
Water Utilities Series

PSTN Switch-Off, 3G Retirement, 2G Sunset, and Water Utilities

Protecting pumping stations, alarms, and remote access
through every network transition

Version:

2.0

Date:

March 2026

The Converging Risk

Consider a pumping station connected to the PSTN by a single analogue line. That line carries the autodialler that alerts the control room to faults, the dial-up link for SCADA polling, and the telemetry feed that confirms the site is operating normally. When the line is quietly disconnected during the PSTN switch-off, all three go silent simultaneously. The first indication of a problem is a pollution incident downstream. This is not a theoretical scenario; it is the specific risk that PSTN cessation creates at thousands of remote, unmanned water sites across the United Kingdom.

The risk does not end with PSTN. Vodafone, EE, and Three have completed their 3G network retirements^{19,20,21}; Virgin Media O2 is completing its shutdown in early 2026 and has already ceased inbound roaming, making its 2G and 3G network unavailable to multi-network IoT SIMs¹⁸. 2G sunset programmes are confirmed, with EE beginning from May 2029¹⁶ and Vodafone during 2030¹⁷. For water utilities that deployed cellular connectivity as a PSTN replacement on a single-network basis, a 2G-only device now faces a second forced migration. PSTN cessation, 3G retirement, and 2G switch-off are converging risks that demand a connectivity strategy resilient to all three.

The migration from PSTN to IP-based and cellular connectivity also introduces new considerations around network security and segmentation. Analogue lines were inherently isolated; they carried a single function and were not addressable from the public internet. Replacing them with IP-connected devices at remote, unmanned sites means that operational technology (OT) networks, including SCADA, alarm telemetry, and process control, must be properly segmented and secured from the outset.

This guide is therefore intended for water utility operations, asset management, IT/OT security, and compliance teams responsible for planning the migration from PSTN and managing the impact of 3G retirement and 2G sunset on remote site connectivity.



Recommended actions: 30 / 60 / 90 day priorities

First 30 days: Complete a PSTN and cellular dependency audit. Identify every analogue line, the device it serves, and the site's criticality rating. Include any existing 2G-only cellular devices. Assess the current OT security posture at each site.

Days 30–60: Prioritise flood-critical and compliance-critical sites. Confirm cellular coverage across multiple operators, assess power resilience requirements, and begin procurement processes for proven replacements, such as CSL DualCore routers, DualCore Resilient SIM (rSIM®); and VoiceLink. Define network segmentation and firewall policies for OT traffic.

Days 60–90: Commence phased installation at priority sites. Test alarm escalation, remote access, and OT network segmentation under realistic conditions, including power-loss and single-network-failure scenarios.

Planning window

A typical water utility migration, covering site surveys, procurement, installation, and commissioning, can take 9–12 months across a large estate. With the January 2027 PSTN deadline approaching¹⁵ and 2G sunset confirmed for 2029–2030, utilities that have not commenced planning are operating within a compressed timeline.

PSTN incidents are already rising

UK Government (DSIT) guidance notes over 2,600 major PSTN incidents in 2024/25, including exchange failures affecting alarm and telemetry systems³. Ofcom's Connected Nations 2024 report recorded a 45% increase in significant PSTN resilience incidents⁴. The national WLR stop sell is in effect; full withdrawal is set for 31 January 2027^{1,2}.



Which Assets Are at Risk?

PSTN dependencies persist in locations that are operationally critical but geographically remote. The same sites may also rely on legacy cellular devices now vulnerable to 2G sunset.

Asset type	PSTN dependency	Consequence	Replacement
Pumping stations	Alarm panels, SCADA dial-up, autodiallers	Faults undetected; pollution	CSL DualCore router + VoiceLink; rSIM® in third-party devices
Treatment works	Process monitoring, alarms, voice	Delayed response; compliance	CSL DualCore router + VoiceLink
Storm overflows	Level sensors, EDMs, alarms	Missing EDM data; non-compliance	CSL DualCore router; rSIM® in third-party monitors
Ancillary sites	Single-line PSTN	Silent site; no visibility	CSL DualCore router or VoiceLink

⚠ Power Resilience Checklist: Flood-Critical Sites

PSTN lines typically provided line power for basic telephony. Cellular routers and IP voice devices require local power. Every migration must address power resilience at the site level.

