



Telephone Line Monitoring Zebra System

Telephone Line Monitoring Zebra system

The Zebra system is a powerful telecommunications monitoring solution. It combines support for ETSI Lawful Interception with very dense passive monitoring in one hybrid solution. The Zebra system is suitable for law enforcement as well as intelligence gathering and is scalable from 16 E1 carriers (or equivalent channels) to more than 5,000 E1 carriers (or equivalent) in one integrated system.

References

- [1] ETSI TS 101 671 V2.13.1 (2006-01), Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic.
- [2] Telephone Line Monitoring Zebra E1-T1
- [3] Telephone Line Monitoring Zebra E1-T1 Gateways

Glossary

Bearer	Transmission bearer, typically of SDH/SONET optical transmissions. E.g.: STM-1, STM-4, etc bearer. Analogous to carrier (below).
Carrier	Transmission carrier, typically of PDH transmissions. E.g.: E1, DS3, etc carrier. Analogous to bearer (above).
ETSI LI	Lawful interception method standardized by the ETSI. See [1].
FTP	File transfer protocol (TCP/IP). See [1]
Hi-Z	High impedance buffering used to insulate passively monitored carriers from potential noise and signal reflections originating from the monitoring equipment.
ISDN PRI	Primary rate (E1/T1) ISDN. See [1]
LED	Light emitting diode
LI	Common abbreviation of ETSI LI (above).
LIID	Lawful intercept identifier. See [1]
MC	Monitor centre
PBX	Private branch exchange
PLMN	Public land mobile network – GSM, 3G.
Primary rate	2.048 Mbps (E1) or 1.544 Mbps (T1). See ITU-T Recommendation G.703
PSTN	Public switched telephone network – fixed line networks.
WAN	Wide area network

