交付、运营，努力实现全数字化驱动。“十二五”期间，中车株洲所通过开展产品研发设计数字化工作，各新产品设计周期普遍缩短了约 30%，工程更改减少了约 20%，研发成本降低了约 10%，大大提高了企业技术创新的水平和能力。中车株所产线通过信息化和自动化手段升级，从人、机、料、法、环、测的维度进行全面质量管理，促进基础管理与技术的提升和优化，实现生产过程和生产管理的智能化。

中车株所目前已经建成涵盖轨道交通及工业领域大数据存储管理与分析挖掘业务，可支持海量工业设备数据接入的大数据平台，实现了打通设计、制造、物流、售后、质量等各个领域的关键数据，并形成闭环，产生服务价值。然而，轨道交通行业的特点是资产密集、长周期运营，而且信息非常分散，这就导致它对产品的质量和安全方面要求比较高。中车株所在追求企业转型升级的同时，对工控系统安全的认识达到了一个新的高度。积极推进企业级系统集成，实现生产和经营的无缝集成和上下游企业间的信息共享，开展基于横向价值网络的协同创新，在企业间的设计协同、制造协同方面逐步由原来的纸质信息传递，转变为以

三维设计模型为核心的电子文件交换，带来了便利的同时，也带来了商业秘密泄露、图纸数据随意篡改、电子文件残留等数据安全风险，需要搭建一套轨道交通行业数据安全云平台。

敏捷科技充分结合中车株所轨道交通工业互联网系统的实际情况，有针对性的制定具体解决方案：

（1）构建轨道交通行业面向工业设计数据全生命周期安全管理的解决方案，为企业间的高效协同提供一个安全平台。

（2）全面构筑轨道交通行业工业数据智能安全云平台，确保工业设计环境中上下游企业在高效协同的同时，减少数据泄露风险，确保轨道交通行业向数字化、智能化、绿色化安全转型升级。

（3）确保云平台上各项云应用数据全生命周期的安全可控。

2. 项目简介

本项目借助敏捷科技核心专利技术，基于我国密码标准算法构建。通过终端数据智能安全防护、网络数据安全防护、因公外出数据、云平台数据安全管控防护等数据防护作用，确保中车株所工业设计环境中上下游企业在高效协同的同时，防止商业秘密数据外泄、防止数据恶意篡改、减少图纸数据大范围分发的数据残留风险。

3. 项目目标

1、提高中车株所工业互联网系统信息安全防护能力和高效协同管理水平。

对系统敏感数据进行智能识别、分级加密、权限管控，全方位提高自身信息安全管控能力，有效解决中车株所内部合法用户有意或者无意的信息泄漏。

2、满足合规性要求

满足工信部《工业控制系统信息安全行动计划（2018-2020 年）》及相关指南要求，落实工控系统常态化检查评估、风险通报、事件应急等工作，同时加强工控系统使用人员的安全意识及技能培训。

3、数字中车战略目标的契合

集团先后对各子公司开展了安全性评价标准查评，并与敏捷科技合作，对系统进行数据防泄漏体系建设工作。

二、项目实施概况

本项目在工业互联网体系架构的基础上应用了基于工业控制系统的防护手段，针对工业设计数据面临的威胁，借助敏捷科技核心专利技术“电子文件安全标签”、“高速高通云存储加密技术”，基于我国密码标准算法构建，通过阅后即焚、安全云盘、数字签名、透明加密等功能，构建了面向工业设计数据全生命周期安全管理的解决方案，确保中车株所智能制造数据集中管控的同时实现安全可靠管理，有效保护中车株所的核心资产、知识产权及其它相关数据。