- ✓ **CSL DualCore Router:** battery/UPS backup to maintain alarms and SCADA during mains failure
- ✓ **CSL VoiceLink:** built-in 8-hour battery for voice continuity during power interruptions
- ✓ **Site UPS / battery cabinet:** sized for minimum hold-up time per site risk classification
- ✓ **Test under power-loss conditions:** verify alarm escalation, remote access, and failover during mains outage

Regulatory Obligations Driving Connectivity

Section 82 of the Environment Act 2021 introduces Continuous Water Quality Monitoring (CWQM) duties around storm overflows and sewage disposal works, requiring upstream and downstream measurement of parameters including dissolved oxygen, pH, turbidity, and ammonia at specified intervals^{12,13}.

Separately, **Defra's** Storm Overflows Discharge Reduction Plan requires Event Duration Monitoring (EDM) data, specifically discharge frequency and duration, to be published in near real time from January 2025¹¹. Both obligations depend on uninterrupted connectivity and power resilience at remote monitoring sites.

Why connectivity matters for compliance

CWQM sensors transmit at regular intervals determined by regulatory and operational requirements. EDM monitors must report discharge events in near real time. If the cellular connection to a storm overflow or sewage works fails, the utility loses both the data and the ability to demonstrate compliance. The regulatory consequence extends beyond a simple data gap. Loss of connectivity creates an evidential shortfall that can be difficult to defend during assurance reviews, incident investigations, and regulatory scrutiny.



Sector-Wide Enforcement: The Regulatory Direction

Regulators are increasingly linking equipment and monitoring failures at remote sites to enforcement outcomes. When connectivity to an unmanned site is lost, routine faults escalate into pollution incidents, and those incidents attract regulatory consequences.

Pumping station and equipment failures

Recent prosecution cases across the UK water sector demonstrate that a single equipment fault at a remote pumping station or wastewater works can result in significant fines when detection is delayed and sewage discharges into watercourses. Fines for individual incidents can be substantial, and escalate further where detection delays are shown to have worsened the environmental impact.

Systemic monitoring gaps attract systemic penalties

Ofwat has pursued enforcement action with substantial penalty values where systemic wastewater management failings have been identified. The regulatory direction is clear: gaps in monitoring and telemetry across an estate are treated as systemic issues, not isolated incidents, and penalties are scaled accordingly.

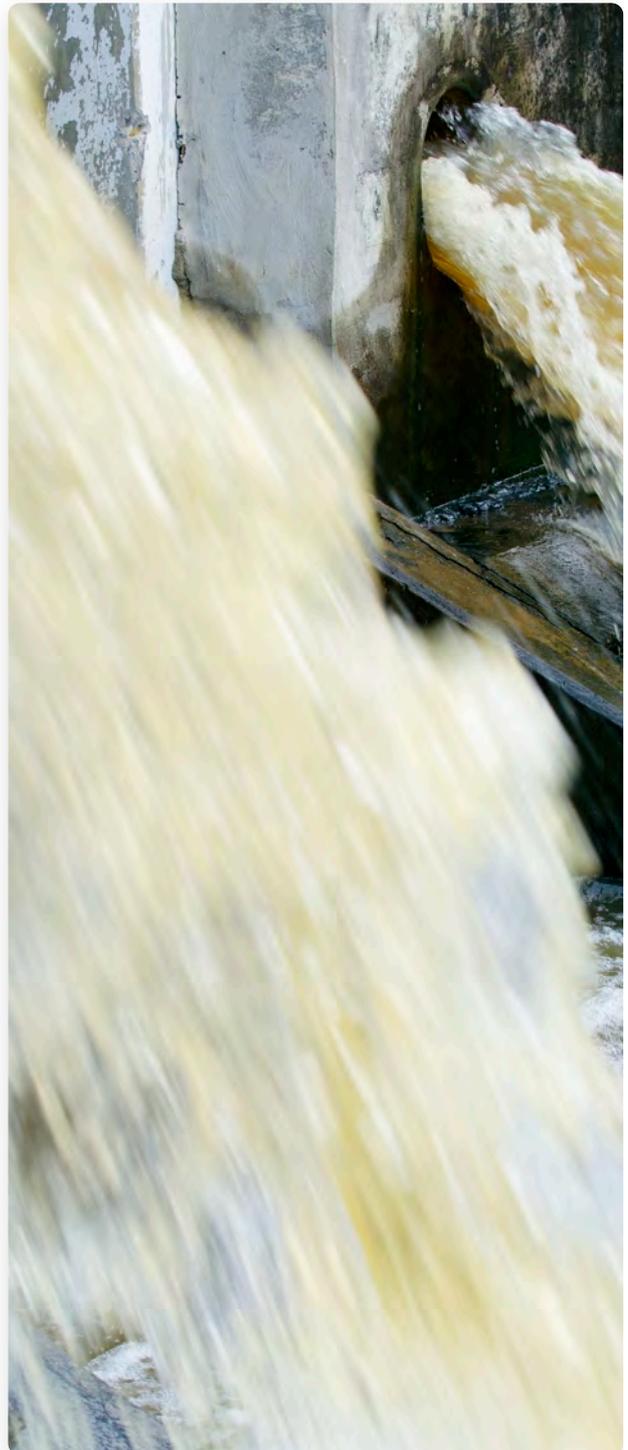
Repeated incidents at the same site type

