

Creating High-Availability SS7 and SIGTRAN Signaling Applications in Telecommunication Networks

A White Paper from Telesoft Technologies

DX-TDP-GEN-MK-WP-33207-01

Where **innovative thinking**
meets **engineering excellence**



Contents

Executive summary	3
The need for high-availability telecommunications systems	3
Telesoft Technologies high-availability solutions	4
C-Cure for protection in TDM circuit switched communications networks	5
C-Cure for protection in IP communications networks.....	7
Summary	9
References	9

Executive summary

This paper outlines the accepted need for high-availability applications in telephony network architectures via the use of redundancy within network architectures. Telesoft Technologies' C-CURE security application can be used in SS7 and SIGTRAN signaling applications to create robust applications with 99.999% reliability for communication systems.

The C-CURE security API allows application/system developers and integrators to create robust, high-availability signaling applications for both TDM and next generation IP networks that meet the reliability standards expected by end-users and demanded by network operators.

The need for high-availability telecommunications systems

Telecommunications operators rightly demand resilient telecommunications networks that are reliably available every second of every day. Communication networks are usually designed to be available for at least 99.999% (five 9s) of the time, which equates to less and five and a half minutes per year downtime in continuous operation. In addition to reliability carrier-grade systems require very fast fault recovery through redundancy, ensuring that failures are effectively masked to end-users.

In order to meet these stringent demands communications system architects typically eliminate single points of failure in the signaling (SS7/SIGTRAN) connections and equipment supporting signaling connections. Typical reasons of failure that need to be considered in design resilience include:

- Signaling link failure
- Signaling interface hardware failure
- Server application node failure, including power outages, operating system problems and application software issues

High-availability systems nearly always build in redundancy using active/standby configurations to meet these stringent requirements for network resilience. In a typical scenario shown below if server application node "a" below fails then node "b" immediately takes over. Node "a" is typically known as the active (or primary) node while node "b" is known as the standby (or secondary) node.

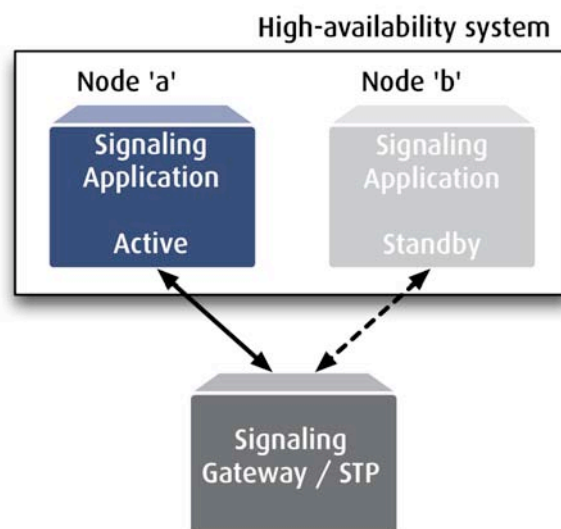


Figure 1: Typical High-availability system with built-in redundancy

By building redundancy into the system we ensure that single node failure need not be catastrophic. If node "a" goes down then node "b" takes over operations to the overall network without disruption.

Telesoft Technologies high-availability solutions

Telesoft Technologies designs and develops software components for OEM telephony developers called the TDAPI software framework. The C-CURE security application API is provided as part of this TDAPI software framework as a mechanism to implement redundancy in application servers across SS7/SIGTRAN environments.

C-CURE security application API allows dual node operation in an active/standby configuration sharing a single point code (in SS7) or routing key (in SIGTRAN). If the active node fails then the standby node takes over without disruption.

The C-CURE architecture is shown in figure 2 below. Both nodes run identical copies of the software stack processes. In normal operation the processes running on the active node regularly update the security application in that node. The security application mirrors this data to the security application on the standby node thus creating a complete data set. In this way if a failure occurs then the standby plane immediately takes over, becoming the active plane and taking over the workload with no service disruption.

