SCIFs - State of the Art and Future Considerations

diyscif

May25, 2021

Abstract

This paper will examine the different constructive and technical measures employed by governmental, non-governmental, and corporate actors to protect their secret communications in the physical realm. It will define the target ideal state of "information security", identify information sources that must be controlled to reach this state, set up quantitative limits on these information sources discoverable externally, provide example attack techniques, and propose various passive and active countermeasures to reach these limits and defend against these attacks. Finally it will present an example module that achieves these specifications measurably.

Note, this paper is limited in scope to constructive and technical measures and does not focus on IT or organisational security measures, like encryption, security-related review/monitoring of employees, and classification levels. It also does not dwell on specific countries bureaucratic protocols, but instead aims to present a unified picture of the global state of the art.

Contents

1 What is a SCIF?

Sensitive compartmented information facility (SCIF) is a term used by U.S. military and intelligence organizations to describe secure, enclosed areas designated for handling sensitive, classified information. They come in many different shapes and sizes, each designed for a specific mission demand. They can be installed permanently in buildings, designed as mobile units, set up temporarily, and even built aboard aircraft and naval vessels. What unites these different variants is the common goal of creating a designated space with rigorous security practices that thwarts all relevant passive outside observers and active attackers.

SCIFs are by no means exclusive to U.S. government institutions. They are used internationally by a wide variety of actors, from other governments to international organizations to corporations and NGOs. The term has become the most commonly used and will also be used in this paper to refer to structures specifically built to protect information processed inside them.

Most countries keep their specifications for these secure facilities secret. The United States, however, have published comprehensive information on their engineering practices under Intelligence Community Directive (ICD) 705 “Sensitive Compartmented Information Facilities” and its associated technical specifications. In this paper, ICD 705 will be supplemented by private contractors’ informational material, documents released under the Freedom of Information Act (FOIA), leaked documents, and scientific literature to create a comprehensive picture of the current state of the art and give an outlook on future improvements.

2 Information Security - Ideal State and Practical Tradeoffs

A communication link or room is considered secure if information travelling through it cannot be intercepted by unauthorized parties. This is a theoretical ideal state that *cannot* be reached. However, one can employ various countermeasures to secure a communication link or room to such a degree that it can be practically considered as secure against an attacker with certain resources.

Both defenders and attackers are constrained by limited resources. Viewing attack techniques from a resource perspective allows a defender to determine whether they are “in scope”, given the threat level, and if countermeasures must be deployed against them. Resources are best expressed in terms of cost, time, and technical skill required. Taking into account these parameters, the defender is able to develop a mission-specific threat model that allows him to employ his *limited* resources effectively to defend against the most likely and serious attacks.

The IC Tech Spec-for ICD/ICS 705 (Office of the National Counterintelligence Executive 2012, p. 20) bases its threat modelling on country-level threat ratings derived from the Department of State’s (DoS) Security Environment Threat List (SETL). Specifically, the ICD establishes appropriate construction criteria based on the host country’s SETL technical threat rating. A country-level view is most useful to government organizations, however, other actors, especially corporate actors, may have to rely on different factors to determine threat level. Other possible criteria from which to derive a threat level include value of information handled and named/identified threats.

The fundamental assumption for threat modelling is that it is highly unlikely for an attacker to expend more resources to carry out an attack than the objective value of the attainable information.

3 Passive Outside Observer

There are various information sources that can leak from the secure facility and be intercepted. These can generally be grouped into visual, acoustic, and electromagnetic information source leaks. A passive observer can use different sensors, like telescopic cameras, directional microphones, and high-sensitivity anntenae, to capture and analyze these information source leaks and draw conclusions about the sensitive information processed. A covert location outside the SCIF perimeter is almost impossible to detect and counteract. Therefore, information leaks must be prevented at the source.

3.1 Visual

Visual leaks are any direct view of sensitive information or surface whose reverberations can be captured with a laser and then translated into usable information. When speaking, glass panes or mirrors in a room are set into vibration. When there is visual insight into the room (e.g. from the neighboring building), a laser beam can be directed onto these reflecting surfaces and the reflected beam can be received again. The reflected beam is modulated by the oscillations. By demodulation, the conversation can be made audible (Wolfsperger 2008, p. 463). Direct views can also provide valuable insights into information processed and even serve as a basis for other attacks, like lip-reading of sensitive discussions.

Barring holes in the SCIF perimeter, like propped-open doors, visual leaks can only be captured through windows.