Enforcement records show that the same types of site, particularly wastewater pumping stations and treatment works, appear repeatedly in prosecution cases over successive years. This pattern illustrates how the underlying risk persists until the monitoring infrastructure itself is upgraded. Replacing the connectivity layer is not optional maintenance; it is a precondition for breaking the cycle of repeated incidents.

The common precondition across these cases, delayed detection of a fault at a remote, unmanned site, is the precise scenario that PSTN cessation and 2G sunset make more probable across every water utility estate.

The enforcement trend is accelerating

Ofwat has signalled a tougher approach to water company enforcement, with penalty values reflecting the scale of systemic failings. Equipment failures at remote, unmanned sites are a recurring factor in prosecution cases. Utilities that can demonstrate continuous monitoring and resilient connectivity are better positioned to defend against enforcement action.



Cellular Connectivity Solutions After PSTN

Addressing the converging risks outlined in the preceding sections requires more than a like-for-like swap of legacy connections. Water utilities need a connectivity architecture that delivers resilience across multiple network cores, maintains separation between OT and IT traffic, provides the monitoring visibility that regulators increasingly expect, and remains operational through successive network retirements including 2G sunset. The following sections outline how this can be achieved in practice.

CSL's managed connectivity platforms address five core requirements: maintaining voice access, securing resilient data paths for alarms and telemetry, enabling remote access to reduce site visits, providing network-level resilience against both outages and technology retirements, and delivering OT network security and segmentation.

CSL DualCore Routers

Water utility sites present challenging deployment conditions: outdoor cabinets, temperature extremes, high humidity, and locations where physical access may be infrequent. CSL's DualCore routers are designed for these environments, providing a hardened, managed connectivity platform that supports **alarm telemetry**, **SCADA backhaul**, **voice** (via additional VoiceLink integration), and **secure remote access** from a single device per site.

Each router supports **DualCore connectivity**, providing **two independent operator profiles** and **automatic network failover** at the hardware level. If one mobile operator experiences a local or core network outage or sunsets 2G at a given location, the router automatically transitions to another available radio network, or the second core network operator's network (reacting to the coverage available at the site), without manual intervention or hardware replacement.

CSL's routers are centrally managed through CSL's connectivity management platforms and support services, providing estate-wide visibility of device status, signal quality, data usage, and failover events. This management layer enables proactive identification of sites experiencing coverage degradation before it affects alarm or telemetry performance.



Purpose-Built for Critical Infrastructure

Unlike consumer or enterprise routers, CSL's routers are engineered for unattended deployment in challenging environments. The **metal enclosure**, **industrial-grade components**, and **dual independent multi-network SIM slots** reflect the design philosophy: reliability at remote sites where failure has compliance and safety consequences.

Key capabilities for water utilities include **managed VPN tunnels** for secure SCADA backhaul, **firewall policies** applied centrally and enforced at the device level, support for **legacy serial protocols** alongside modern IP-based systems, and **over-the-air firmware and configuration updates** that eliminate the need for site visits to maintain the connectivity layer.

