以“零事故”为目标，筑牢智慧水利网络安全底板

齐向东
（奇安信科技集团股份有限公司，北京 100037）

摘要：随着数字化转型加快推进，智慧水利亟需以“零事故”为目标，打造工业互联网边缘可信防护系统、数据安全系统和态势感知系统，建立与智慧水利发展相协调的全面、系统、智能的网络安全体系。在网络安全事件发生时，运营单位能快速采取相应措施，使其不对业务、资产、生产等造成影响。

关键词：水利工程；网络安全；零事故
中图分类号：TV213.4 **文献标识码：**B **文章编号：**1007-7839(2022)Sup2-0011-03

Aiming at “zero incidents”, build a solid network security system for smart water conservancy

QI Xiangdong
(*QI-ANXIN Technology Group Inc., Beijing* 100037, *China*)

Abstract: With the acceleration of digital transformation, smart water conservancy urgently needs to aim at “zero incidents”, build an industrial internet edge trusted protection system, data security system and situational awareness system and establish a comprehensive, systematic and intelligent system which is coordinated with the development of smart water conservancy. When a network security incident occurs, the operating unit can quickly take corresponding measures to prevent it from affecting business, assets and production activities.

Key words: water conservancy projects; network security; zero incidents

1 新挑战，智慧水利的网络安全存在2个突出短板

水利工程是国民经济关键基础设施的重要组成部分，数字化转型是维护水安全、保障水资源可持续利用的重要工具。近年来，水利行业贯彻网络强国、数字中国的总体部署，牢牢把握“水利工程补短板、水利行业强监管”这一重点任务，加速开展全面数字化转型，不断推进智慧水利建设。随着新一代信息技术在水利系统得到广泛应用，水利工程建设与管理的数字化、网络化、智能化水平得到不断提升。

新机遇伴随新挑战，水利网络面临的最大挑战就是网络安全威胁。虽然水利信息化建设取得积

收稿日期：2022-11-07
作者简介：齐向东(1964—)，男，教授级高级工程师，硕士，主要从事网络安全领域的研究工作。

极成效，但是网络安全防护能力偏弱，与信息化水平不同步。从整体上看，我国水利网络安全基础较差，防护水平低，没有进行系统性顶层设计规划，尚未形成完整的安全防护体系。当前，水利网络面临2个较为突出的安全短板：工业控制系统网络安全和数据安全。

1.1 工业控制系统网络安全

工业控制系统网络安全是确保水利设施平稳运行的命脉。工业控制系统（PLC，SCADA等）是水利设施的重要组成部分，广泛应用于闸站控制、库坝监测、水网调度、水资源监测等业务场景，是水利网络运行的核心控制系统。目前，我国工业控制系统普遍存在资产盘不清、防护不精准、响应不及时等问题。同时，这些控制系统多数采用西门子、施耐德等国外厂商设备，近年来被披露存在大量中高危漏洞，极易遭到木马病毒和黑客的攻击，给水利网络安全运行带来极大的威胁。

1.2 数据安全

数据安全是推动智慧水利高质量发展的基础。数字时代，数据成为关键“燃料”，为经济社会发展增值赋能。但同时，针对关键基础设施数字化系统的攻击愈演愈烈，数据资产也成为被勒索攻击的头号目标。水利行业积累了海量基础数据，每天产生大量新数据，这些数据为水资源利用、水环境监测和水利工程建设提供了重要支撑，是建设智慧水利的宝贵资源。但正是由于水利行业拥有的数据量大、价值高，无法承受运营中断所带来的“蝴蝶效应”，因此成为了勒索组织眼中的“香饽饽”。同时，我国的水利数据中相当一部分仍然处于“裸奔”状态，数据的生产、采集、使用和流转都缺乏基本的安全防护，数据安全防线处于不攻自破的状态。

网络安全与数字化转型是一体双翼。让网络安全始终渗透在整个水利体系之中，是大势所趋和必然要求。面对如此严峻的安全形势，水利行业加强网络安全建设已经迫在眉睫。

2 新目标，智慧水利网络安全亟需向“零事故”进发

过去，人们谈到网络安全，常处在一种高压状态下，不敢以“零事故”为目标。网络安全攻防相长，没有攻不破的网络，没有打不透的墙，漏洞是补不完的。在这样的现状下，很多单位进行网络安全建设时，只针对出现过的安全事故采用相应的防护技术和产品。但是过去没有发生，不代表未来不会发生，这种网络安全建设思路会带来极大的安全隐患。

2022年3月，奇安信科技集团股份有限公司（以下简称奇安信）圆满完成北京冬奥网络安全保障任务，充分证明网络安全“零事故”是可以实现的目标。作为奥运史上首个独家网络安全官方服务商，奇安信创造了奥运史上网络安全“零事故”的世界纪录，不仅证明了“零事故”可以实现，更证明了，只有以“零事故”为目标，努力穷尽所有可能发生的风险，并一一进行防护，才能确保网络安全万无一失。“零事故”不是零攻破。在网络安全事件发生时，只要能快速采取相应措施，使其不对业务、资产、生产等造成影响，还可以称之为“零事故”。网络安全“零事故”具体有以下3条标准：