1. 项目总体架构和主要内容

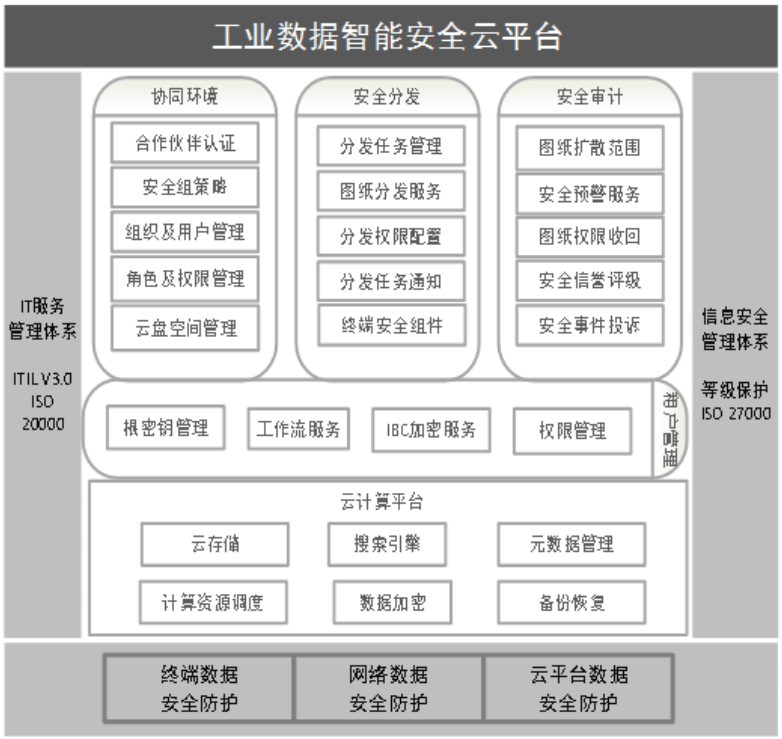

图 1　总体架构图

（1）终端数据智能安全防护：包括数据智能安全子系统、终端虚拟化桌面子系统、终端桌面安全子系统、终端外设控制子系统、文件透明加密子系统等五个子系统，有效防止机密信息泄漏。

（2）网络数据安全防护：提供虚拟安全网络子系统，确保具体业务应用系统环境的专用性和“干净性”，实现了基于具体业务应用系统的动态“专网专用”，也从安全管理角度上对网络数据进行安全精细化管理。

（3）平台数据及因公外出数据使用安全管控防护：实现对移动设备在外使用过程中全程保护，有效的杜绝外出人员主动和被动的数据泄密，实现了外出移动设备的授权使用、安全认证和电子文件的便捷高效、安全可用。

