

WHITE PAPER

HSL VIDEOBAR DIODE

Technical Brief: Security Architecture

TABLE OF CONTENTS

Overview	3
Understanding Videobars	3
Security Threats	4
Microphone and Speaker Exploits	5
Camera Exploits	8
Interface Attacks	9
Attacking Onboard Storage	9
Attacking Internal Memory	10
HSL Videobar Diode	11
Videobar Diode Architecture	12
Unidirectional Data Flow	13
Physical Disconnection	13
Device Emulation	13
Host Emulator and Interface Routing	14
USB Conditioner and Tamper-Resistant Reset	15
Audio Security Channels	16
Connect/Disconnect Relays and Manual Access Control	17
Conclusion	18

OVERVIEW

HSL's Videobar Diode addresses critical security vulnerabilities inherent in video/sound bars, particularly for organizations managing multiple air-gapped networks at different classification levels. This solution enables the secure use of these devices while protecting against information leakage between isolated networks.

UNDERSTANDING VIDEOBARS

Videobars are all-in-one conferencing devices combining cameras (often 4K with wide-angle lenses), beamforming microphones, and high-quality speakers in a single unit. Soundbars include microphones and speakers without cameras. These devices are typically mounted near displays in meeting rooms and executive offices.

Some devices include only some of these interfaces (such as a webcam with only a camera and microphone, but no speaker). While this subset of peripherals may not fit the technical definition of a videobar or soundbar, they use much of the same technology and therefore present many of the same security risks.

SECURITY THREATS

While convenient, videobars with internal clients, Wi-Fi, Ethernet, or Bluetooth connectivity pose substantial security risks. These built-in computing platforms can execute applications, record audio, and store data without third-party security oversight, making them particularly dangerous when shared across air-gapped networks.

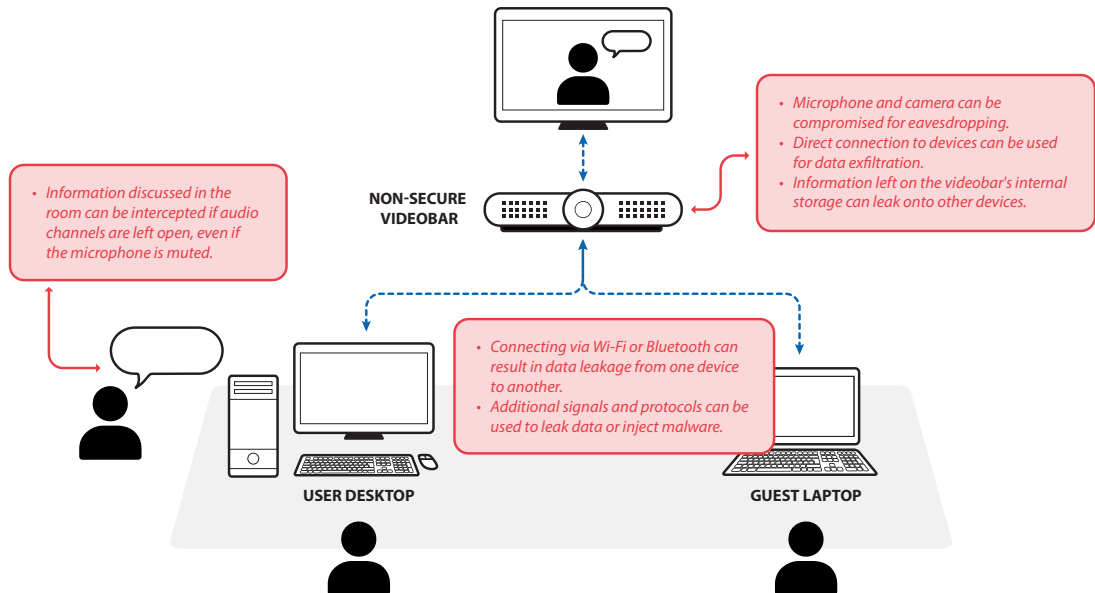


Figure 1. A diagram of a possible conference room setting and its potential vulnerabilities

MICROPHONE AND SPEAKER EXPLOITS

Videobars connect to network infrastructure and rely on embedded operating systems that are susceptible to both remote and physical compromise. Once an attacker gains access through firmware vulnerabilities, unpatched software, or social engineering attacks on network credentials, they can activate the camera and microphone array independently of the device's intended operation. Unlike visible indicator lights that users might monitor, these compromise scenarios can operate covertly through firmware manipulation that disables status LEDs while maintaining full sensor functionality.

