AES SWISS SECTION NEWSLETTER

108th. Issue

INFORMATION ON NEXT MEETING

The Audio Installation at the Basel Tattoo

Location: Kaserne Basel

Monday, 16th of July 2007, 19h30-ca. 22h45

SPEAKERS: Thomas Strebel (Technical Director/Sound Designer, Audiopool GmbH, Basel)

Dave Haydon (Director Out Board Electronics / UK)

ORGANISER: Attila Karamustafaoglu

LANGUAGE: English and German

The Swiss AES Section is happy to be able to organize this meeting before the upcoming holiday season. On the occasion of the Basel Tattoo open-air, it will be able to visit the venue and get a presentation of the sound system and even visit the general rehearsal of the show itself one day before the public opening!
The sound system of this show is equipped with a TiMax system from Out Board Electronics which is able to track the actors and apply according delays to the loudspeaker channels to avoid phasing and cancellation effects while maintaining good intelligibility and locateability.
There are even two control rooms which are recording and producing a CD of the event which will be on sale already on the 19th as well a live broadcast to the tattoo street in front of the venue. Further there will be a 5.1 production made for the DVD production by tpc.

This special meeting will be structured roughly in following order:

1930h gathering at the entrance of the Tattoo open-air venue.

Ca. 1930h – ca. 2000h explanation of the overall project by Thomas Strebel

Ca. 2000h – 2030h presentation of the TiMax system by Dave Haydon

Ca. 2030h – 2100h Tour through the venue and the technical installations

Ca. 2100h – 2245h Free visit of the show rehearsal (for those people which want to see it).

Please subscribe as early as possible at www.swissaes.org / programme

REPORT ON PREVIOUS MEETING

The Genesis of Modern Computing, Digital Audio and Compression

Thursday, 21st of June 2007 at Studer Professional Audio GmbH, Regensdorf

SPEAKER: Jon Paul (Jon Paul, Crypto-Museum California/USA)

REPORTER: Attila Karamustafaoglu

It turned out that the ones which missed the event really missed something. Jon Pauls presentation was divided in two parts. The first one was about the history of cipher machines. There, of course the most famous cipher machine was explained with large extent: The Enigma. Interestingly the Enigma existed long before the Second World War. But it was not used very much. When the German Nazi regime gained increasing power in the country, they took the machine out of the public market to allow a safe use of it for their military purposes. The enigma was not the only machine of this type, but it had so many scrambling stages that the encryption resulted in a level which is comparable to a today's 400-bit cipher. This is pretty much, as e.g. for e-Banking a key with a length of 128 bits is used. Jon Paul explained then how several mathematicians of allied forces made attempts to crack it. Many Enigma solutions were developed first by Polish mathematicians starting in 1932, then by the British at Bletchley Park.

Besides Enigma, high command messages were carried by ciphered teletype via radio. A huge machine called the "Colossus" and consisting of several thousand valves finally cracked intercepted messages, at Bletchley Park.

This device is said to having had the computing power of about a Pentium I processor.

The second part then focussed more on speech scrambling, or the audio part, so to say. The roots of it are in the attempt to transmit speech over a telegraph transatlantic cable. The bandwidth of about 300Hz was insufficient to transmit any speech. Homer Dudley of Bell labs invented (in 1928!) a parametric speech synthesizer to synthesize speech with a few bands of voiced (buzz-type) and unvoiced (hiss-type) frequencies. To synthesize these speech sounds, a learning time of more than one year was required! The only successful player of the Voder was Hellen Harper, a Bell Telephone operator. Please see the weblinks below for more information, nice pictures of the Voder demonstration at the 1939 World's Fair in New York and some sound examples. It was explained that this coding mechanism is closely related to and preceeds the CELP codec as in operation in today's GSM and CDMA mobile phones.

Finally the history and construction of the SIGSALY was explained. During the war, the Americans including Dudley improved the Vocoder and added an automatic encoding and a scrambling. The resulting speech scrambling machine was called SIGSALY and was a dramatic technical achievement. When it was finished it was set up in 12 locations worldwide. 13 people were required to operate one terminal and the key, which was in form of a random noise signal came on two vinyl type records lasting for 12 minutes of encryption. One record was required at each end for scrambling and descrambling. After this very interesting presentation, the evening was concluded at the Trend-Hotel nearby with a small group. The Swiss AES Section wants to thank Jon again for this very interesting evening.

For more information please visit:

http://davidszondy.com/future/robot/voder.htm

http://www.wikipedia.org (enter SIGSALY)

http://www.nsa.gov/publications/publi00020.cfm

http://www.nsa.gov/publications/publi00019.cfm