One device, multiple functions. Each CSL DualCore router can replace several legacy connections: alarm panel PSTN line, SCADA dial-up link, and remote access modem. The result is a single managed, secured, and resilient cellular platform.

CSL DualCore Router

A hardened, managed connectivity platform with built-in DualCore failover, integrated VPN, firewall, and network segmentation for remote OT environments.



Network Segmentation: Isolating OT Traffic

When water utilities migrate from analogue lines to IP-based cellular connectivity, they are connecting operational technology assets to a modern data network for the first time. Without proper segmentation, SCADA controllers, alarm panels, and monitoring sensors become reachable from networks that should not have access to them.

How CSL implements segmentation

CSL's routers support network segmentation at the device level. OT traffic, including SCADA telemetry, alarm escalation data, and process control communications, is logically separated from any other traffic. Each traffic type can be assigned to a distinct VPN tunnel or VLAN, ensuring alarm and telemetry data travels over a dedicated, isolated path to the utility's control room or Alarm Receiving Centre.

This approach aligns with established OT security principles, including the Purdue Model for industrial network architecture and NCSC guidance on securing operational technology.

Securing Remote Water Sites

Every CSL router establishes an encrypted VPN tunnel between the remote site and the utility's designated endpoint. Managed firewall policies are applied at the router level, controlling which devices and protocols are permitted to communicate over the cellular connection.

Critically, all CSL connectivity operates over a **private APN**, meaning traffic from remote sites avoids traversing the public internet. The private APN provides network-level isolation before VPN encryption is even applied, creating a defence-in-depth architecture: private APN at the network layer, encrypted VPN tunnels at the transport layer, and managed firewall policies at the device level.

CSL's managed security model means that firewall rules and VPN configurations are maintained centrally and applied consistently across the entire estate. When vulnerabilities are identified or security policies change, updates can be deployed remotely without requiring site visits, an operational advantage especially significant for utilities managing hundreds of remote sites.



CSL VoiceLink

Not every site requires a full Digital Voice transformation programme, but many still need basic voice capability for maintenance teams, emergency response, or contractor coordination. CSL VoiceLink converts PSTN calls to 4G VoLTE, enabling existing analogue-dependent devices, including pumping station autodiallers, to continue making voice calls after PSTN withdrawal.

VoiceLink incorporates built-in battery backup to maintain voice availability during short power interruptions. Because VoiceLink is deployed alongside CSL's routers, utilities can consolidate voice, telemetry, and alarm connectivity through a single managed account and set of secured platforms per site.

Water sector context. The UK water sector relies on an estimated 25,000 PSTN lines¹⁴. VoiceLink provides a retrofit path for these connections without the expense of replacing existing voice alarm devices, emergency callers or autodiallers.

CSL VoiceLink

PSTN to 4G VoLTE converter with built-in battery backup. Plug-and-play installation for existing call systems, autodiallers, and emergency phone lines.



Why Single-Core Roaming-Only Connectivity Falls Short

Water sites frequently occupy valleys, rural areas, or locations with inconsistent cellular coverage. A roaming SIM may be unable to maintain service if coverage degrades on the currently selected network. Because roaming relies on inter-operator agreements and device-level network-selection policies, switching behaviour may not be deterministic.

What core diversity means

CSL's DualCore rSIM® carries two separate network identities on a single SIM, enabling automatic failover between completely discrete core-network operators and end-to-end secure pathways without dependence on single points of failure.

How rSIM changes operational resilience

When deployed within third-party monitoring devices, this DualCore cellular architecture maintains alarms, SCADA telemetry, and remote access even during sustained disruption on one operator's network.

The SIM's monitoring system applet detects data or voice degradation and switches networks or core paths autonomously. This means that resilient DualCore technology can be applied to devices with limited inherent switching capability or sophistication, without requiring firmware changes or manual intervention at the device level.

Failover comparison

Method	Recovery exposure	Core diversity?
Single-core roaming SIM	Hours to restore, provider-dependent	No
CSL DualCore rSIM®	Autonomous (configurable)	Yes: always

rSIM's monitoring intervals are centrally configurable to adapt to device requirements and monitoring contexts. rSIM is GSMA SGP.32 aligned²².