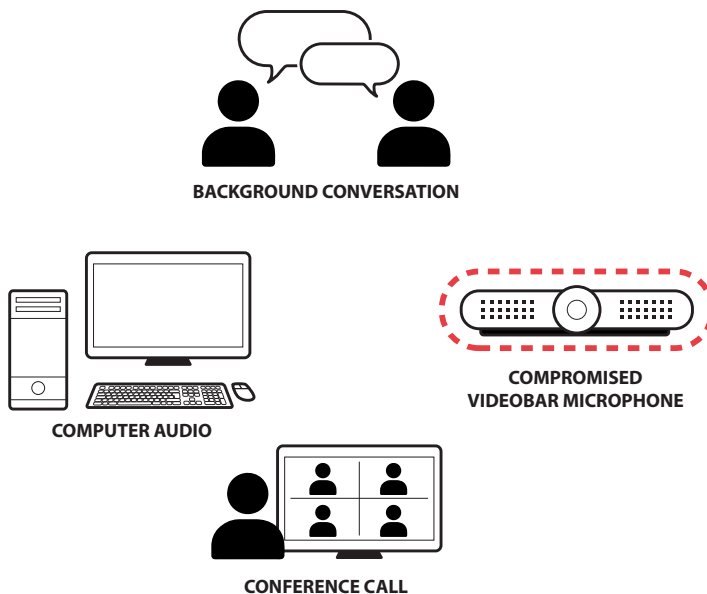


Figure 2. A compromised videobar can be used to eavesdrop on conversations.

Microphone Eavesdropping

One of the most direct security risks of connecting to a videobar is a compromised or unattended microphone. Attackers can enumerate the USB device and covertly open an audio input stream, compromising the videobar's microphone without needing physical access to it. When connected to a KVM switch, a compromised host computer may use the mic to keep an audio channel open even while the user is working on another host. This allows attackers to continually listen to and record conversations, audio from other computers, and any other potentially sensitive audio information.

Speaker-to-Microphone Conversion

Even if the videobar's microphone is muted or disabled, the mechanical functions of speakers can create an often-overlooked vulnerability. Speakers convert electrical signals into acoustic vibrations. However, this function can also be applied in reverse: acoustic vibrations applied to a speaker can generate electrical signals. An attacker with access to the audio output circuitry can essentially reverse-engineer the speaker into a functional microphone, albeit with reduced sensitivity and frequency response compared to purpose-built microphone elements.

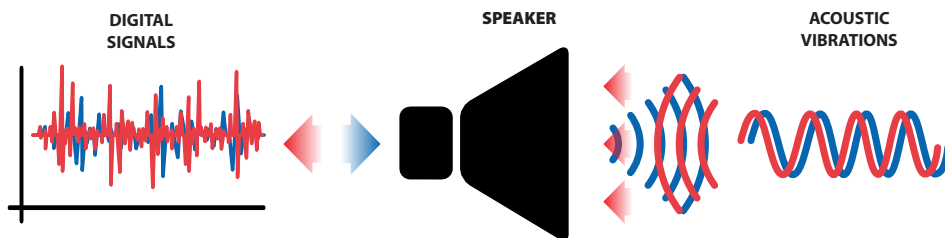


Figure 3. A compromised speaker can be used as a microphone.

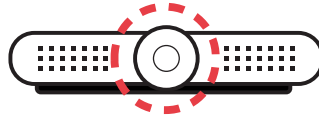
This type of attack is particularly insidious because organizations frequently rely on the apparent “safety” of simply muting the microphone when discussing sensitive information. Meanwhile, the speaker drivers remain electrically connected to the videobar's processing chain, providing an alternative pathway for audio capture. While the recovered audio quality may be inferior to a dedicated microphone, speech remains intelligible at typical conference room volumes, and sensitive discussions become vulnerable to extraction.

High-Frequency Data Transmission

An attacker can modulate sensitive data onto ultrasonic carriers, transmit through compromised speakers, and receive via strategically positioned microphones in mobile devices or concealed surveillance equipment.