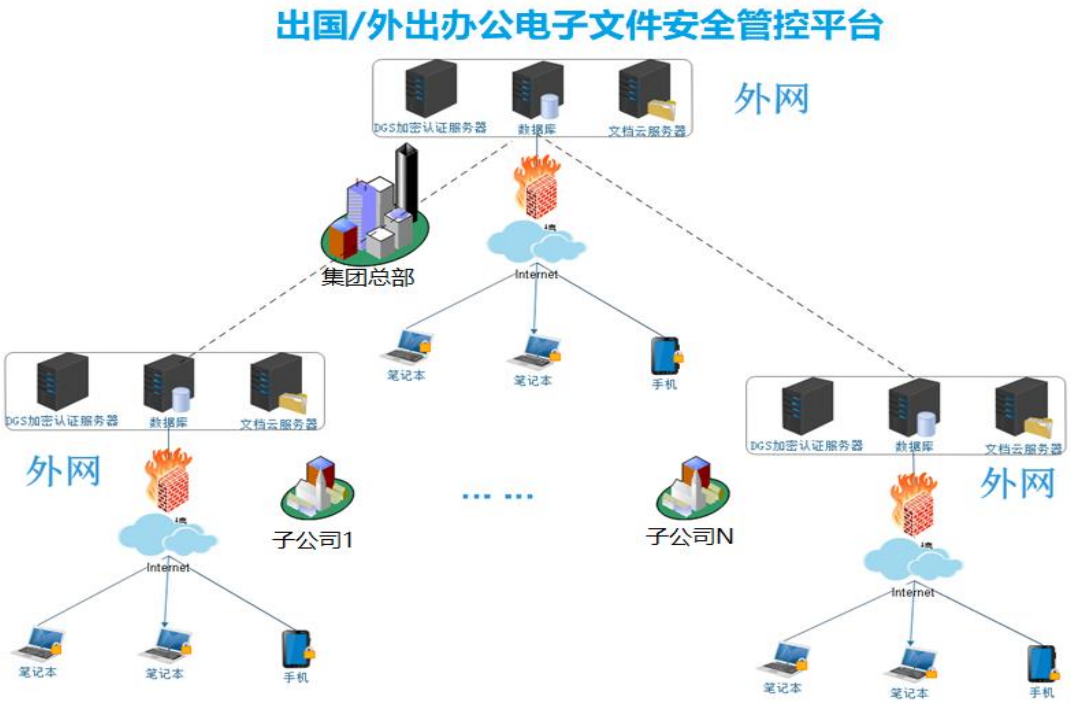

图 2　电子文件外出使用安全管控系统拓扑图

2. 应用场景

针对工业设计数据面临的三大威胁，工业数据智能安全云平台构建了面向工业设计数据全生命周期安全管理的解决方案，包括工业**图纸协同研发设计环节**的安全可控，**及图纸下单给外协方的电子商务结算环节、**出图进行资源调配确定**生产计划环节**，直至下发至智能车间**生产环节**，及后续产品发布环节的图纸安全控制问题。

图 3 安全协同设计图

随着市场竞争的日趋激烈和中车株所信息化的发展，跨专业、跨地域的基于网络化协同设计极大地缩短产品设计和研发周期，快速研发出适应市场变化和需求的产品，提高企业的竞争能力。项目所在的上下游企业通过商务往来沟通项目设计需求调研，并进行项目可行性分析，在确认项目可行后设计人员进行样本设计，并分发给上下游企业进行图纸校验，校验无误后进行试制、定型。从需求、可研、设计、试制、定型的全过程会产生一系列数据，这些数据在项目各环节经多个上下游企业流转，中车株所工业数据智能安全云平台确保协同设计过程中数据从产生、流转、存储和利用都处于安全管控之下，确保协同设计数据全生命周期的安全无泄漏。

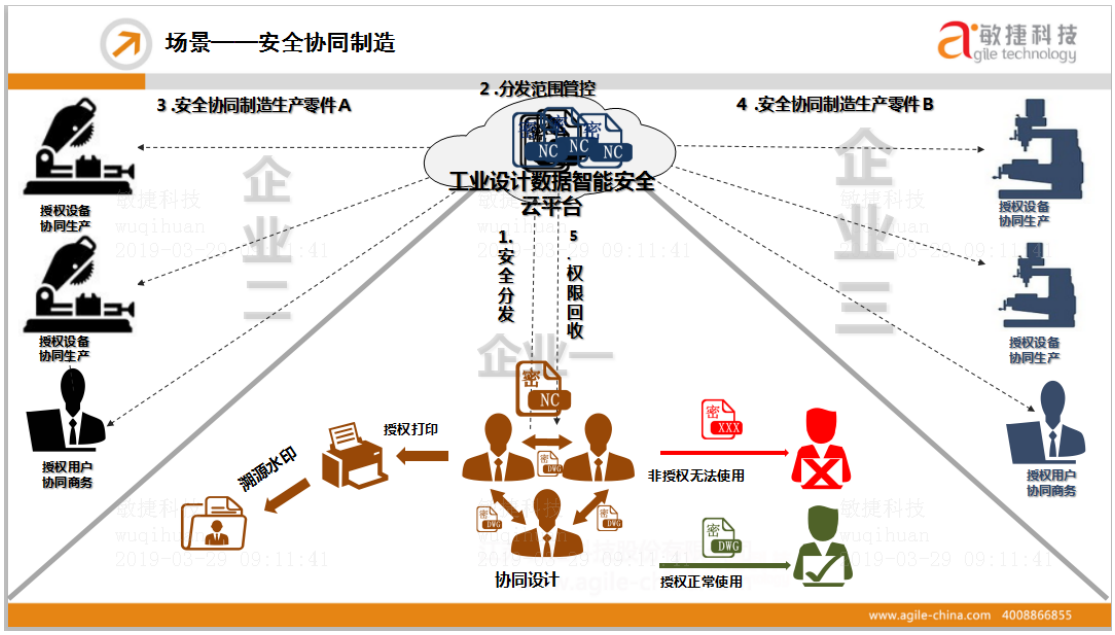

图 4 安全协同制造图

通过协同制造，中车株所各上下游企业间可以进行生产进度信息的高度、实时共享，实现其透明化。同时，项目相关企业的生产过程数据信息在网络协同制造链中顺畅流动，可以大大提升智能制造的效率。设计部门将设计图纸通过工业数据智能安全云平台安全分发给各协同制造生产零件企业进行生产制作，给外协企业的机密文件进行授权，非授权人员无法使用文件，授权时可设置时间、次数，不同的外协企业获取文件后必须通过各自特定的外发浏览插件打开外发文件，而且文件受到严格的权限控制，阻止了文件从外协企业泄密。