One Deployment, Three Transitions

For water utilities, a single deployment decision, standardising on CSL DualCore routers, VoiceLink, and/or rSIM, provides resilience across PSTN withdrawal, 3G retirement, and 2G sunset, rather than requiring successive migration programmes each time a network technology is retired.

Resilience Through 3G Retirement and 2G Sunset

Vodafone, EE, and Three have completed their 3G retirements^{19,20,21}. Virgin Media O2 is completing shutdown in early 2026, with inbound roaming already ceased on 2G and 3G for multi-network IoT SIMs¹⁸. 2G sunset programmes are confirmed, with EE beginning from May 2029¹⁶ and Vodafone during 2030¹⁷. For any water site migrated from PSTN to a single-network cellular device, these retirements present a risk of a second connectivity failure.

CSL's DualCore architecture directly addresses this. Because each router or rSIM® carries two independent core operator profiles, the device is not dependent on any single operator's technology roadmap. If one operator sunsets 2G at a given location, the router or rSIM automatically fails over to the second operator where coverage is available at the site, maintaining service continuity without manual intervention or hardware replacement. CSL's routers operate on 4G, so the device radio hardware itself is not dependent on legacy 2G or 3G network availability. Indeed, as 3G is retired, access to 4G through re-farming is improving.

Reducing Truck Rolls with Secure Remote Access

CSL's routers provide secure remote access to SCADA outstations through encrypted VPN tunnels, reducing unnecessary site visits and enabling faster fault restoration.

Illustrative truck-roll savings

A utility managing 500 remote pumping stations, each averaging three investigative visits per year at £150 per truck roll, faces £225,000/year. Eliminating one unnecessary visit per site saves £75,000/year; eliminating two saves £150,000.



Practical Migration Approach

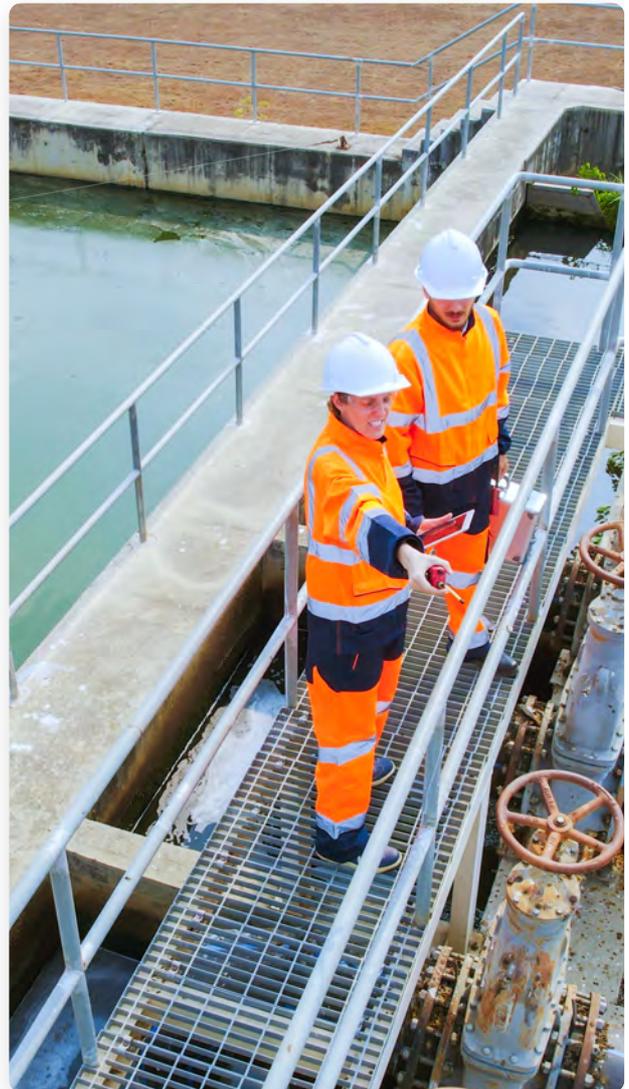
- **1.** Audit all PSTN lines and existing cellular devices. Flag any 2G-only devices for priority replacement. Assess OT security posture at each site.
- **2.** Identify flood-critical and compliance-critical sites for priority migration.
- **3.** Standardise on CSL DualCore routers for site connectivity, telemetry, remote access, and OT network segmentation. Deploy rSIM® in third-party monitoring devices that require DualCore resilience.
- **4.** Deploy CSL VoiceLink where voice access remains a requirement.
- **5.** Implement battery-backed resilience at the router and voice layer for priority sites.
- **6.** Define and apply network segmentation policies, VPN configurations, and managed firewall rules across the estate.
- **7.** Test alarm escalation, remote access, and OT segmentation under power-loss and single-network-failure scenarios.