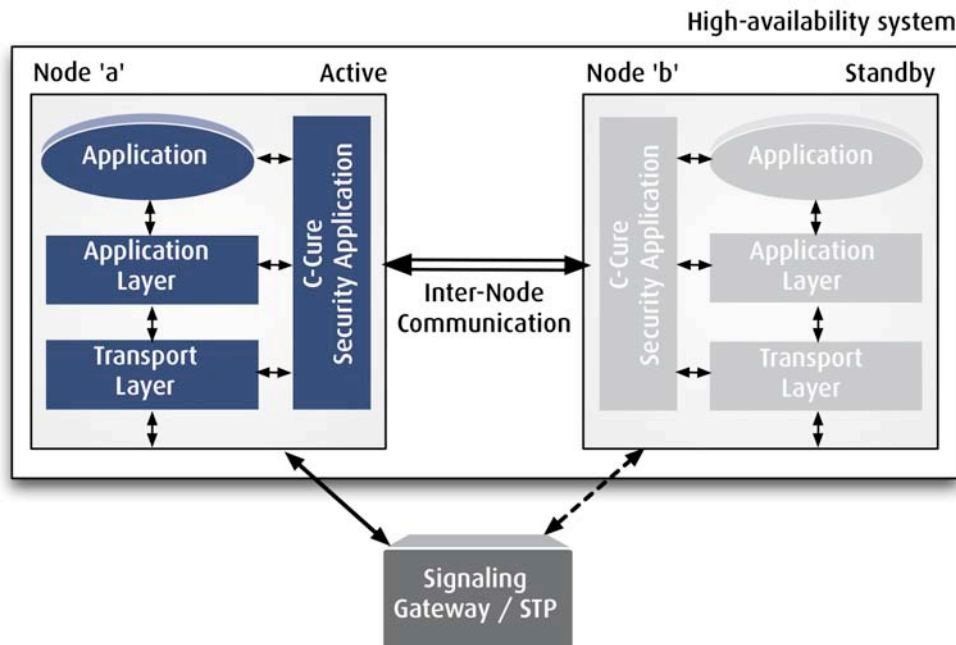


Figure 2: Telesoft Technologies C-CURE security API links active/standby nodes

The C-CURE application is responsible for managing the inter-node communication, for arbitrating active-standby status of the two nodes and for sending and receiving checkpoint data. Using the C-CURE security API application developers can create robust, highly resilient applications. In this context highly resilient is defined such that the node is always available. At the MTP layer 3, minimum service disruption is taken to mean that the route-set status will be preserved.

C-CURE allows communication between nodes via TCP sockets, typically via redundant Ethernet connection. It provides control of Active/Standby state and functions for sending and receiving checkpoint data. An example application using the TDAPI software framework and C-CURE security API is provided with the development kit that can be easily adapted by application developers to build redundancy into their application.

C-Cure for protection in TDM circuit switched communications networks

Within a TDM environment SS7 signaling is used to provide the setup and control calls as well as provide non-circuit related services such as SMS & USSD. A typical signaling stack for an SS7 signaling environment running on a TDM circuit switched network is defined below:

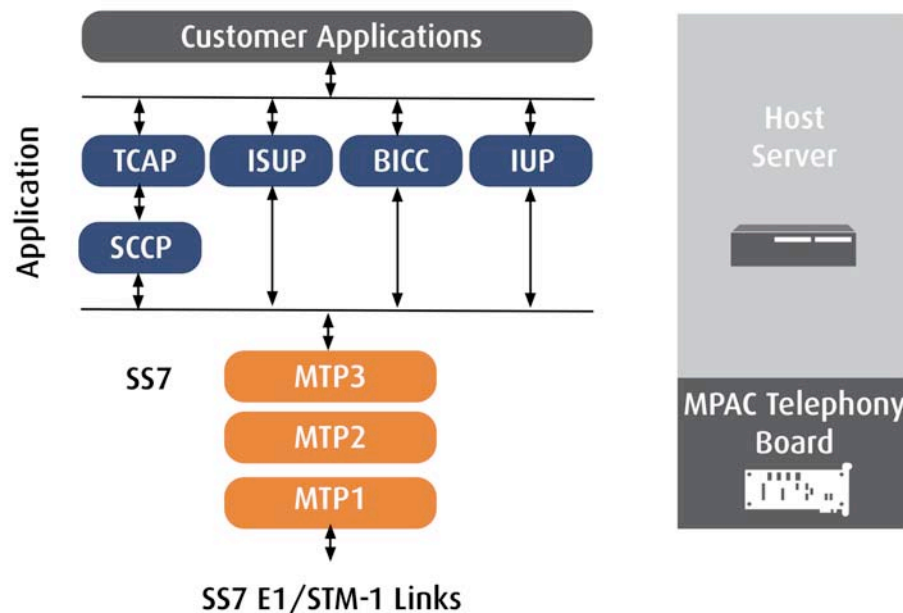


Figure 3: SS7/TDM network signaling stacks

Specialized hardware is required to access TDM networks. Telesoft Technologies MPAC Telephony Boards provide reliable SS7 interfaces between the user application running on a host server and the telephony network. Designed to interface directly with the network they take care of the signaling tasks required to communicate with the host network.