Figure 1: Laser Microphone Sptectra M+

Capture Technique	Cost	Time	Technical Skill Required
Direct View	medium	low	low
Lip Reading	medium	low	medium
Reverberations Captured by Laser	high	low	medium

3.2 Acoustic

Acoustic leaks are sound waves that escape the enclosed areas, either directly or through structure-borne sound transmission. These can be captured with directional microphones, contact microphones, and well placed conventional microphones. An example of such an advantageous placement would be in an unmuffled ventilation or heating duct.

Acoustic leaks provide some of the most valuable insights. Discussions, conferences, and chatter contain secrets in their purest form. Through them, an attacker doesn't only attain sensitive material, he also gains insight into underlying priorities and considerations, much more so than from a leaked document. Like Christoph Waltz's character from the 2009 Quentin Tarantino film "Inglourious Basterds" says "I love rumors! Facts can be so misleading, where rumors, true or false, are often revealing."

Figure 2: Parabolic Microphone G-PKS PRO EX

Digital sound processing software can further enhance an outside passive attackers capabilites to reconstruct, clarify, and analyze sound leaks.

Capture Technique	Cost	Time	Technical Skill Required
Directional Microphones	medium	low	low
Contact Microphones	low	medium	medium

Capture Technique	Cost	Time	Technical Skill Required
Conventional Microphones	low	medium	medium

3.3 Electromagnetic/TEMPEST

Compromising electromagnetic waves unintentionally emitted from information processing equipment, like computers, screens, and even printers are another source for information leaks. These radio or electrical signals, sounds, and vibrations can be captured with antennae, microphones, and other sensors, and allow inferences to be made about the information processed, sometimes even allowing its complete reconstruction (Liu, Samwel, Weissbart, Zhao, Lauret, Batina, Larson 2020). They can also serve as a side-channel for attacks on cryptography (Genkin, Pachmanov, Pipman, Tromer 2015). The techniques for extraction and analysis of compromising electromagnetic emanations fall under the commonly used U.S. National Security Agency codename TEMPEST (U.S. National Security Agency 1972).

These attack techniques require high technical skill to develop, however once established are easy and fast to reproduce with affordable equipment. Although execution is fast, reconnaissance, planning and setup, especially for well-protected facilities, can entail significant time expenditure.

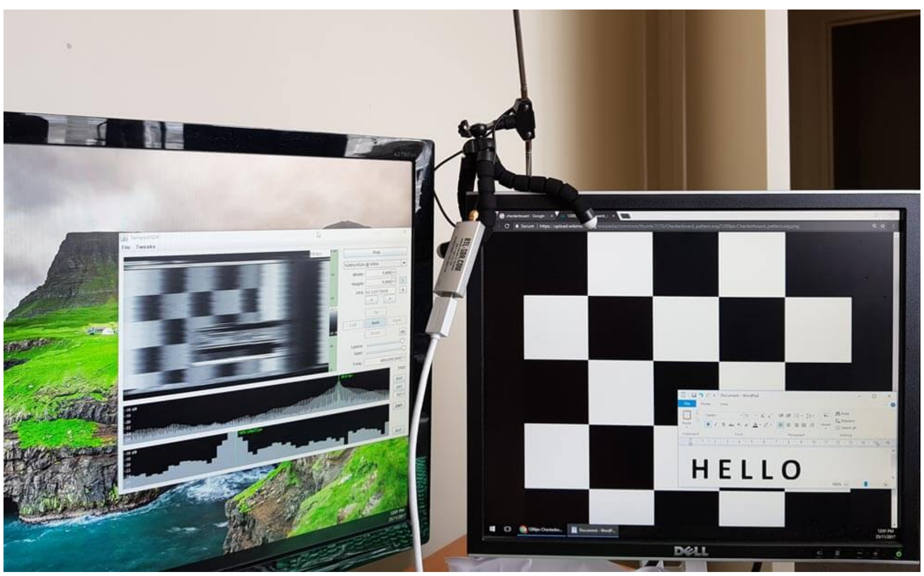


Figure 3: Display of one monitor reproduced on another using its TEMPEST emanations and a $40 software defined radio + antenna set up. RTL-SDR.com (2017)

Capture Technique	Cost	Time	Technical Skill Required
Direct Leaks	low	medium	high
Side-channel on Cryptography	low	medium	high

4 Limits

This section will set quantitative limits on information sources available to an outside passive observer. Since information source leaks must be protected at the source, it is important to know the extent of attenuation necessary to assure adequate protection.

4.1 Visual

No visual information should be accessible to an outside passive observer. Visual information source leaks are the easiest to avoid and should therefore be wholly prevented. Even observation of the entrypoint could provide insights into the comings and goings of authorized personnel and should therefore be obscured as much as possible.