Key takeaway

Migrate alarm escalation and telemetry first, with OT traffic segmented and secured from the outset. Prioritise flood-critical and compliance-critical sites, deploy encrypted remote access to reduce truck rolls, and test under both power-loss and network-failure conditions. A single deployment decision now provides resilience across PSTN withdrawal, 3G retirement, and 2G sunset, avoiding successive migration programmes as each network technology is retired.

PSTN and Cellular Dependency Audit Scope

- **Line-by-line inventory** mapped to connected device (alarm panel, autodialler, SCADA RTU/modem, lift station controller), including existing 2G-only cellular deployments.
- **Resilience gap assessment:** site power (battery/UPS), cellular coverage across multiple operators, and required uptime for flood-critical or compliance-critical sites.
- **OT security review:** current network segmentation, VPN and firewall configurations, and unsecured OT devices that would be exposed by migration to IP-based connectivity.
- **Migration and test plan:** replacement technology, commissioning steps, and evidence of alarm escalation, remote access, and OT segmentation under power-loss and network-failure conditions.



CSL has supported managed connectivity migrations across critical infrastructure estates for over two decades, including water utilities, telecare providers, and fire and security operators.

DEPLOYMENT SNAPSHOT

Major UK Water Utility: Over 3,000 Telemetry Sites

A water utility serving millions of customers relied on PSTN for telemetry at thousands of remote sites. Data was logged locally and often delayed until end of day, limiting fault visibility.

Working with our partner, CSL deployed a dual-managed connectivity platform across over **3,000 sites** ahead of the 2027 PSTN deadline. The result:

- ▶ **Continuous telemetry uplink** across all migrated sites, replacing end-of-day batch uploads with live data feeds to the control room
- ▶ **Faster fault detection** enabling proactive maintenance and reducing average response times from hours to minutes
- ▶ **DualCore resilience at every site** with no single-network dependency and managed failover across independent core operators
- ▶ **Single migration programme** covering PSTN withdrawal, 3G retirement, and 2G sunset without requiring further hardware intervention



Turning a Deadline into a Resilience Opportunity

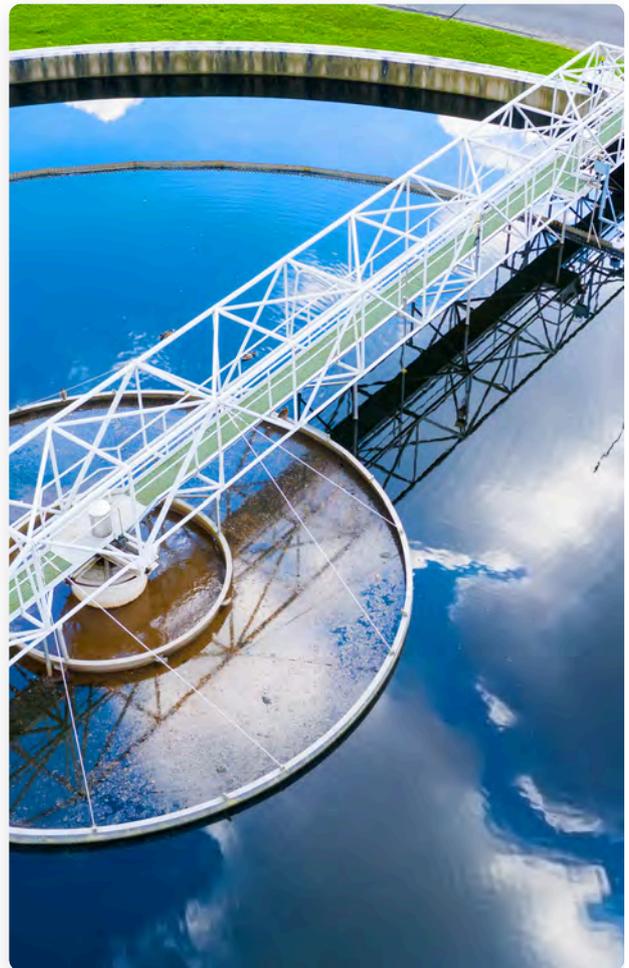
For water operators, the convergence of PSTN cessation, 3G retirement, and 2G sunset represents both an operational risk and an opportunity to fundamentally upgrade site resilience and security. The operators that act now will avoid compliance exposure and gain measurable operational advantages: reduced truck rolls, faster diagnostics, improved flood response, and a strengthened OT security posture^{7,8,9,10}.