System Integrators and OEMs use MPAC Telephony Boards and TDAPI software framework to access and control the network and create media, signaling, switching and monitoring applications. TDM interfaces supported include electrical (E1/T1) and optical (STM-1/OC-3) of various combinations on a modern PCI-Express (PCIe) form factor board that fits into any modern server (SUN, IBM, DELL etc). The TDAPI software framework, shown in figure 4, includes protocol support for WIN, MAP, CAMEL and ISUP (as well as the C-CURE security application) allowing application developers to create complex applications that interact directly with the network and users.

In TDM environments, the C-CURE security application provides the mechanism for controlling and data state check pointing of the protocol stacks in order to provide redundancy. The nodes continuously swap checkpoint data in order to stay in lock step. In the event of failure of the active node (node a) the C-CURE API sends a 'go worker' signal to the standby node (node b) which immediately takes over node a's work with no interruption in service.

In addition to the C-CURE security API environment SS7/TDM architectures also protect against physical link failure by the distribution of signaling links across MPAC telephony boards and servers. By spreading signaling links in a link-set across two or more physically separated nodes (i.e. nodes 'a' and 'b' in this example) the network architect protects against failure of a single signaling link, MPAC Telephony Board or host server as shown in figure 5.

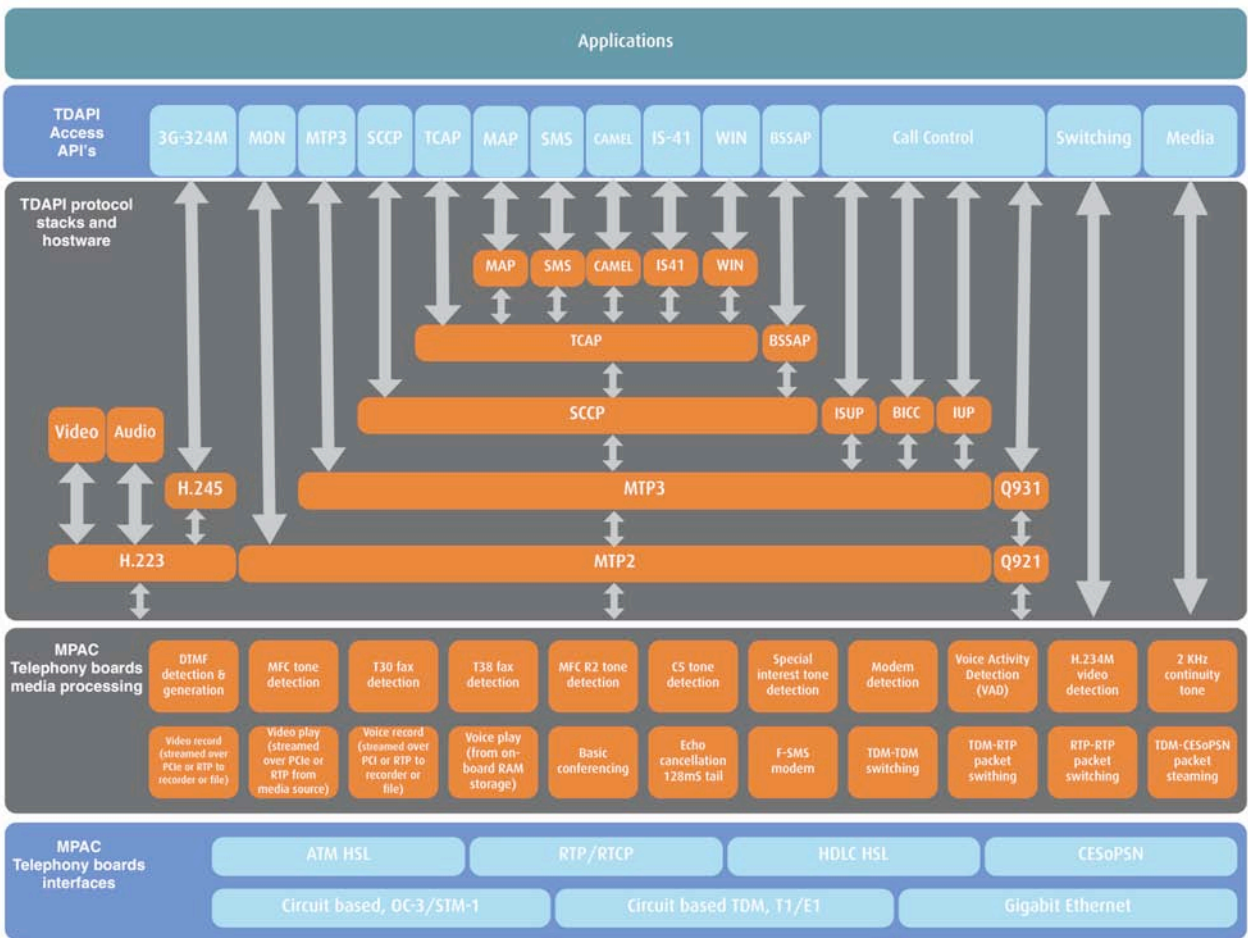