This attack method is difficult to detect through conventional security monitoring because the transmissions are inaudible to the human ear and may not trigger detection systems calibrated for audible frequencies. While the amount of data that can be sent over audio is modest compared to conventional network exfiltration, it is still enough to transmit encryption keys, authentication credentials, or compressed documents.

CAMERA EXPLOITS



**VIDEOBAR WITH
A COMPROMISED CAMERA**



**USER
CREDENTIALS**



**SENSITIVE
DOCUMENTS**



**PERSONNEL
IDENTITIES**

Figure 4. A compromised camera can be used to capture sensitive visual information.

A videobar's camera has the same vulnerabilities as its speakers and microphone, with the added risk of exposing visual information. Just as with the microphone, an attacker can enumerate the videobar's camera and open a video stream in the background, capturing anything in the camera's field of view. Captured video can expose documents on display, the content of computer screens, and even the identities and credentials of personnel in the room.

INTERFACE ATTACKS

Many enterprise-grade videobars increase their functionality through user-friendly integrated operating systems and onboard storage, and each of these capabilities introduces significant additional risk in secure environments. A videobar running a full operating system may support interactive features that allow connected computers to share input control, transfer files, or access peripheral interfaces through the videobar as an intermediary. A compromised computer could exploit the shared interface layer to probe, infiltrate, or inject malicious code into a separate secure machine connected to the same videobar.

ATTACKING ONBOARD STORAGE

Onboard storage compounds the risk of data exfiltration. Videobars that cache call recordings, configuration data, or session content may retain fragments of sensitive information long after a meeting concludes and participants have disconnected. An intruder who gains remote access to the file system can potentially recover that information, gleaning authentication credentials cached during device pairing or documents that were shared during a presentation. Unlike a dedicated computer, videobar storage is typically opaque to IT and security administrators, operates under proprietary firmware management, and may not be covered by existing data handling policies.

ATTACKING INTERNAL MEMORY

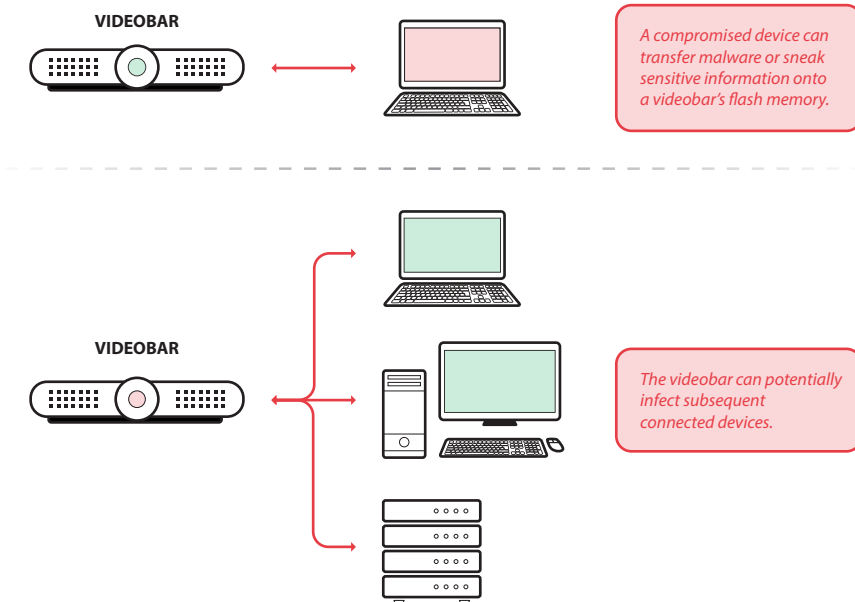


Figure 5. A videobar's internal flash memory can be used to spread malware or smuggle information.

Attackers can use a videobar's internal flash memory to leak data or inject malware onto connected devices. They can also recover cached call recordings or recover credentials from a videobar's onboard storage. A compromised computer can exploit the shared interfaces of a videobar's integrated OS to access separate connected devices. If the videobar is compromised, every device connected to it can be compromised as well.

HSL VIDEOBAR DIODE

High Sec Labs' Videobar Diode protects against the most common security risks that face any meeting room. The diode operates as a gateway between the videobar and the connected peripheral devices, keeping audio and video channels closed until the user manually opens them. Rather than relying on software-based security measures that can be hacked or subverted, the Videobar Diode implements hardware-based protection, preventing data leakage and unauthorized infiltration.

