ATSC 3.0 Migration

Easy, Reliable and Secure Migration

## Challenges of Deploying ATSC 3.0: A New Era In Broadcast

ATSC 3.0 represents a major improvement to broadcasters and broadcasting infrastructure, but like any new and powerful technology, there are many hurdles to be overcome.

From the requirement to migrate to a 100% packet-based infrastructure, the requirements posed by keeping the existing ATSC 1.0 networks on-air through the transition and finishing with securing both the new and old infrastructure from the risks posed by today's cyber threat landscape, the process seems fraught with challenges.

Delivering STLTP and SFN Reliably

Traditional STL links are typically served with either DVB-ASI microwave, IP Microwave, or IP-based terrestrial links. ATSC 3.0 STLTP and SFN links requires precise IP packet distribution and has proven to be very intolerant of any disruption in packet flow between the gateway and the exciter.

VideoFlow analyzes the internal structure of the STLTP payloads and guarantees delivery exactly on time, with configurable deterministic path latency and a de-jittered output that ensures stability to the exciter. VideoFlow's solution meets the increased reliability requirements for STLTP to avoid exciter resyncs due to delay, jitter or loss in the transport netowk.
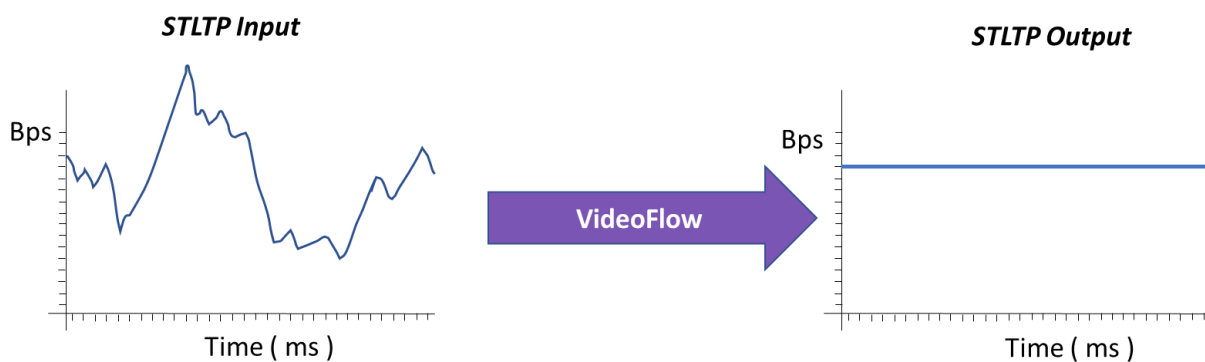
In addition to correcting any transport stability issues, the VideoFlow solution can add multiple layers of redundancy to overcome any momentary or prolonged disruption in the primary transmission path. VideoFlow can also provide load-sharing, so existing microwave infrastructure can be reused.
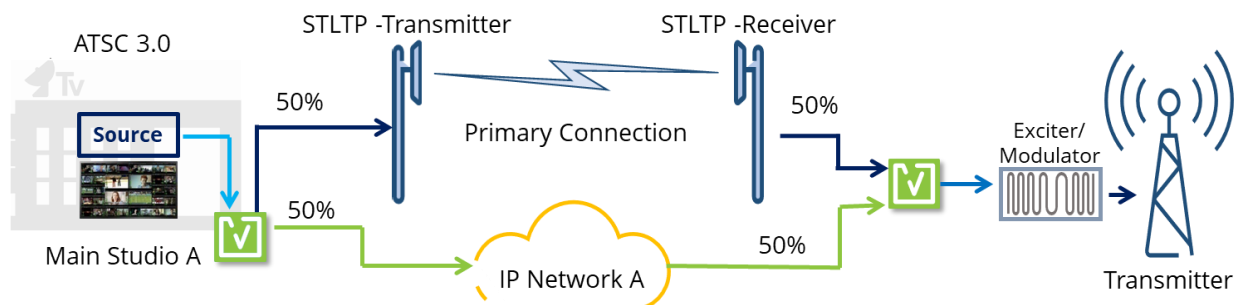
Managing the transition to ATSC 3.0 – The Lighthouse

The "Lighthouse" or "service aggregator" solution is being used as an interim steppingstone in the transition between ATSC 1.0 and ATSC 3.0. Here too, VideoFlow plays a central role in delivering the broadcast streams to the designated market Lighthouse for service consolidation.

VideoFlow makes the delivery to the lighthouse reliable and feature-rich, with a comprehensive set of 2022 Transport Stream Monitoring and Analysis Tools, a full API for monitoring and control access, and the ability to transcode and deliver TS and OTT-based confidence return feeds from ATSC1 sources back to the station-contributors. In addition, the same Video Flow equipment can be used for the STLTP link from the Lighthouse to the Transmitter, thereby optimizing VideoFlow utilization and reducing costs.