Next step: Book a PSTN and cellular dependency audit

Confirm which safety-critical paths, power resilience gaps, and OT security exposures exist across the estate. Identify any 2G devices at risk from network retirement. CSL's specialist team will scope the audit, map dependencies, and deliver a prioritised migration plan.

Request an audit: [csl-group.com/contact-us](https://www.csl-group.com/contact-us)

Background reading: [Download CSL's PSTN Switch-Off eBook](#)



Frequently Asked Questions

When is the PSTN switch-off?

Full PSTN withdrawal is scheduled for 31 January 2027. The national WLR stop sell, applicable across all Openreach exchanges, has already ceased new analogue line provisioning^{1,2}.

What breaks first at remote water sites?

Alarm escalation paths and SCADA dial-up links are typically the first to fail, as they depend on analogue connectivity that cannot be re-provisioned once the WLR stop sell applies.

How do 3G retirement and 2G sunset affect water utility connectivity?

Vodafone, EE, and Three have completed 3G retirement^{19,20,21}; Virgin Media O2 is completing in early 2026 (inbound roaming already ceased). 2G sunset is confirmed: EE from May 2029, Vodafone during 2030. Any site relying on a single-network 2G device faces connectivity loss. CSL's rSIM® DualCore architecture mitigates this by carrying two independent core network operator profiles with automatic failover and multi-network local radio capability on both core profiles.

What are CSL DualCore routers?

Purpose-built, hardened connectivity devices for challenging OT environments. Each provides built-in DualCore connectivity with two independent core network operator profiles and automatic network failover. The routers also support managed Private APN, VPN and firewall policies, network segmentation, and secure remote access. Centrally managed through CSL's connectivity platforms.

Why does network segmentation matter?

Migrating from isolated analogue lines to IP connectivity means OT devices are on a data network for the first time. Without segmentation, SCADA controllers and alarm panels could be reachable from unauthorised systems. CSL's routers enforce segmentation at the device level, aligning with NCSC guidance on securing OT.

How is remote site security managed across a large estate?

CSL's managed security model applies firewall rules and VPN configurations centrally and deploys them consistently across every router. When security policies change, updates are pushed remotely without site visits.

Do we need battery backup?

Yes, for any flood-critical or compliance-critical site. Unlike analogue lines, cellular routers require local power. Battery backup ensures alarms and remote access remain available during mains outages.

How does rSIM differ from a roaming SIM?

A roaming SIM relies on inter-operator agreements with limited control over switching. CSL's rSIM® carries two independent core operator profiles (each with multi-network capability) on a single SIM, enabling deterministic failover, including resilience against 2G sunset. The SIM itself monitors traffic and intelligently switches core networks as required under the configuration rules applied.

Can existing analogue alarm voice-call panels work with cellular?

In most cases, yes. CSL VoiceLink converts PSTN calls to 4G VoLTE, enabling existing analogue alarm voice-call or data panels and autodiallers to continue operating without expensive hardware replacement.

Is Digital Voice the same as PSTN switch-off?

Digital Voice is BT's consumer brand for IP telephony, but the underlying driver is the same: PSTN/ISDN withdrawal. The replacement strategy is the same: managed cellular connectivity via CSL's routers, with power resilience, DualCore failover, and OT network security.

What happens to SCADA dial-up links after PSTN?

Legacy dial-up SCADA links will cease to function once the PSTN line is withdrawn. These should be migrated to cellular-based IP connectivity using CSL's routers, which support serial and IP protocols used by common RTU and SCADA outstation equipment.