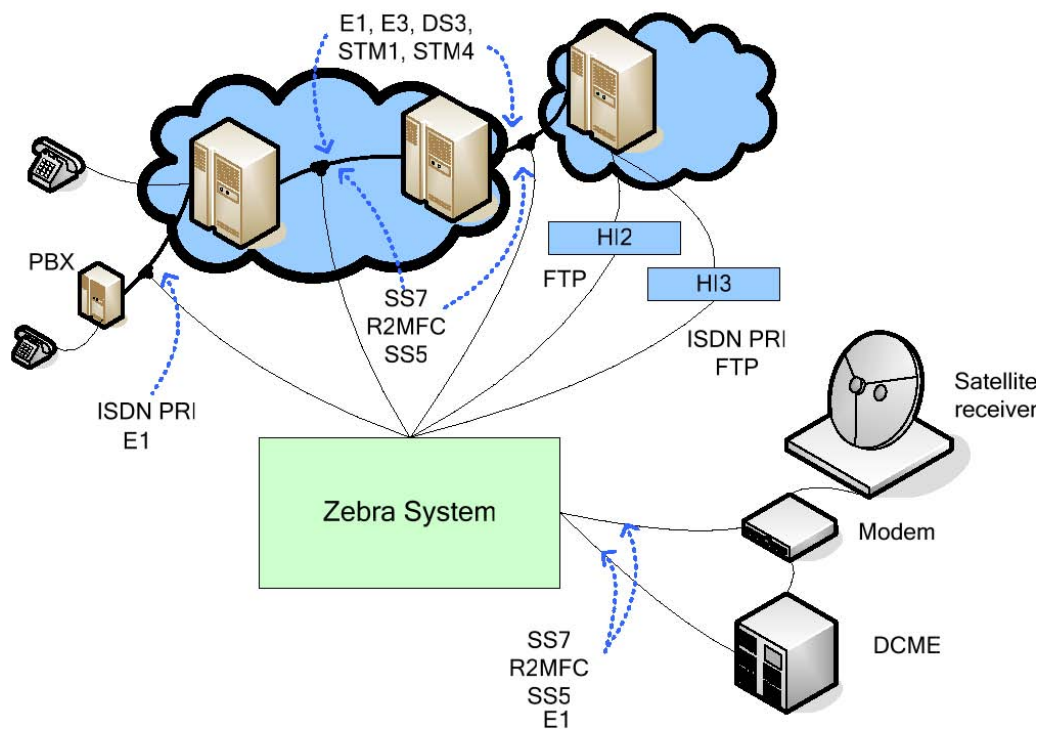


Figure 1. System overview

System overview

Figure 1 shows how the Zebra system couples to the carriers of telephony networks. Active FTP and ISDN PRI protocol stacks support the ETSI LI handover interfaces 2 and 3 for circuit and packet switched interceptions. Passive SS7, R2MFC and SS5 protocol stacks support passive monitoring between switches in a carrier network, as well as between the gateway switches. The same passive protocol stacks support interception of satellite streams. A passive ISDN stack supports trunk-side interception of PBX traffic.

The support for these interfaces and protocols allow the Zebra system to be applied to any type of monitoring in the carrier network, including PSTN and PLMN networks.

The Zebra system can capture intercepts in the following modes:

- Passively – the system connects passively to carriers or bearers between switches. Hi-Z buffers hide the Zebra system from the monitored network. No additional load is placed on the monitored network. Sessions on the monitored carriers/bearers are detected by protocol analysis or VOX activity. The system can be configured to record all traffic on the monitored carriers/bearers.
- Actively/LI – The system connects actively to the ETSI Lawful Interception handover interfaces 2 and 3 of one or more switches. A marking terminal is used to mark targets in the monitored network. The switches of the monitored network select monitored sessions based on the marked targets. The switches make calls to the Zebra system over ETSI LI HI3 containing the content of the circuit switched monitored sessions and push files containing the content of packet switched monitored sessions to a file server of the Zebra system. Intercept related information is sent to the Zebra system by switches of the monitored network over ETSI LI HI2.

Passive monitoring is typically used for large scale intelligence gathering while active monitoring/LI is mainly used for law enforcement. A Zebra system can be configured to support both actively and passively monitored interfaces in one system.

Passive monitoring

The Zebra system is a very powerful passive monitoring system. Figure 2 shows the configuration of a passive Zebra system (coupling to monitored carriers not shown) with the following capabilities:

1. Connect to 384 bi-directional E1 carriers.
2. Record every session on every channel.
3. Store all intercepts for 7 days.
4. Demodulate all fax and internet sessions.