Finally, VideoFlow provides an extensive IT-centric toolset to quickly fault isolate any outage or degradation of service. This comprehensive packet toolset includes TCPDump, VNStat, NMAP, MDR, Traceroute, Speed Testing, and other utilities that provide a common toolset to be leveraged by both the broadcasting and IT professionals.

Uniquely, these tools allow broadcast and IT teams to work together, not point fingers.
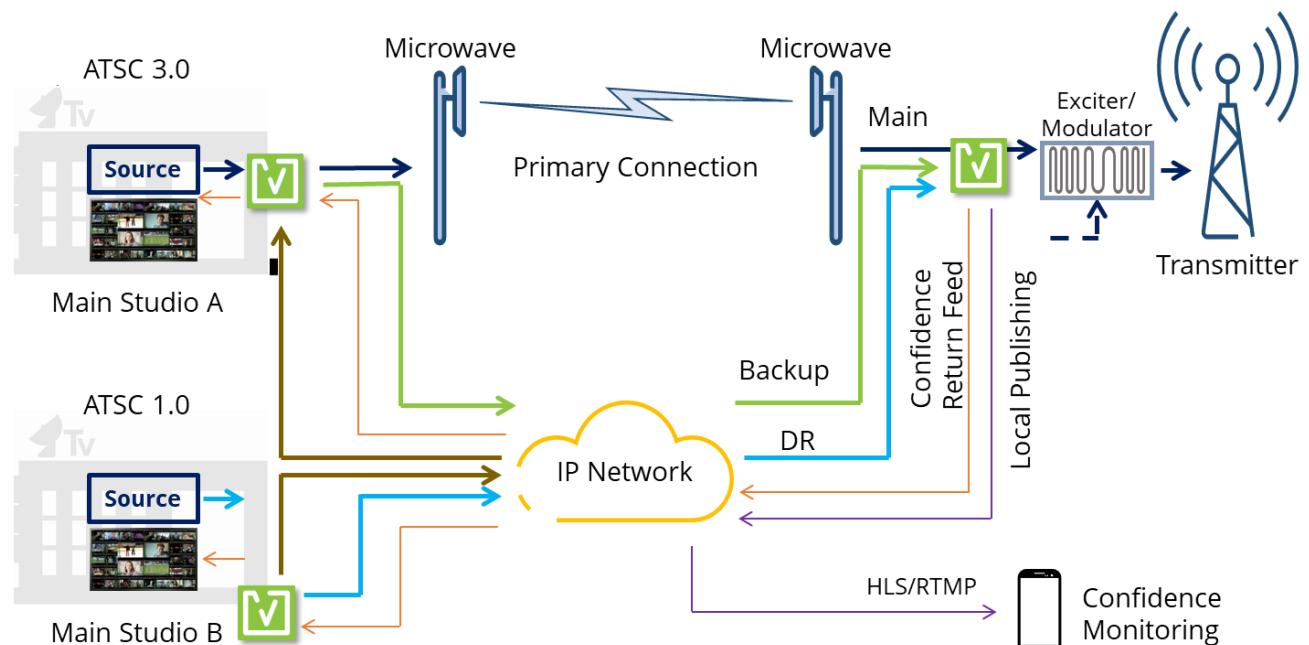
Cyber Security Challenges in ATSC 3.0

One of the major changes that ATSC 3.0 brought to broadcasting technology is the IP network infrastructure. The flexibility and power that IP brought also introduced new vulnerabilities into the broadcast network. The IP network connectivity that now runs from the studio all the way up to and including the transmitter introduces new points of failures in the form of cyber vulnerabilities.

As a pioneer in broadcast delivery over the public Internet – VideoFlow has been designed from the ground up to be cyber-secure. It provides a hardened OS that is designed with a minimal attack surface. VideoFlow DVG has a built-in firewall and a military-grade encrypted VPN and can secure its content from end-to-end.

The VideoFlow solution has gone through EBU R-143 Cyber Security Auditing to both conform and validate security to the industry best practices and helps to make your cyber security team's job easy and transparent.

Given the inherent vulnerabilities of an IP topology, VideoFlow provides you with the highest level of resilience against any type of cyber-attack.

Video Flow Solves all ATSC 3.0 Migration Challenges

VideoFlow's inherent IP-based design has made it the natural solution for deploying new ATSC 3.0 broadcast services. VideoFlow solutions span the gamut from existing ATSC 1.0, through the migration process with the Lighthouse solution, and finally with STLTP links to the exciter. It also protects broadcasters from the new and emerging cyber security dangers introduced by the IP infrastructure.

All VideoFlow solutions provide:

- **Reliability** – Ultimate reliability with secondary and tertiary resilience.

- **Ease-of-Deployment** – Comprehensive toolkit to quickly fault isolate and resolve faults.

- **Maximum ATSC 3.0 cybersecurity** – Comprehensive security optimized for a product designed to be deployed on the open public Internet.

- **Complete set of solutions for ATSC 3.0** – Lighthouse delivery and STLTP native transport modes.