Figure 4: TDAPI software framework

Links in a link-set load share traffic such that if one link fails then the signaling is carried instead through the remaining active shared link. For example if link “a” fails then the signaling will instead be routed through link “b” and, via an inter-board communication bus, to the active signaling application in node “a”.

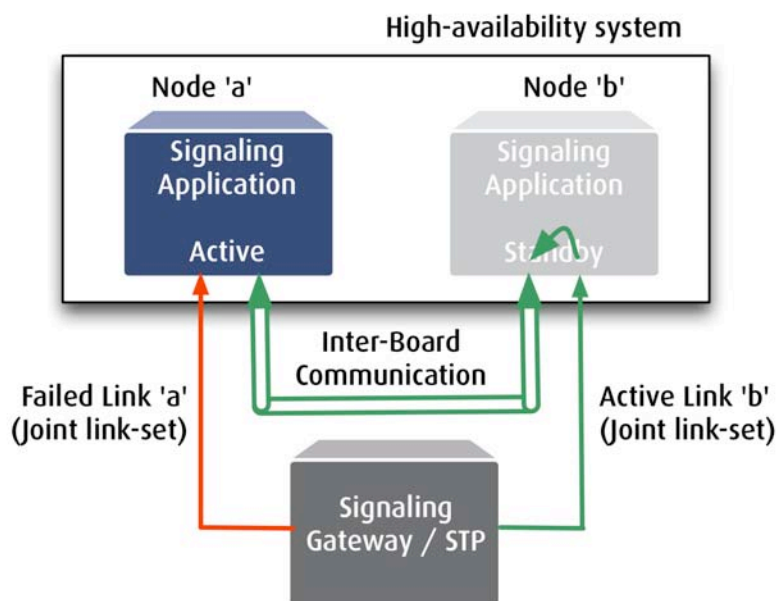


Figure 5: SS7 Signaling link failure mechanism

C-Cure for protection in IP communications networks

In IP next generation communication networks the lower layers of the SS7 signaling stack (MTP1, 2 and 3) are replaced by the equivalent SIGTRAN signaling stack (IP, SCTP, and M3UA) as the transport layers over which the higher level (level 4 and above) protocols run, leaving the upper stack unchanged. A typical signaling stack for a SIGTRAN signaling environment running on an IP network is defined below:

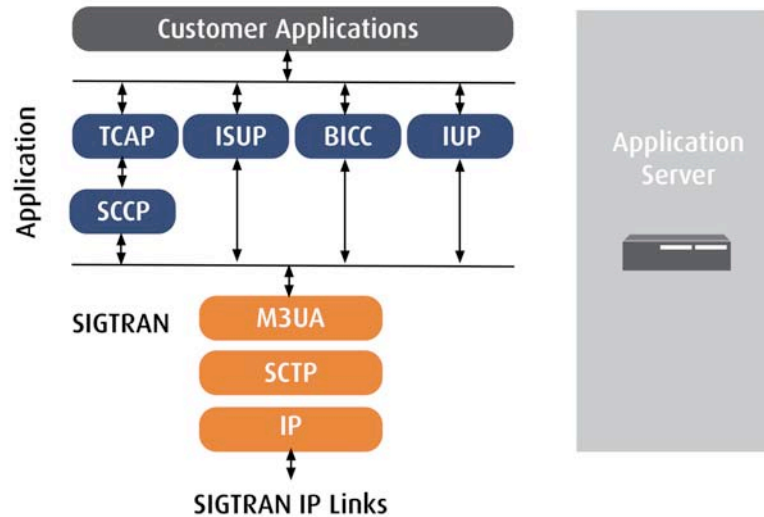


Figure 6: SIGTRAN/IP network signaling stacks

Instead of the signaling running over fixed E1 they now run over Ethernet. SIGTRAN software and associated C-CURE security application runs on the host compute server and does not require additional hardware. Redundancy is built into this architecture in a similar way to TDM circuits in that the C-CURE software now interacts with the M3UA (MTP3 user adaptation layer) and application to checkpoint data and transfer it between the active and standby nodes. In this way the standby node is always ready to take over, if the active node were to fail, with no loss of information.