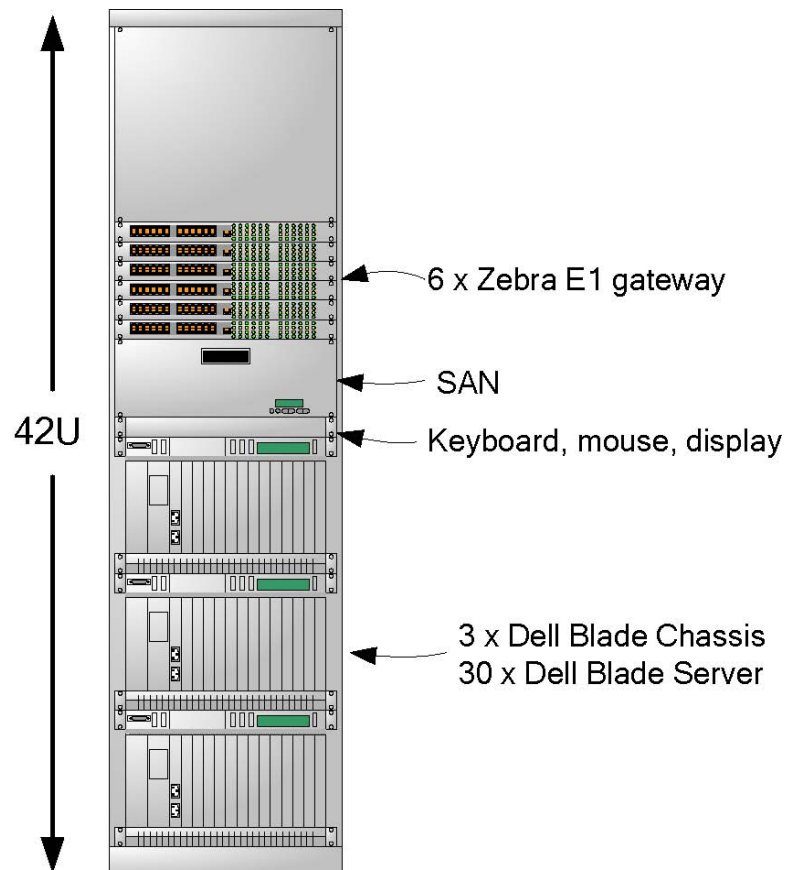


Figure 2. 384 x E1 passive monitoring system

Such a system is capable of monitoring any configuration of protocols on its input carriers, including: SS7 ISUP and TUP, SS5, R2MFC. When no signaling is available recordings can be triggered on VOX. Future versions of the system will support H.323, SIP and other packet protocols. These protocols are normally transmitted on $n \times 64$ kbps hyper channels, as well as unstructured PDH and SDH/SONET carriers. A system can support a mixture of PDH and SDH/SONET interfaces, e.g.: E1 and STM4.

The philosophy of the Zebra passive monitoring system can be summarized as: store everything, filter for known targets, and search the past for new targets.

Active monitoring

The Zebra system supports ETSI LI handover interfaces 1 and 2 as specified in ETSI TS 101 671 V2.13.1 (2006-01).

The Zebra enhanced user station will support user access to all LI meta data by 2007Q1.

Zebra Gateway



Figure 3. Zebra 128 E1/T1 gateway

The Zebra system connects to monitored networks by means of the Zebra gateway. The Zebra gateway is used to extract monitored TDM traffic and send it to processing servers of a switched local area network. This approach has a number of advantages:

1. Supports all types of channels – the Zebra system can process any combination of individual E0 (64 kbps) TDM channels, $n \times 64$ kbps hyper channels and unstructured primary rate (1.544/2 Mbps) streams.
2. Unlimited scalability – the Zebra gateway sends the contents of each monitored stream to the server requesting it. This allows the monitored traffic to be fanned out to as many servers as required for the load.
3. Density – the Zebra E1 gateway couples 128 E1 inputs in each 1U 19" rack module. This helps to reduce the footprint of a monitoring system significantly. For example, Figure 2 shows a system capable of storing and processing 100% of the traffic on 384 bi-directional E1 streams in a single 19" cabinet.

The Zebra E1/T1 gateway supports long haul and short haul termination (down to -45 dB) at 120 Ω , 100 Ω and 75 Ω .

The Zebra 128 \times E1/T1 gateway is currently available. A gateway for SDH STM-1 and STM-4 as well as E3/DS3 will be available in 2007Q1. Both E1/T1 and SDH/E3/DS3 gateways can be used in the same system.

See reference [2] for more details.

Coupling

The Zebra system can couple actively or passively to monitored networks.

