CML Microcircuits

COMMUNICATION SEMICONDUCTORS

Upgrading Analogue Radios with Digital Voice Encryption Easily and Cost Effectively

White paper

Reference: 7011WP Issue: B
Date: June 2014

1 INTRODUCTION

There has never been a greater need than now, to ensure secure voice communication on analogue radio systems. Many organisations rely on HF, UHF, VHF radio communication and assume/require that voice communication is private, to eliminate business espionage and guarantee staff personal safety.

New digital communication systems that are being rolled out present 'digital' as being inherently secure. At first sight, digital appears to be the answer. However there are drawbacks, these being the implementation cost and the requirement to substitute all existing radios with expensive digital replacements.

There are 100's of millions of analogue radios in the field today, all providing reliable operation and good service. Applications include Two-Way Radios (TWR), Private Mobile Radios (PMR) used in personal communication, through to industrial and security installations, door entry and gate access systems that are transitioning to wireless communication to reduce installation cost. All these systems have an expectation of good voice privacy.

This paper presents a highly integrated, cost-effective solution allowing an analogue radio to be upgraded to include real-time digital voice encryption, along with a number of other radio features normally associated with expensive digital radios.

2 VOICE SCRAMBLING SOLUTIONS

The current solution to providing rudimentary voice privacy on analogue radio is via the use of analogue voice scramblers of which there are a number of methods and solutions available on the market today. Although these are potentially easy to implement, they only offer low-level voice security, degrade the overall voice quality and provide no additional features that are becoming the norm on new digital radio implementations.

Digital encryption is the answer; however, retrofitting digital encryption into an existing analogue radio has a number of complications that need to be addressed. The most important one is how to transport good quality digital voice through a radio's audio channel with its associated limited bandwidth, without modifying the radio's RF (Radio Frequency) section.

3 DIGITAL VOICE ENCRYPTION HAS THE ANSWER

Digital voice encryption is achieved by digitising voice using a low bit rate vocoder and transporting this data via a low bit rate modem through a radio's audio path. A number of challenges need to be overcome to realise a genuine working system.

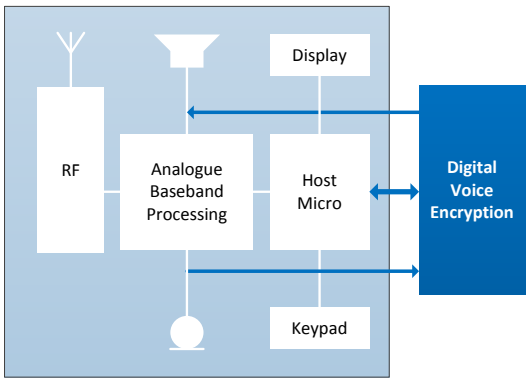


Figure 1: Typical Analogue Radio and Digital Voice Encryption Connections

3.1 Audio path bandwidth

The audio path frequency response in a typical analogue radio is very narrow, typically 300Hz to 3kHz. In a 12.5kHz channel radio the audio can start rolling-off as low as 2.55kHz. This narrow bandwidth sets the first challenge, getting enough modem data within the allowed bandwidth to transport the digitised voice. Figure 2 shows a typical analogue radio audio response along with the 12.5kHz and 25kHz channel templates.