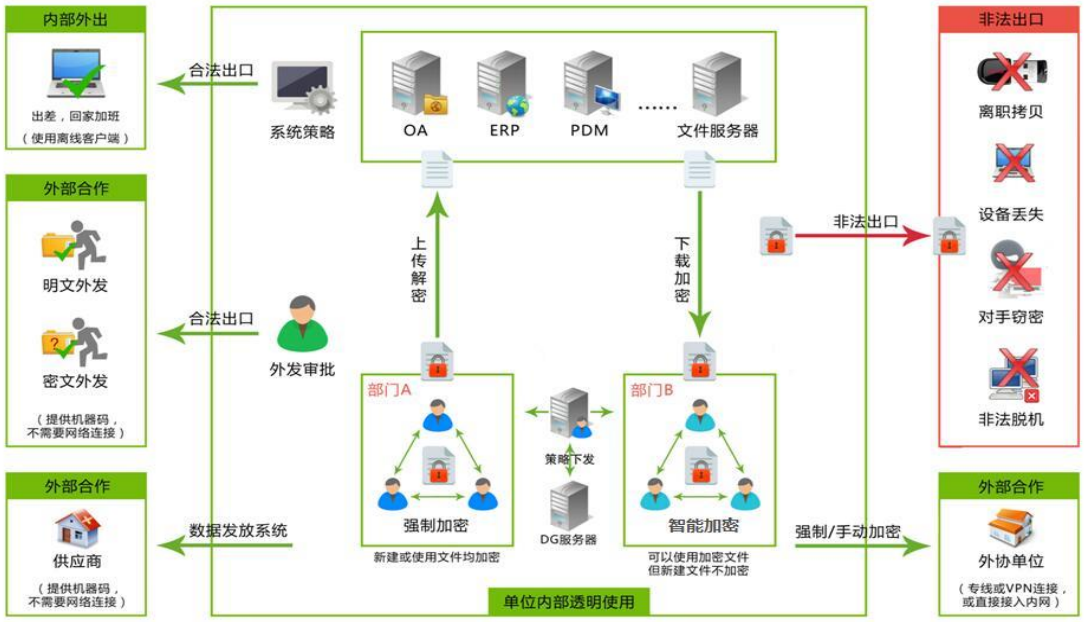

图 5 智能防泄漏应用场景

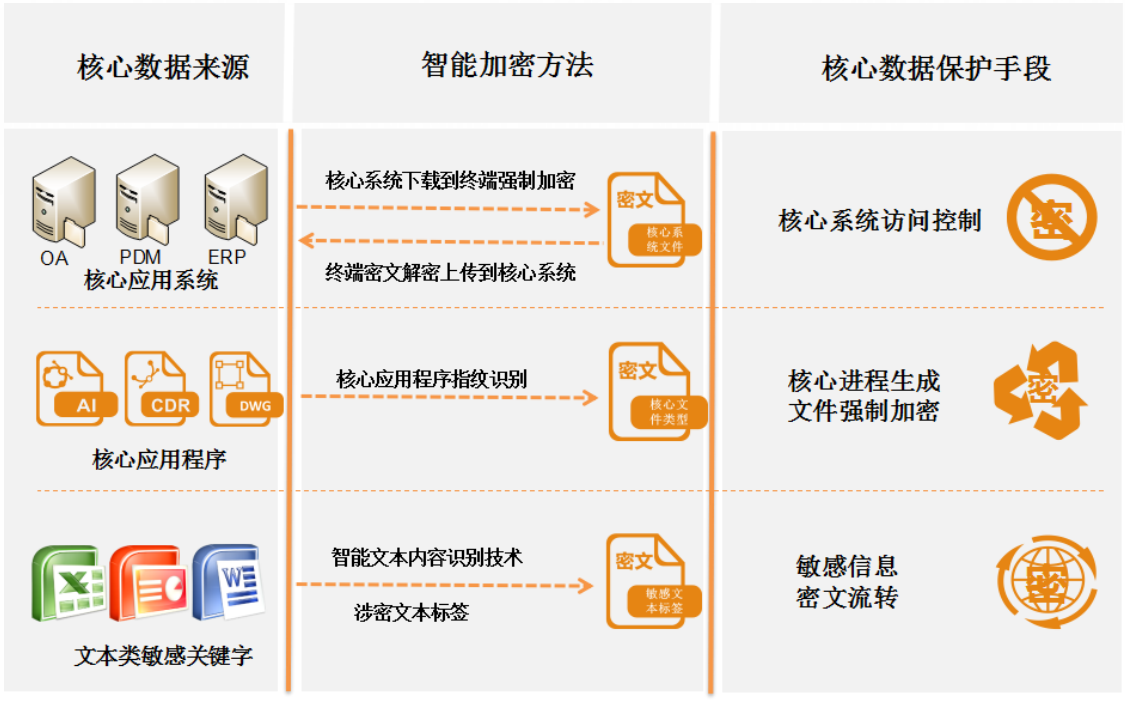

图 6 核心数据强制加密保护模式

图 7 终端数据智能防泄漏保护模式

图 8 多种系统集成模式

3.安全及可靠性

敏捷科技在数据管理及数据安全方面已经有十余年的开发经验，并积累了大量的客户案例与客户需求。本项目的研究试验将依据敏捷科技现有的大量客户基础和客户需求，采取自主创新开发模式开展。

（1）首先，我们将通过调查国内若干典型企业，充分了解企业对系统的需求。总结已有的研究成果，吸取新的技术及新的需求，保证有一个高的技术起点而不是从零开始。

（2）其次，我们将参照有关的技术标准规范，跟踪技术最新的发展方向，为用户提供一个先进的、可扩展的、开放的数据安全平台。

（3）此外，在软件的开发方面我们将实施严格的软件工程管理，组织多家用户实施及测试，确保产品的质量。

（4）最后，我们将真正实行切实的产业化运行机制及可持续发展的技术支持。

项目所采用的内核级主动加密、应用软件指纹识别的加密槽等技术通过科技成果鉴定属国内外首创，填补了智能制造安全领域的技术空白，弥补高端和前沿研究开发方面的不足。

三、下一步实施计划

1. 加大工业互联网安全技术研发力度

大力开展工业数据安全前沿技术的攻关工作，研发自主可控且满足工业互联网特点的专用数据安全防护工具，提升工业设计协同平台数据分析能力，实现全方位感知工业数据安全态势。