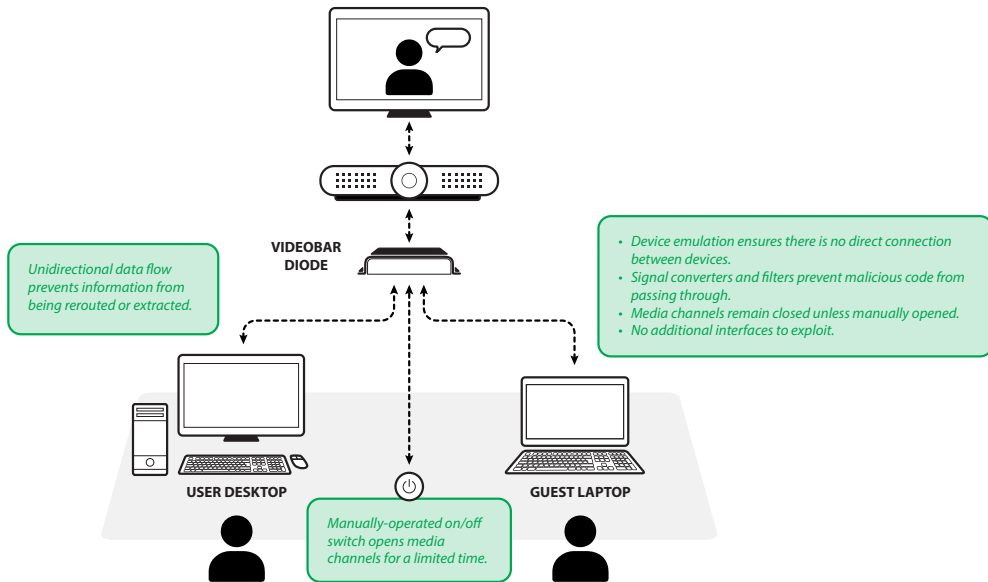


Figure 6. Integrating an HSL Videobar Diode protects against security risks.

VIDEOBAR DIODE ARCHITECTURE

The Videobar Diode addresses threats by employing multiple internal security features:

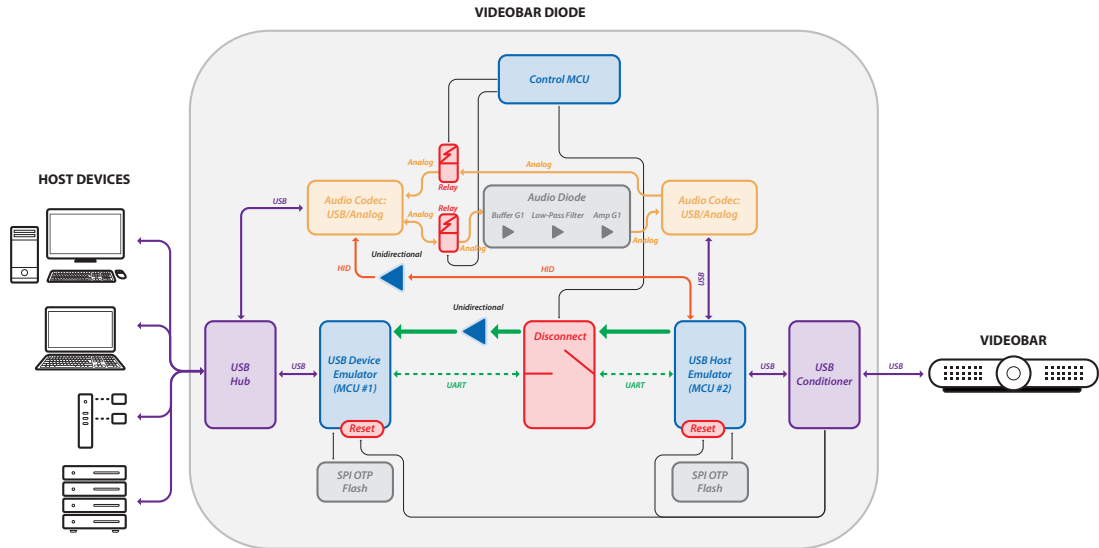


Figure 7. Diagram of the Videobar Diode's internal architecture.