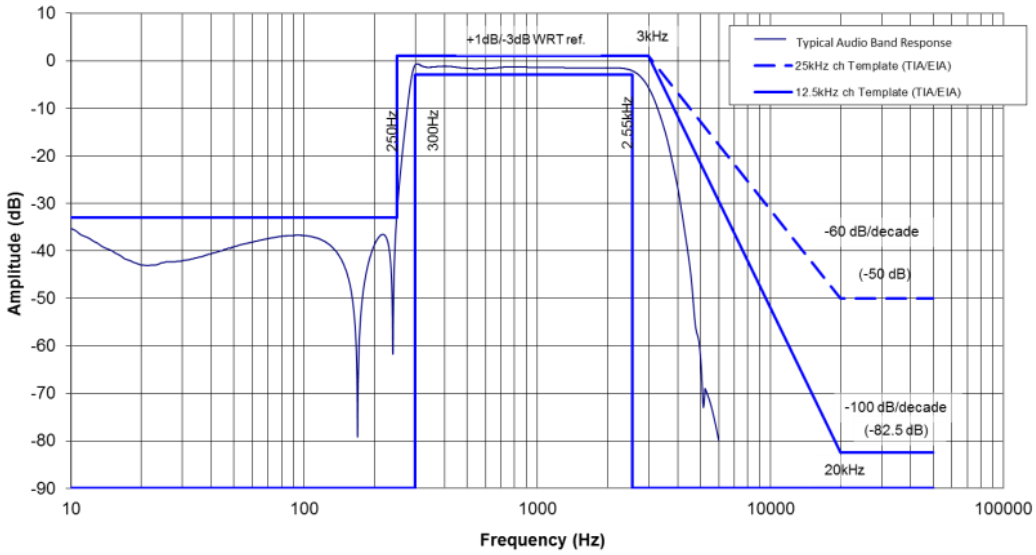


Figure 2: Typical Analogue Radio Audio Response

3.2 Modem selection

Modem selection is crucial to the performance of the overall system. A low cost, low complexity, robust modulation scheme is required, that can provide enough data bits to transport the digital voice and have some left over to mitigate potential errors in the transmission and enable a structured over-air interface protocol.

2400 baud Fast Frequency Shift Keying (FFSK), also known as Minimum Shift Keying (MSK), is a good choice. It provides excellent raw Bit Error Rate (BER) performance, typically achieving better than $1x10^{-4}$ BER at a 12dB Signal to Noise Ratio (SNR), this equates to 1 potential error in 10,000 bits transmitted. The modulation bandwidth fits easily within a radio's audio channel allowing simple connection into a radio system via the microphone and speaker sections.

3.3 Digitising voice

The next challenge is finding a low bit rate Vocoder that provides good quality voice and does not use all the available data bits.

There are a number of low bit rate vocoders available, this article focuses on the low cost, Robust Advanced Low Complexity Waveform Interpolation (RALCWI) vocoder available from CML Microcircuits, that is ideally suited to this application.

The RALCWI vocoder algorithm has a bit rate option for 2400 bits/s and provides a number of advanced operations to ensure a high level of voice quality is maintained at this low bit rate. Stand-alone ICs are available with no licencing fee and no royalty, the CMX618 RALCWI Vocoder includes: vocoder, audio codec, FEC and advanced features such as Packet Loss Concealment (PLC) with the CMX7011 Digital Voice Processor adding additional functionality as described in this paper.

3.4 Air interface protocol

A good air interface protocol design is crucial for achieving the optimum overall system performance and provisioning for advanced digital features such as packet data capability. A Header Frame is used at the start of any transmission; this contains synchronisation data, user-programmable addressing to select a user or group of users, a format field to specify the type of payload and the encryption seed. Only the encryption seed is transmitted, not the encryption key/algorithm ensuring a high level of security.

Embedded within these data frames: error detection/correction, interleaving/whitening techniques may also be employed to further mitigate transmission bit errors caused by fading or signal quality at the fringes of RF reception. A basic outline of a working air interface structure is shown in Figure 3.

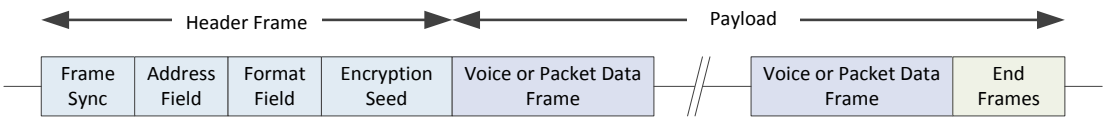


Figure 3: Digital Voice Air Interface Structure

Late-retry and re-entry scenarios need careful consideration. In a typical analogue system, if a caller turns on the radio or comes out of a deep fade during a transmission, the receiving radio would continue reception and the latter part of the message would be received. In a digital system if the frame header is missed or synchronisation has been lost due to a deep fade, the receiving radio will not be able to decode the received data and the remaining part of the call would be lost completely.

To duplicate the analogue radio operation in a late-entry/re-entry situation, Header Frames must be inserted at intervals throughout the call. Due to the limitation of the available data bits, occasionally voice frames would need to be replaced with Header Frames. The negative side to this is that the removal of good voice frames could cause unwanted voice distortion. To potentially eliminate these effects completely, the RALCWI vocoder noise gating feature is used as shown in Figure 4.