2. 建立纵深防御机制

按照“双网双机、分区分域、等级防护、多层防御”的指导方针，建立健全企业信息安全纵深防御体系，防止信息网络瘫痪、防止应用系统破坏、防止业务数据丢失等，以确保信息系统安全稳定运行，确保业务数据安全。

四、项目创新点和实施效果

1. 项目先进性及创新点

（1）创新关键技术

- 数据加密技术、数据传输安全和身份认证管理。
- 数据挖掘技术、分布式索引检索技术。
- 移动办公、嵌入式技术。

（2）可以生产全系列的工业互联网数据安全产品

- 提供全系列工业互联网数据安全产品，可以满足不同工业设计系统信息安全防护项目的需要。
- 工业互联网数据安全产品覆盖了整个生产监控系统的核心部分。

（3）满足高性能要求的数据集中管控平台技术

- 提升了现有 PC 的使用效率，实现了 IT 部门对分散的 PC 的集中式管理。
- 增加了高度安全性和灵活性。
- 使用习惯的无需改变、PC 应用的无缝兼容、个性化桌面应用的灵活调用。

（4）持续的先进技术支持

- 针对云计算环境下非结构化数据与结构化数据的透明加密处理。
- 基于分区分域分级设计的云安全运维与安全管理。

2. 实施效果

敏捷科技工业数据智能安全云平台在中车株所上线应用以来，实现了企业内部及产业上下游、跨领域生产设备与信息系统的互联互通、资源共享、数据集成安全共享，提高了企业数据安全防御能力，推动株洲的轨道交通产业，企业与企业之间、企业与政府之间的良性互动，为促进全国工业互联网行业持续健康发展提供有力支撑。