4.2 Acoustic

Acoustic emissions must be reduced by at least a weighted sound reduction index of $R'_w = 52$ dB. This measure roughly corresponds to the Sound Transmission Class 50 listed in the IC Tech Spec-for ICD/ICS 705 as an enhanced rating for areas that provide for amplified conversations (Office of the National Counterintelligence Executive 2012, p. 66). We use this as a general minimum measure, because the IC Tech Spec is geared towards military and other government facilties that provide a large measure of Security in Depth (SID), meaning that only semi-trusted personnel ever get within earshot of the SCIF. Security in Depth is a “multilayered approach, which effectively employs human and other physical security measures [like fences, walls, and guarded entry gates] throughout the installation or facility to create a layered defense against potential threats” (Naval Facilities Engineering Systems Command Northwest 2012, p. 20). Additionally, SID increases the probability of detection of nefarious activity because of continuous friendly-forces presence (Office of the National Counterintelligence Executive 2012, p. 3). These conditions cannot be guaranteed for all locations, especially in the corporate realm, so we strive to compensate reduced SID with a higher degree of sound insulation. When possible, $R'_w = 52$ dB should be exceeded.

R'_w represents the resulting sound insulation between two rooms, taking into account all sound transmission paths (Tichelmann, Pfau 2000, p. 26). This explicitly includes not only transmission through dividing components, but also so-called “flank transmission” over adjoining building components. In this phenomenon sound waves cause vibrations in flanking walls and then linearly travel through them into the other room (Möser 2009, p. 254). R'$_w$ is a cummulative value calculated on the basis of the weighted sound reduction index of each component R_w (Tichelmann, Pfau 2000, p. 34).

R_w is calculated by measuring sound transmission from one test cabin into another divided by the test component. The test is carried out in one-third octave or octave steps. White noise, a random signal with equal intensity across different frequencies, with the given bandwidth is used as test sound. A frequency response curve R is thus obtained in the so-called building-acoustics frequency range between 100 Hz and 3.15 kHz. The frequency response curve R is then compared to a reference curve B in order to derive a single comparison value. In the comparison, the reference curve is shifted in 1 dB steps onto the frequency response curve until the sum of the undershoots S_U of the frequency response curve compared to the reference curve is less than 32 dB. (Möser 2009, pp. 256–257)

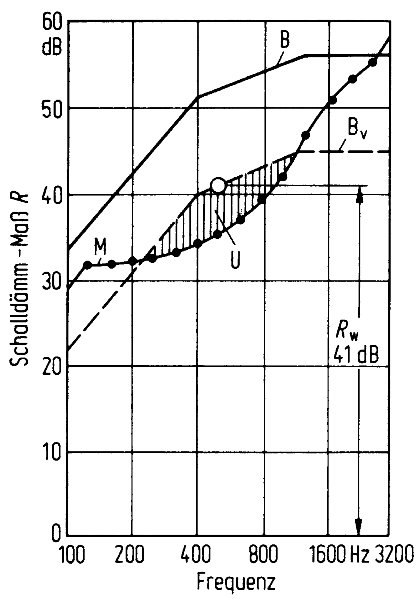


Figure 4: For the definition of the weighted sound reduction index R_w. B = Reference curve, B_v = Shifted reference curve, M = Measured values, U = Undershoots of M compared to B_v. Gösele, Schröder (2004)

From this diagram we can also see that for a R_w = 52 dB (the reference curve) the fundamental frequency of the male voice - 125 Hz - only undergoes a sound attenuation of ca. 35 dB. Given a 60 dB conversation sound-level the sound attenuation is not sufficient to protect from a close proximity attacker. Passive sound-attenuation measures should be specifically evaluated in the 125 Hz to 300 Hz range, and significantly exceed the reference curve's performance.

Airborne sound transmission via ventilation and structure-borne sound transmission via ducts, such as water and ventilation pipes, can significantly reduce sound insulation (Deutsches Institut für Normung 2018, p. 19). In some cases they can even provide direct channels for an outside observer to capture sound on (Office of the National Counterintelligence Executive 2012, p. 13). Hence, they must be treated with special attention. A mistake on a component penetrating the SCIF perimeter, like a duct or vent, can render useless all other attenuation.

4.3 Electromagnetic/TEMPEST

Electromagnetic emissions should be reduced by the values defined in National Security Specification for Shielded Enclosures NSA 94-106. This specification sets forth an attenuation for a 1 kHz - 1 MHz H (magnetic) Field of 20 dB @ 1KHz, 56 dB @ 10 kHz 90 dB @ 100 kHz, and 100 dB @ 1 MHz. For a 1 kHz - 10 MHz E (electromagnetic) Field it requires 70 dB @ 1kHz, and 100 dB at 10 kHz, 100 kHz, 1 MHz, and 10 MHz. For a 100 MHz - 10 GHz Plane Wave it also requires 100 dB attenuation.