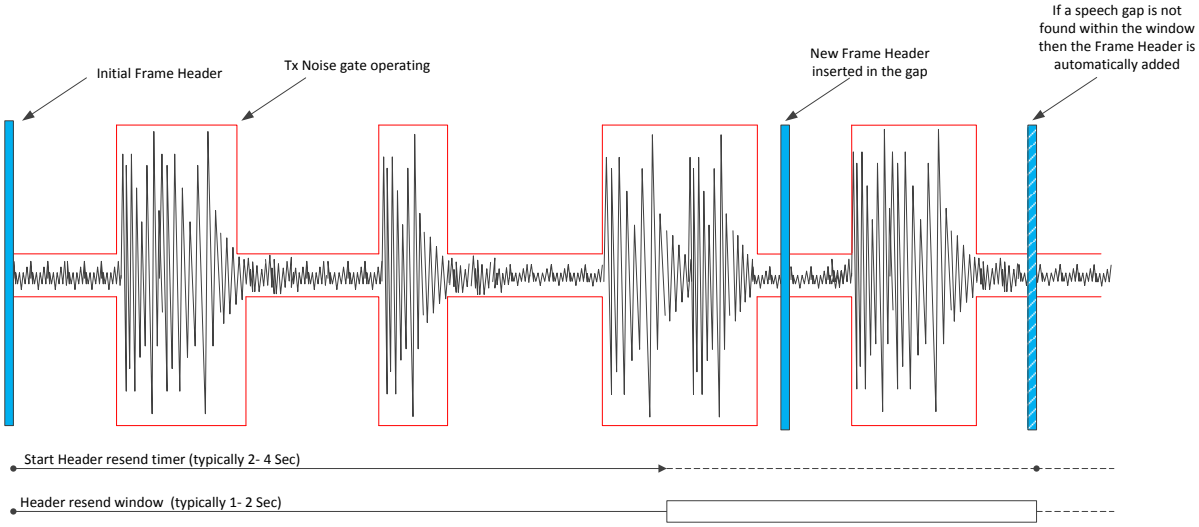


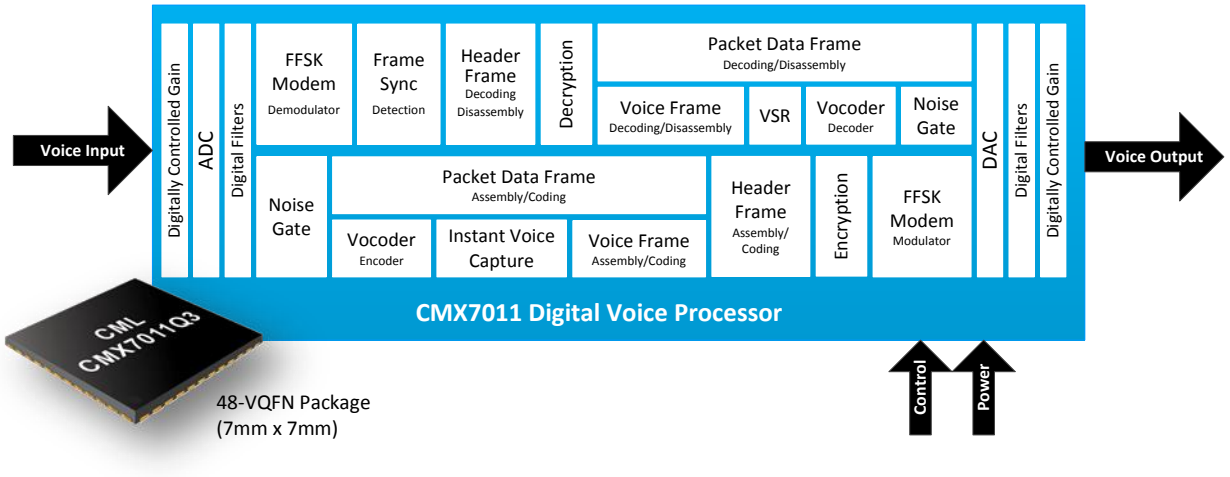
Figure 4: Noise Gating and Repeated Header Frames

In transmit repeated Header Frames are inserted within the voice data. When the Noise Gating function indicates that the voice level is below a pre-set threshold (no voice activity) a new Header Frame is inserted. The receiving unit detects the repeated Header Frame, mutes the audio momentarily and then uses the Vocoder PLC function to eliminate any potential voice pops and bangs.

4 PRODUCT REALISATION

The final challenge is product realisation. Size, cost, performance and ease of implementation are all very important, ensuring that upgrading an analogue radio with the digital advantage is realistic, easily achieved and cost effective.

