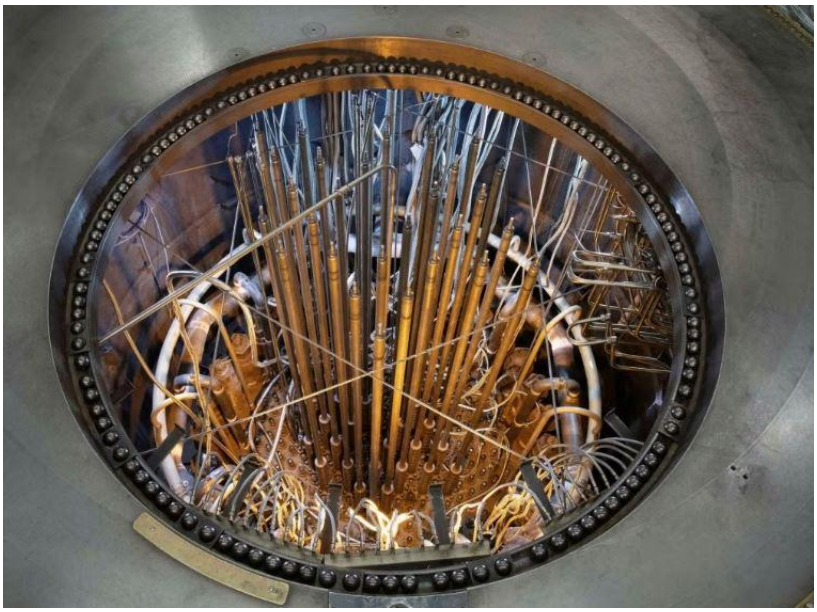
# 区块链——解决数据造假的新手段

福岛核灾难带来的深刻创伤，促使日本高度重视核安全。然而近期曝出一桩丑闻：为加快政府审查进度，滨冈核电站官员篡改并伪造了地质构造安全数据。该核电站及其营运单位中部电力公司，刻意挑选对其有利的地质构造数据作为安全测试的依据，从而得出了几乎完全伪造的结论。

日本原子力规制委员会（NRA）对此予以强烈的谴责，并提议对中部电力旗下所有核电站的整套安全数据进行全面审查。

这并非核安全领域首起数据篡改案例。2012 年，韩国水电核电公司（KHNP）发现，其五座核电站中有 7682 个依据伪造测试报告供应的反应堆安全和冷却系统部件——涉及近 2114 项测试，占供应链中全部设备测试的 0.7%。这些部件如若在关键时刻失效，可能会酿成灾难。

更近期的例子是挪威的哈尔登（Halden）反应堆（已于 2018 年关闭），该反应堆被发现在多次实验中进行了有组织性的、且极难被发现的数据篡改。这座实验堆曾向全球众多反应堆提供信息和数据，这些伪造的结果很可能在世界范围内产生连锁影响。



哈尔登反应堆项目自 1958 年起在挪威能源技术研究所运行，但被发现多次篡改数据（图片来源：OECD）

伪造、篡改或编造数据事件，除了可能给公共安全带来灾难性后果外，还会严重损害核能领域的公众信任，许多国家和地区对核技术本就持谨慎态度。此类丑闻还将产生重大的商业和监管影响，进而损害整个行业。若不采取明确切实的步骤加强信息安全性，核能行业将面临反复踏入信息陷阱的风险。

**为何数据验证至关重要**

上述公然篡改数据的事件仍然相当罕见——但其共同点在于：绝大多数事件本可以通过统一的数据验证标准来预防。

在验证数字数据时，需要确认以下四点：

- 真实性：文件是否真实？是否经由相应的授权机构采

用相应程序认证和批准？

- 来源：谁在何时创建了它？最终文件的时间印章是否与其原始创建时间相符？
- 完整性：文件是否曾被修改？如果在某个时间点被认证为正确，此后是否发生过变更？
- 保管链：文件是否曾易手或被第三方改动？接收时的文件与发送时的文件是否一致？

确保所有要素对于重要文件的安全至关重要。如果缺乏可靠验证全部四项要素的方法，将面临多重问题。首当其冲的是无意的、偶然的更改。例如，在检查文件过程中不小心删掉一个“0”，这是常见的人为失误。随着 AI 越来越多地应用于大型数据集的检查，此类错误引发的影响可能会被放大。

其次，数据的无法验证使文件更容易被故意篡改，这一点也恰恰被核领域一些颇受关注的案件所印证。通过对变更、保管链、来源进行严格的全程追溯，监管机构、管理层及其他利益相关方就能更容易识别出问题乃至欺诈行为发生的环节。在大多数案件中，欺诈行为通常都是在多年后才被揭露，而且往往是由外部团体和举报者曝光——这也凸显了发现问题的难度。

第三，数据管控和完整性方面的薄弱标准为攻击网络安全敞开了大门，内部数据被细微篡改——这是监管机构多年

来一直担忧的威胁。

在对安全至关重要的核能领域，尤其是在不同的司法管辖区之间，显然缺乏统一的、公认的、有关数据完整性的标准。不同国家在数据领域的法规标准各不相同，但这些法规通常只规定了计算机的正确设置，而忽略了数据本身的验证和完整性。

在全球化趋势加速演进、AI 赋能的伪造工具层出不穷的今天，数据防伪已成为一个可能对整个行业产生广泛影响的紧迫问题。

**行业应如何应对**

在这些数据丑闻风波之后，愈发清晰的是，缺乏统一且广受认可的数据验证标准，正成为一个日益凸显的漏洞。为扭转这一局面，应该采用那些不仅满足上述四要素面、还能在不同司法管辖区间进行独立验证的可靠技术。

区块链就是这样一种技术。曾主要用于加密货币，但其作为可公开访问、安全且私密的信息与交易账本的本质，赋予其在验证数据完整性方面具有显著优势。该技术无需将敏感信息放在公开账本上——一种称为哈希值的、具有固定长度的唯一字母数字字符串可作为数据的数字指纹，并且可以使用市场上已有的工具进行独立验证。这就创建了一条有效且不可篡改的审计轨迹。此外，这些标准可以跨国家、跨机构使用，从而成为消除司法管辖区差异的更佳方式。

基于区块链的数据完整性标准意味着监管机构、组织和管理者可以更轻松地识别数据完整性问题。这样的系统还可以对数据篡改做出更快速、更灵活的响应，对妄图进行数据造假的行为形成强大的威慑。

无论最终采用哪种技术，毋庸置疑的是，如果此类丑闻持续发生，核能行业将面临致命的信誉危机。如果缺乏万无一失的方法来保障对数据篡改行为的迅速识别，不仅公共安全会受到威胁，整个行业的安全也将岌岌可危。核工业亟需制定一个可全面推广、论证的数据验证标准。

对外合作部 李安琪 供稿

编译自国际核工程官网

文章内容不代表本公众号观点