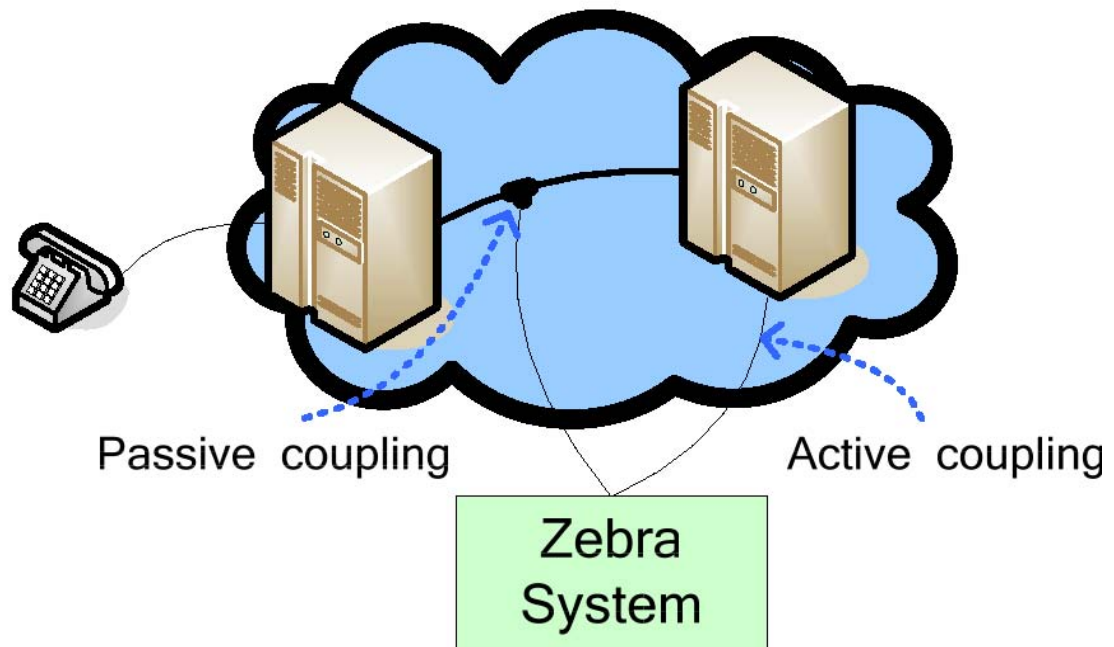


Figure 4. Coupling

Passive coupling is used for passive trunk monitoring applications and is invisible to the monitored network. No network resources are consumed by the passive monitoring of carriers.

Active coupling is typically used for ETSI LI monitoring. The network actively couples with the monitoring equipment and makes monitoring calls to the monitoring equipment. Monitored network resources are required for making the observed calls to the monitor centre.

The management of large amounts of carrier cable can be a challenge, especially in large passive monitoring systems. We offer a modular coupling system that supports the connectivity management of large numbers of monitored carriers in conjunction with optional high impedance buffering (Hi-Z) and LED indication of the status of passively monitored carriers. One coupling frame is required for each Zebra E1 gateway to connect to 128 E1 inputs (64 bi-directional).

Figure 5 shows a Zebra coupling frame for 128 twisted pairs. This coupling frame occupies 9U rack space.

Hi-Z buffering

We offer an optional hi-z buffer with the Zebra coupling frame (Figure 5). The Hi-Z buffer module consists of a single printed circuit board that mounts behind the coupling board. It has a smaller profile than the coupling board and, therefore, consumes no additional rack space.

The Zebra Hi-Z buffer ensures that any signal flowing back to the monitored network is at least 20 dB attenuated and, therefore, prevents interference with the monitored carriers. Hi-Z buffering is used in passive monitoring applications where the Zebra system T's off live monitored carriers between switches (Figure 4, passive coupling).

Another application of the Hi-Z buffer is to split an E1 input off to multiple devices, for example, redundant gateways, protocol analyzers, etc.