2.1 业务不中断，确保水利设施平稳运行

保障各类闸站控制与监测业务不因网络攻击中断，是水利网络安全防护的基本目标。数字时代，业务系统走向开放互联。攻击者通过业务系统的一个弱点，能够打击一片。水利的重要网络设施、信息系统是关键信息基础设施，一旦发生业务中断，轻则会造成营业收入、口碑受损，重则触犯法律，直接威胁社会生产生活和国家安全。2022年8月，英国某水厂疑似遭到勒索攻击，IT系统被迫中断服务；2021年2月，黑客入侵美国一家水厂，通过更改氢氧化钠浓度，给自来水“投毒”，差点酿成悲剧。

2.2 数据不出事，拧紧水利数据“安全阀”

数字时代，数据是关键生产要素，它穿行社会各个领域，为数字经济发展提供动力。收集好、利用好、储存好水利数据，对发展水利事业，确保国家长治久安意义重大。在运营者手中，水利数据可以用来有效进行河流监管、防洪救灾、水资源调度。但水利数据一旦被丢失、被篡改、被抹除、被勒索，或落入有心人手中，后果不堪设想。2022年6月，印度地方洪水监测系统遭到勒索攻击，由于没有及时更新防火墙，安装杀毒软件，攻击者轻易得手，全部水文数据均被加密并且无法备份，对印度水利行业造成重创。

2.3 合规不踩线，助力水利运营主体行稳致远

长期以来，很多人都有一个误解，认为合规是网络安全工作的目标，事实上，合规是网络安全的基本要求和底线。企业不遵守网络安全规范，就像没有打牢地基，注定无法长久。近年来，《网络安全

法》《网络安全等级保护条例》《关键信息基础设施安全保护条例》等相继颁布实施，为各行各业的网络安全建设提供了根本遵循。2017年，党中央发布《党委（党组）网络安全工作责任制实施办法》，网络安全工作一把手责任制进一步得到强化。水利行业作为农业命脉、生态安全源头、改善民生的关键，如果忽视网络安全规范，抱有侥幸心理，会为运营者、行业、国家带来严重后果。

3　新举措，坚决夯实智慧水利的网络安全底板

水利行业应该严格遵循网络安全“零事故”的3条衡量标准，开展周全的网络安全建设，建立与智慧水利发展相协调的全面、系统、智能的智慧水利网络安全体系。

3.1　打造工业互联网边缘可信防护系统

水利行业的规模和场景决定了工控系统的信息接入点数量庞大、分布广泛，设备管控难度大，在网络边缘埋下了巨大的安全隐患。不法分子很容易利用终端网络接口进行仿冒接入，并对内网进行探测入侵，进而控制核心业务系统。

工业互联网边缘可信防护系统通过常用接入控制技术，对网络中的各类IP流量、工控流量进行解析与控制，评估其合规情况，对非法流量强制进行网络阻断，以实现对控制系统的安全防护。而且控制器会旁路部署于核心交换或汇聚交换处，借助镜像流量对管控区块内设备通过边界的行为进行识别以及合规管控。在旁路部署模式下，不会改变客户原有的网络拓扑和使用习惯，即使接入控制器宕机也不会对客户网络造成中断，有效保证了业务的连续性。

3.2　打造数据安全系统

随着水利行业的数据总量急剧攀升和数据价值提升，数据集中化不断深入推进，大数据平台、大数据中心建设热火朝天。水利部印发的《关于推进水利大数据发展的指导意见》，明确强调水利行业要推进数据资源共享开放。但是，数据在大集中的同时，也将导致风险大集中，很容易引发数据泄露、数据滥用。一旦大数据中心受到安全威胁，将波及企业分支机构、营业网点，甚至导致业务停摆、客户重要数据丢失。

水利网络亟需建立完整的数据安全系统，从特权账号管理、数据防泄漏、数据态势感知、API安全监测、数据库审计等多个层面，构筑多层次、无死角的综合防御体系，确保一切操作行为可追踪、可溯源。另外，还要打造数据流通安全系统，基于“数据不动程序动、数据可用不可见”的理念，不分享原始数据，只分享数据的价值，确保数据所有权和使用权分离，从而解决隐私保护和数据挖掘之间的矛盾，让数据价值最大化。

3.3　打造态势感知系统

受制于水利网络的庞大规模和复杂应用场景，水利行业在面对网络安全威胁时，往往拿不出行之有效的应对措施。从整体来看，行业普遍缺乏多维度风险感知能力，很难全面掌握威胁，导致风险感知不及时、响应不及时，甚至安全事件已经发生了还不知情。因此，水利行业可以在业务内网、水利专网和大数据中心建立三级的态势感知体系，实现监管、运营和攻防态势感知“三合一”。比如让第一级的态势感知对全面的流量数据进行分析，发现异常行为，形成告警；告警汇集到第二级态势感知后，安全运营人员根据这些流量告警信息进行研判分析，做出响应处置，形成安全事件；安全事件到达第三级的态势感知后，结合上级掌握的更全局的数据，做出决策，下达指令，协同多方进行处置，实现无缝衔接。