References

- 1 Openreach GEN046/23: Reminder of WLR UK Stop Sell (5 September 2023).
- 2 BT Wholesale: Product stop sells and FTTP exchange upgrades. btwholesale.com
- 3 UK Government guidance: Moving landlines to digital technologies. gov.uk
- 4 Ofcom: Connected Nations UK Report 2024 (PSTN resilience incidents). ofcom.org.uk
- 5 Ofwat: Enforcement cases and penalty decisions. ofwat.gov.uk
- 6 Environment Agency: Water company prosecution records and enforcement action. gov.uk/environment-agency
- 7 CSL VoiceLink: PSTN to 4G VoLTE converter. csl-group.com/support/voicelink
- 8 CSL IoT Routers: Instant, resilient, secure connectivity. csl-group.com/support/csl-router
- 9 CSL rSIM: DualCore resilience and automatic network switching. csl-group.com/solutions/rsim
- 10 CSL white paper: Building IoT Resilience (multi-network/multi-link). csl-group.com/white-papers
- 11 Defra: Storm Overflows Discharge Reduction Plan (August 2022). gov.uk
- 12 Defra: CWQM programme: provisional technical guidance (April 2023). assets.publishing.service.gov.uk
- 13 Environment Act 2021: Section 82 (continuous water quality monitoring). legislation.gov.uk
- 14 Cambridge Management Consulting: How the PSTN Switch-Off Will Impact the Public Sector (2022 water industry PSTN line estimate). cambridgemc.com

Full article: *PSTN Switch-Off, 3G Retirement, 2G Sunset, and Water Utilities* (v2.0, March 2026).

© 2026 CSL Group Limited. All rights reserved. No part of this publication may be reproduced or distributed without prior written permission from CSL Group. rSIM is a registered trademark of CSL Group Ltd. Information correct at time of publication. CSL Group accepts no liability for decisions made on the basis of this document.

References (continued)

- 15 Openreach: The UK's PSTN network is closing – information and key dates including 31 January 2027 full withdrawal. See Openreach statements for full information.
- 16 EE Business: 2G network switch-off beginning May 2029. business.ee.co.uk
- 17 Vodafone: 2G network phase-out during 2030. vodafone.com/news
- 18 Virgin Media O2: Getting your business ready for 2G and 3G inbound roaming changes. news.virginmediao2.co.uk
- 19 Vodafone UK: 3G switch-off confirmation. vodafone.co.uk
- 20 Three UK: 3G switch-off. three.co.uk
- 21 EE: 2G and 3G switch-off information. ee.co.uk
- 22 GSMA: SGP.32 eSIM IoT Architecture and Requirements specification. gsma.com/esim

Glossary

APN	Access Point Name. The gateway between a mobile network and a private or public IP network. A private APN ensures traffic avoids crossing the public internet.
ARC	Alarm Receiving Centre. A facility that monitors alarm signals from remote sites 24/7.
CWQM	Continuous Water Quality Monitoring. Section 82 duty requiring measurement of dissolved oxygen, pH, turbidity, and ammonia around storm overflows.
DualCore	CSL's connectivity architecture providing two independent mobile core network operator profiles with automatic failover. Built into CSL's routers and available as rSIM for third-party devices.
EDM	Event Duration Monitoring. Records the frequency and duration of storm overflow discharges; data must be published in near real time from January 2025.
OT	Operational Technology. Hardware and software that monitors or controls physical processes (e.g. pumps, valves, sensors).
PSTN	Public Switched Telephone Network. The legacy analogue telephone system being withdrawn by 31 January 2027.
rSIM	CSL's resilient SIM technology. Each rSIM carries two core network operator profiles, enabling deterministic network failover.
SCADA	Supervisory Control and Data Acquisition. Systems used to monitor and control remote infrastructure such as pumping stations and treatment works.
VLAN	Virtual Local Area Network. A method of logically segmenting network traffic to isolate OT from other data.
VoLTE	Voice over LTE. Voice calls carried over the 4G mobile network rather than legacy circuit-switched infrastructure.
VPN	Virtual Private Network. An encrypted tunnel between a remote site and the utility's control centre or ARC.
WLR	Wholesale Line Rental. The Openreach product underpinning analogue PSTN lines; national stop sell is in effect.