As VoIP and IP multimedia subsystems (IMS) packet networks emerge operators are now using these networks to carry signaling. The good news is that it is straightforward to migrate SS7 signaling applications that were originally designed using MPAC Telephony Boards and the C-CURE security application to SIGTRAN/server only solutions. The higher-level protocols, such as ISUP and SCCP will be identical, thus requiring only the lower SS7 signaling layers (1-3) to be changed. The applications themselves are typically isolated from these and are therefore easily ported to next generation networks.

Typical Applications

The C-CURE Security software is used in conjunction with Telesoft Technologies' TDAPI software that incorporates a rich set of telephony protocols. Key protocols supported include:

- MAP, CAMEL, SMS, IS41, WIN, TCAP, SCCP, ISUP, BICC, IUP, M3UA, SCTP

Application developers and system integrators use this TDAPI software (along with the C-CURE security software for high-availability) to create robust applications for communication networks including:

- Signaling gateways
- Protocol converters
- Cellular network nodes: GMSC, SMSC, HLR, MSC, VLR, EIR etc
- SMS & USSD messaging gateways
- Missed-call alert systems
- Roaming services: 'welcome roamer', 'steering', 'bon voyage' etc
- IN service nodes (SCPs and STP) / CAMEL
- Voice and video gateway/mail platforms

Telesoft Technologies' TDAPI software (and MPAC telephony boards) has been used extensively throughout the world. Today more than 250 operators in mobile, fixed and IP networks deploy our products in over 100 different networks. Our products are approved for interconnect with most of the world's major carriers and switch vendors, including BT UK, T-mobile Germany, Telecom New Zealand, AT&T USA to name but a few.

Summary

Telesoft Technologies C-CURE security application, part of the TDAPI C-language software API suite, provides a robust mechanism to initialise and control nodes in high-availability signaling systems. C-CURE allows dual node redundant signaling applications to be easily managed in an active/standby configuration. Checkpoint and other management information automatically flows between the two nodes to keep them in lock step so that if the active node fails the standby node can take over in an instant with minimal disruption to the overall network.

In this way signaling applications, such as SMSC nodes or call control soft switches for backhaul of signaling links over the IP network, can easily reach the required five 9's (99.999%) reliability standard that network operators demand.

Telesoft Technologies C-CURE security API works with SS7 technology in the form of MPAC Telephony Boards that support TDM networks and SIGTRAN technology in the form of software only solutions that support IP networks. This ensures that end applications designed in TDM networks can be easily ported to next generation networks as migration becomes necessary.

About Telesoft Technologies

For more than 20 years the world's leading Operators, SIs, OEMs and application developers have relied on our signaling, media and monitoring platforms. They continue to depend on our technology to deliver revenue and non-revenue generating solutions for mobile and converged networks in areas such as media services, fraud, billing, roaming, monitoring and location.

As networks evolve our experience in real-world deployments coupled with our engineering prowess and financial stability ensures we are the partner you can rely on.

More information is available at <http://www.telesoft-technologies.com>

References

1. DX-TDP-GEN-US-GU-18066 Rev 15, TDAPI C-CURE Security API Reference
2. DX-OKE-GEN-MK-DS-32839 Rev 01, OKEFORD Installed Base
3. TDAPI Quick Reference Guide, <http://www.telesoft-technologies.com/products/mpac>

Telesoft Technologies, the Telesoft Technologies logo design, C-CURE, TDAPI and MPAC are trademarks or registered trademarks of Telesoft Technologies Ltd or its subsidiaries. All other brand and product names may be trademarks of their respective companies. Copyright ©2010 by Telesoft Technologies Ltd. All rights reserved.

Where **innovative thinking**
meets **engineering excellence**



Telesoft Technologies Ltd,
Observatory House,
Blandford, Dorset DT 11 9LQ UK

T. +44 (0)1258 480 880
F. +44 (0)1258 486 598
E. sales@telesoft-technologies.com

Telesoft Technologies Inc.
Suite 601, 4340 Georgetown Square,
Atlanta GA 30338 USA

T. +1 770 454 6001
F. +1 770 452 0130
E. salesusa@telesoft-technologies.com

Telesoft Technologies Ltd (Branch Office),
Building FC-24, Sector 16A, Noida 201301,
Uttar Pradesh, India

T. +91 120 466 0300
F. +91 120 466 0301
E. salesindia@telesoft-technologies.com