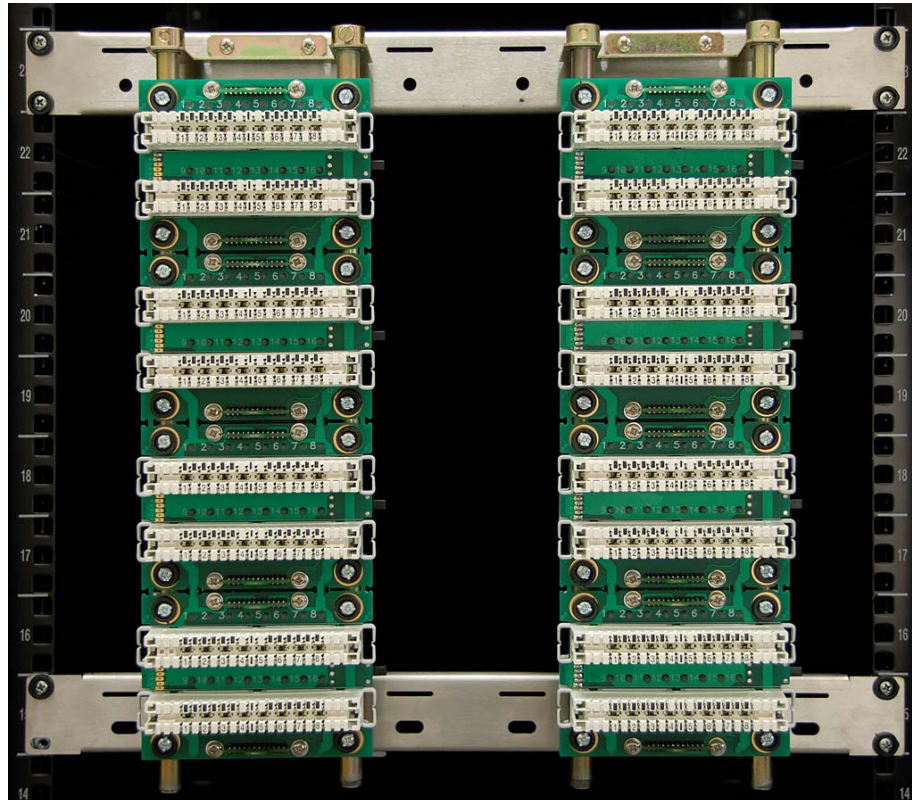


Figure 5. Carrier coupling frame for twisted pair

Access control

The configuration and intercepts stored in the Zebra system are only accessible to authorized users of the Zebra system.

User workstation

We currently offers a basic user station for filtering and browsing stored intercepts, playing audio and viewing fax/modem intercepts.

The Zebra enhanced user station that will offer sophisticated filtering and searching, playback and visualization of content, as well as the viewing of fax/Internet sessions, will become available by 2007Q1. The Zebra enhanced user station is also designed with integrated link/network analysis to assist investigators in the visualization of associations between targets.

Administration workstation

The Zebra admin workstation supports the following functions:

- User management – the administrator can create and manage the users of the system
- Interception management – the configuration of intercepted carriers, including machine assisted SS7 CIC mapping and the automatic classification of SS5, SS7 signaling and SS7 audio channels
- Signal and signaling analysis – allows the administrator to view signaling messages, listen in real-time to channels, manually record channels and visualize the content of recordings
- Health monitoring

Migration between Zebra deployment units

Modern interception systems are often geographically distributed. The Zebra system supports the migration of intercepts between geographically distributed Zebra deployment units. A set of filters can be configured to determine which intercepts are migrated.

Migration filters select intercepts based on telephone numbers and content type (for example, voice, fax and data).

It is possible to configure remote deployment units to pre-process intercepts before migration, for example, compression of voice recordings or demodulation and decoding of fax and internet intercepts. By configuring migration filters to migrate processed intercepts more information can be migrated over a WAN link.

Compression

Intercepts are stored at the original compression rate (e.g.: G.711 A-law or μ -law). Many processes, like fax/modem demodulation and speaker identification, require audio in the original format. Voice intercepts can be compressed:

1. when migrated between Zebra deployment units, or
2. when stored for a configurable period of time.

Any codec available for the Linux system can be integrated with the Zebra system. The following codecs are available by default and free of licensing constraints:

1. G.711 A-law and μ -law.
2. Speex 5 kbps – 15 kbps.

The following table lists the available code rates for Speex that are supported by the Zebra system. Field tests indicate that 8 kbps provide acceptable quality for most intelligence applications.