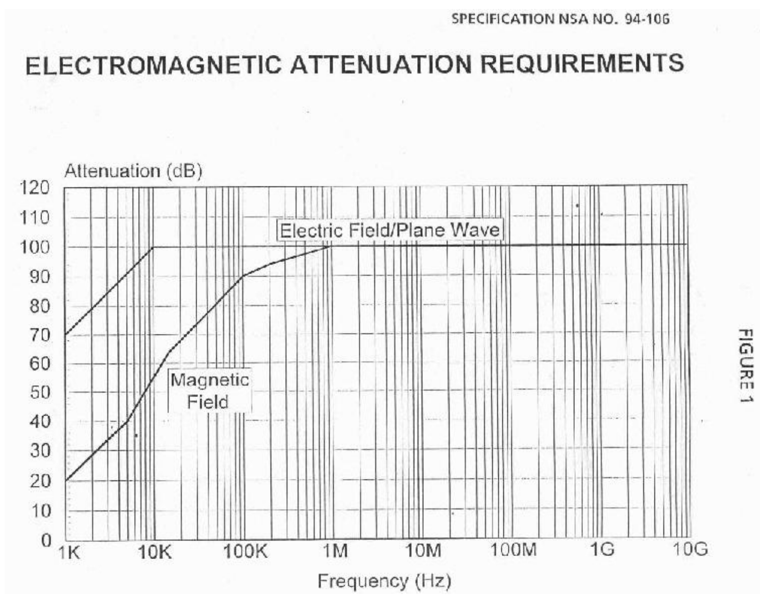


Figure 5: Electromagnetic Attenuation Requirements. U.S. National Security Agency (1994)

The field test is carried out with a parallel setup. A continuous wave source generates a wave in the range of 1 KHz to 10 GHz. Two antennae are placed, one on either side of the shielding. One antenna acts as a transmitting (TX) antenna and the other as a receiving (RX) antenna. The antennae are separated by a distance of 61 centimeters plus the wall thickness. The signal from the

RX antenna is fed back into a reciver. Attenuation levels can then be read from a spectrum analyzer. Magnetic field, electronic field, and plane wave attenuations are then measured at various specified frequencies. Attenuation tests are performed around the entire door frame, air ducts, filters and through any accessible joint or penetration. (U.S. National Security Agency 1994)

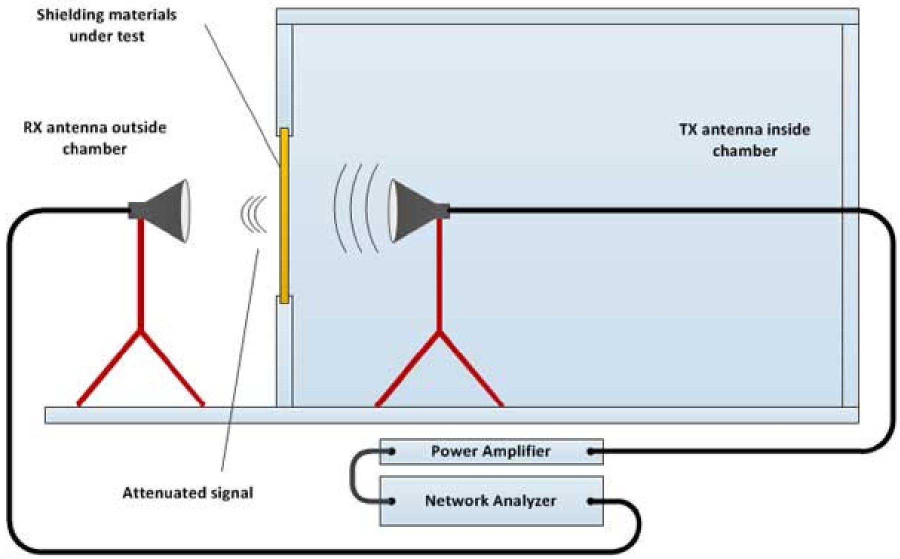


Figure 6: Test setup for NSA-94-106. EMCTEST Technologies (2018)

A RF shielding system is only as effective as its weakest component (Krieger Products 2015). Shielding material faults and gaps in the shield should be carefully avoided. These holes become more critical the higher the frequency of the shielded field (Wolfsperger 2008, pp. 292–293).