UNIDIRECTIONAL DATA FLOW

Traditional videobars allow bidirectional communication between connected devices and the conferencing system, which creates the risk of device exploitation and data exfiltration. Enforcing unidirectional data flow allows information to travel in only the required direction, providing no return path for reverse transmission. Even if the videobar is compromised, an attacker who attempts to extract data from connected devices or establish covert communication channels encounters a hardware barrier that cannot be bypassed through software exploitation.

PHYSICAL DISCONNECTION

The Videobar Diode mitigates the risk of eavesdropping by keeping the audio and video channels closed by default, physically disconnecting the videobar from the connected devices until it is opened manually by a user. Rather than relying on the supposed safety of muting the microphone, this makes it impossible for the videobar's microphone to send audio while the channel is closed. To prevent the channels from being accidentally left open, the Videobar Diode automatically closes them again after a set time.

DEVICE EMULATION

Rather than directly connecting the videobar to any devices, the Diode uses emulation technology to present itself to the peripheral devices as the videobar itself and vice versa. This allows it to receive information from both ends and filter any unwanted signals before transmitting, keeping the videobar and peripherals separate at all times.

HOST EMULATOR AND INTERFACE ROUTING

The host emulator, implemented on a dedicated microcontroller (MCU #2), serves as the Diode's interface with the videobar itself. Connecting via a USB conditioner, it presents itself to the videobar as a standard host PC, allowing the videobar to operate normally without recognizing that it is connected to a security device rather than a conventional computer. Because the videobar believes it is communicating with a trusted endpoint, it behaves predictably and exposes its full interface set, which the host emulator then parses and routes.

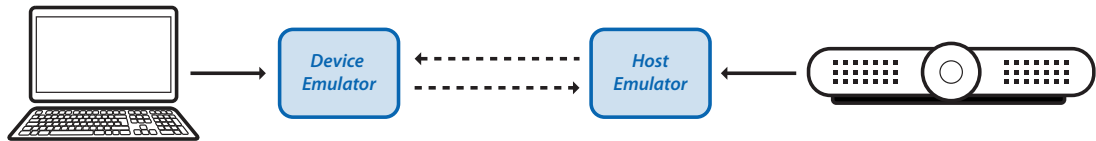


Figure 8. The videobar only communicates with the internal host emulator, never the host computer itself.

Each interface is handled according to a strict routing policy. Camera output is forwarded via a dedicated parallel data line to the device emulator, maintaining the video signal on its own isolated pathway throughout its transit through the Diode. Speaker and microphone signals are each routed to separate, dedicated USB-to-analog codecs, beginning the signal conversion process that forms the foundation of the audio security architecture. Critically, any interface that does not conform to the expected profile or cannot be positively identified is immediately terminated.

USB CONDITIONER AND TAMPER-RESISTANT RESET

The USB conditioner detects the connection state of the videobar, and any connection or disconnection triggers a simultaneous hardware reset of both the host emulator and the device emulator MCUs. This ensures that neither MCU can accumulate data that can be leaked across connections.

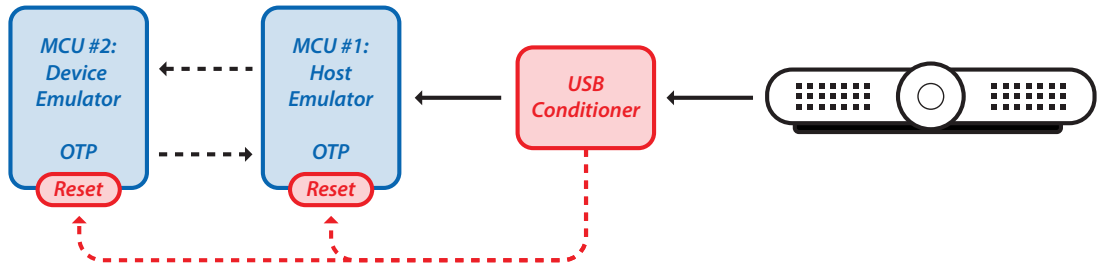


Figure 9. The USB conditioner resets the host emulator and device emulator as soon as the videobar is connected.

Both MCUs are programmed using one-time programmable (OTP) processes, meaning the firmware image written during manufacturing is permanently fixed and cannot be altered through software, remote access, or physical manipulation after the fact. Every reset loads an identical, verified image of the original firmware. An attacker who somehow managed to tamper with an MCU during a session would find their changes completely discarded the moment the videobar is disconnected.