Speex codec quality vs bit rate		
Bit-rate (bps)	mflops	Quality/description
2,150	6	Vocoder (mostly for comfort noise)
5,950	9	Very noticeable artifacts/noise, good intelligibility
8,000	10	Artifacts/noise sometimes noticeable
11,000	14	Artifacts usually noticeable only with headphones
15,000	11	Need good headphones to tell the difference
18,200	17.5	Hard to tell the difference even with good headphones
24,600	14.5	Completely transparent for voice, good quality music
3,950	10.5	Very noticeable artifacts/noise, good intelligibility

Fax/Internet processing

The VASTech Zebra system offers integrated fax/modem processing. Protocols supported by integrated demodulator are:

- Full V.90 modem decoding
- All lower modem speeds and protocols
- Group 3 and Group 4 Fax
- All fax speeds and protocols up to and including high-speed V.34
- ISDN BRI – 64 Kbps
- Other Capabilities:
 - V.42 error correction
 - V.42bis compression
 - V.14 async-to-sync conversion
 - STAC Electronic LZS
 - Van Jacobson
 - Microsoft PPC
- Email and internet sessions
 - Decodes PPP, TCP, UDP, HTTP, POP3, SMTP, IMAP, NNTP, IRC, TELNET, FTP, VoIP H.323, ICQ, AOL IM, Yahoo IM, MSN Messenger and many other internet protocols and services

Integration with 3rd party tools

We can offer integration with a number of 3rd party tools, for example,

- Document – offers powerful indexing and searching facilities on documents
- Visual link – offers advanced link analysis capabilities

An integration API is available for integrating other applications with the Zebra system.

Scalability

The system can be seamlessly scaled up as follows:

- 128 E1 inputs (64 bi-directional) per E1 gateway
- Up to 400 bi-directional E1s in each deployment unit
- Multiple deployment units combine into one or more data centers, each with the capacity to store, process and make available to user intercepts from more than 5000 E1s
- Network storage systems – commercial SAN storage is used. This allows the system to be scaled up as required. We currently use the following storage units
 - 1U 19" rack module – over 10 million compressed call minutes capacity
 - 4U 19" rack module – over 50 million compressed call minutes capacity

Any combination of these units can be configured in a Zebra system

Redundancy

Figure 6 shows a Zebra system capable of processing and storing 64 bi-directional E1s. It shows the basic hardware building blocks:

- Zebra gateway – redundant power supply: 240V AC and -48V DC
- Nexsan SAN storage unit – supports redundant power, cooling, fiber channel connections, storage processors (in the case of the 4U 40 TB model). Hard disk drives are hot swappable and configured in RAID 10 arrays for Zebra systems.
- The Dell blade server chassis can be configured with redundant power supplies, fan modules, Ethernet switch modules and fiber channel switch modules. Power supply and fan units are hot swappable.

- Dell blade servers can be configured with two Ethernet ports and two fiber channel ports



Figure 6. Zebra hardware

Roadmap

Our development laboratory is constantly adding new functionality to the Zebra system. The following major features are planned for 2007Q1:

- Zebra enhanced user station – will provide sophisticated filtering, support of the metadata of new protocols and ETSI LI, as well as integrated link analysis
- Comprehensive support of ETSI LI HI2 and HI3 compliant with ETSI TS ETSI TS 101 671 V2.13.1 (2006-01)
- STM1/STM4 gateway – the STM1/STM4 gateway will support 4 STM1 or 1 STM4 interfaces. It will also support up to 4 E3 or DS3 inputs. Any combination of multiplexed channels will be supported on the SDH streams, including: M13, E3 and ITU-T G.747. In addition unstructured streams will be supported at primary rate, 32Mbps (E3) and 42Mbps (DS3)
- VoIP – H.323 and SIP will be supported
- Speaker identification – support for text independent speaker identification is planned



If you would like further Information about ELAMAN,
or would like to discuss a specific requirement or project, please contact us at:

Elaman GmbH
German Security Solutions
Seitzstr. 23
80538 Munich
Germany

Tel: +49-89-24 20 91 80
Fax: +49-89-24 20 91 81
info@elaman.de
www.elaman.de