The answer is high integration. The CMX7011 Digital Voice Processor, implements this complete function in a single chip and additionally provides a host of features not normally found on analogue radios.



4.1 CMX7011 Digital Voice Processor for Analogue Radio

The CMX7011 is a flexible, half-duplex, digital voice encryption processor that provides the digital advantage to conventional analogue two-way radios, wireless door access and gate entry systems.

Real-time digital voice encryption is a key feature of the device, using the embedded RALCI Vocoder and audio band robust data modem. In addition, the embedded Air Interface protocol also implements a number of advanced digital radio features, providing the digital advantage to analogue radio systems.

CMX7011 Implementing the Digital Advantage on Analogue Radio

- Complete digital voice encryption and secure packet data solution: vocoder, modem and air interface protocol
- Easy connection into the radio's audio path and only requires simple host control to set up the device and manage operation
- Secure encrypted digital voice with user-programmable encryption key
- Instant voice capture – eliminates the annoying clipping of the initial voice transmission in PTT (Push-To-Talk) PMR systems
- Late entry/re-entry – allows a user to receive a call part way through a transmission or continue to receive a transmission after a deep fade situation
- Packet data capability – Secure short packet data messaging
- Voice store and retrieve (VSR) – received voice messages can be stored for latter retrieval providing a voice notepad function
- Fast time from product evaluation to radio deployment. The PE0101-7011 Evaluation Kit is available to demonstrate CMX7011 operations and provide a fast and easy platform to connect into real radio system for field testing. Scripts are available to assist product evaluation and host code development.

Figure 4: PE0101-7011

The CMX7011 is a low power 3.3v device and is available in a small 48-pin VQFN and 48-pin LQFP packages. It uses CML's proprietary FirmASIC® component technology, providing maximum flexibility with upgrade capability.

5. What Next

The CMX7011 Datasheet can be downloaded here and the Product Preview here.

Further details of the unique CMX7011 Digital Voice Processor for analogue radio, can be found via the CML website page http://www.cmlmicro.com/products/CMX7011_Digital_Voice_Processor_Encryption/

6. About CML Microcircuits

CML Microcircuits is a world-leader in the design, development and supply of low-power analogue, digital and mixed-signal semiconductors for telecommunications systems globally. The company's wide and varied portfolio means that CML devices are used in an extensive range of industrial and commercial products for licensed and unlicensed wireless voice and data systems.

Focusing on narrowband communications, CML's ICs are found in PMR/LMR, wireless data and marine radio applications, such as TETRA, DMR, dPMR, SCADA systems and AIS. The CML portfolio provides components supporting both RF and baseband functionality, encompassing both leading edge digital and legacy analogue systems.

In addition to our established range of devices, using specialist knowledge and expertise, we are able to offer bespoke solutions to customers. This service includes design assistance, advice and first class technical support. Our *FirmASIC*® approach enables us to work closely with our customers to produce the optimum solution to a given design requirement. The outcome is a product offering that embraces a number of key technologies and delivers the result with fast time to market, ultimate flexibility and low risk.

With its ISO 9001: 2008 certified design, production and marketing facilities and its truly global network of over one-hundred accredited distributors and representatives, CML offers a high-quality product backed by a wealth of design experience and the on-going availability of 'local-knowledge' technical, applications and commercial support. This enables CML, and its customers, to respond to market demands quickly, accurately and cost-effectively.

Each and every CML device is tested at our UK site, including those manufactured offshore, thus ensuring that we can deliver highly reliable products with an extremely low failure rate. Through continual innovation and product development, CML is able to offer technical excellence in its products and services.

CML is supportive of conserving the natural environment and aims to manage its operations in ways that are environmentally friendly and economically viable. CML provides RoHS compliant, lead-free (Pb-free) products. CML's Environmental Policy can be found in the Quality area.

Company Structure

CML Microsystems Plc - CML Microsystems Plc is a holding company for the group's operating subsidiaries: The three CML Microcircuits companies are located in the UK, United States and Singapore. **Hyperstone GmbH**, part of the group since 2003, is a fabless semiconductor and microprocessor design company and is located in Germany, USA and Taiwan.

CML Microcircuits (CML) comprises three member companies of the CML Microsystems Plc group:

- CML Microcircuits (UK) Ltd.
- CML Microcircuits (USA) Inc.
- CML Microcircuits (Singapore) Pte Ltd

June 2014 MPL