AUDIO SECURITY CHANNELS

The audio security channels address the threat of unwanted data carried on digital signals. Both the microphone and speaker pathways are converted from USB digital audio to analog and back to USB digital. The signal that emerges from this chain of conversion carries only the acoustic waveforms that survived the analog stage; any hidden data embedded in the original digital stream is destroyed in the process.

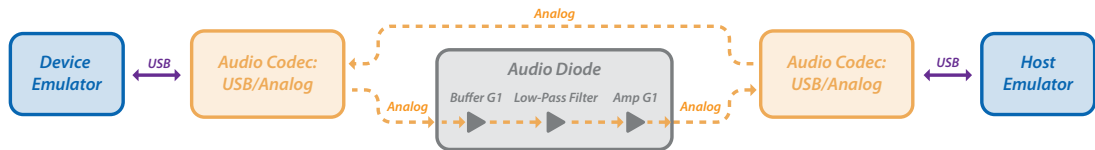


Figure 10. Only analog audio signals travel between the host and device emulators.

While in analog, audio passes through a low-pass filter, which removes any signals too high for the human ear to hear. This directly eliminates the risk of attacks from ultrasonic channels. The speaker pathway carries additional protection: Class D amplifiers impose a strict unidirectional drive characteristic on the speaker transducer, ensuring the speakers can output sound but cannot function as a microphone.

CONNECT/DISCONNECT RELAYS AND MANUAL ACCESS CONTROL

The connect/disconnect relays provide a physical layer of isolation that operates entirely independently of the audio processing subsystems. Controlled exclusively by a dedicated MCU that is separate from any other component in the Diode, these relays physically sever the analog audio lines when audio transmission is not authorized. When the relays are open, there is no electrical connection between the USB-to-analog converters, making data transfer between them physically impossible regardless of what the converters themselves are doing. This hardware-enforced separation cannot be bypassed through software means, firmware manipulation, or signal injection, as the break in the circuit is absolute.

By default, all relays remain closed, meaning all audio channels are physically disconnected. The relays must be opened manually, and they are only open during a timed window. This window defaults to 15 minutes but can be configured for up to 60 minutes depending on operational requirements. When the timer expires, the relays close automatically without any required user action. This design directly addresses the human factor: even if a user leaves a meeting without remembering to close the relays, the Diode closes as soon as time runs out.

CONCLUSION

Modern videobars are built for convenience rather than security, which leads to risks that must be considered when installing one in a secure environment. Microphones and cameras that can be activated covertly, speakers that can be reverse-purposed for audio capture, wireless interfaces that create unmonitored data pathways, digital signals that can carry embedded payloads, operating systems that can bridge otherwise-segregated networks, and onboard storage that retains sensitive residue across sessions: each of these represents a category of risk that software-based solutions are not adequate to address.

The HSL Secure Videobar Diode addresses the vulnerabilities of a videobar by applying a consistent set of security principles at the hardware level. By reducing the interfaces to only the camera, microphone, and speakers, only the signals necessary for conferencing can pass through the Diode's processing chain. The principle of physical separation is realized through dedicated, isolated pathways for each signal type, hardware relays that create absolute breaks in electrical continuity, and independent MCUs that control individual functions without any communication pathway to other subsystems. Unidirectional data flow eliminates the bidirectional communication channels that can allow for data extraction or cross-talk between devices. And signal converters filter out any unwanted data hidden in the audio signals. These measures do not merely reduce the risk of attack; they render entire categories of attack physically impossible.

www.highseclabs.com

High Sec Labs (HSL) develops high-quality cyber-defense solutions in the field of network and peripheral isolation for protecting national assets and infrastructure.

The company, headquartered in Or Akiva, Israel, was founded in 2008 and has a second manufacturing site in the United States.

High Sec Lab's roots are deeply embedded in the defense and commercial industries developing cyber protection solutions. Among its customers are some of the world's leading governments and defense organizations as well as commercial companies such as banks, healthcare providers, and national infrastructure companies.



© 2026 HighSecLabs Ltd. All rights reserved. All trade names are trademarks or registered trademarks of respective manufacturers listed. Specifications are subjected to change without prior notice. Patents: www.highseclabs.com/patents/. HLT39282 Rev 1.0