Apart from airborne electromagnetic waves, emanations can also leak from a SCIF on cables and wires. Instead of travelling through the air, unwanted signals can travel along wires out of the SCIF (Wolfsperger 2008, p. 210) inducing electromagnetic fields where they can be captured and turned into usable intelligence. With the right setup using different tools for power, data, and control connections these information source leaks can be entirely eliminated.

5 Active Attacker

Apart from passively observing information source leaks from outside the secure facility, an attacker can also actively attack the space to place sensors inside the SCIF and transmit sensitive visual, acoustic, or electromagentic information to the outside. He can also seek to weaken the passive attenuation in order to increase the information yield of passive observance.

This chapter intends to give some general ideas about possible attack vectors, not to list out specific attacks and describe their execution. New attack methods are constantly being developed and only few ever get published. Thankfully most can be prevented by sticking to the same established general countersurveillance measures and security practices.

5.1 Visual

The goal of all visual attacks is to place cameras inside the SCIF. These cameras allow an attacker to gain valuable insights into the sensitive information being handled or processed inside the enclosed area. Cameras can be inserted by someone who gains physical access to the space, inserted through HVAC ducts, or drilled through the perimeter.

Another attack avenue is taking over installed CCTV cameras. The video feed from these cameras could allow insights into the SCIF's comings and goings, and, with badly placed cameras, even into the information processed. This attack can also target the built-in cameras of information processing equiptment like laptops.

Cameras transmit video feeds to the outside using radio/electromagnetic waves or wired connections. Wired connections could be specially installed for the attack or hijack existing lines, either directly or as emanations along their unshielded exterior.

Attack Technique	Cost	Time	Technical Skill Required
Inserting Camera	low	low	medium
Hijacking Existing Camera	low	medium	high

5.2 Acoustic

An attacker may also attempt to place a microphone in the SCIF. To do this he can either physically insert a new microphone or hijack one of the built-in microphones of devices already located in the room. Acoustic information is usually most sensitive, especially in conference rooms or discussion areas.

Similar to visual attacks, avenues for placing a microphone are physical entry, HVAC ducts, and hole drilling. In order to exfiltrate information the attacker again utilizes either radio/electromagnetic waves or wired connections, existing or specially placed. Another attack is finding a weak spot in the sound attenuating shell and placing a contact microphone directly on it.

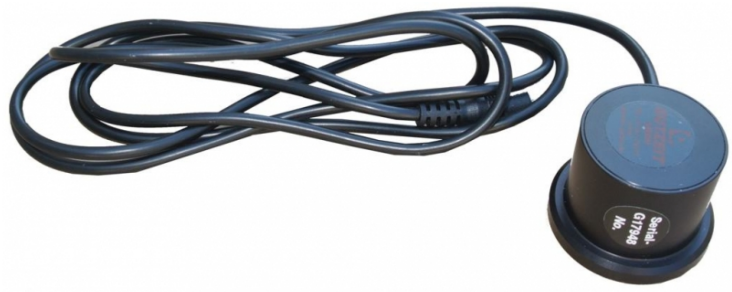


Figure 7: Contact Microphone Gutzeit GmbH

An attacker could also seek to weaken the sound attenuation measures by tampering with the sound masking, destroying insulation or purposely creating sound bridges.

Attack Technique	Cost	Time	Technical Skill Required
Mic over Existing Lines	low	medium	high
Mic over Specially Placed Lines	medium	high	high
Mic Wireless	low	low	medium
Contact Microphone on Weak Spot	low	medium	medium
Hijacking Existing Microphones	low	low	high
Weakening Sound Attenuation	medium	medium	high

5.3 Electromagnetic/TEMPEST

Instead of passively capturing TEMPEST emanations from outside the SCIF perimter, an attacker could also seek to place an antenna within the SCIF. He could then amplify the signals and thereby overpower the shielding or exfiltrate them on some other channel. He could also seek to weaken the electromagnetic shield by purposely creating holes in it or tampering with protective equipment, like power line filters.

Electromagnetic attacks are possible, but it is more likely that an attacker would place acoustic or visual sensors, which provide more direct insight into sensitive information, given the physical access necessary for these types of attacks.

Another attack is taking over devices present in the room and using their wireless capabilities to capture TEMPEST emanations. If these devices are network-connected, an attacker could exfiltrate data on their normal data connection, without having to setup an additional exfiltration path. However, similar to the insertion of bugging devices it is more likely that he will use this high level of operating system access to hijack the device's microphone or camera.

Attack Technique	Cost	Time	Technical Skill Required
Antenna + Amplification	low	medium	low
Antenna + Existing Lines	low	medium	high
Antenna + Placed Lines	medium	medium	high
Weakening Shield	medium	medium	medium
Hijack Existing Device	low	medium	high

6 Countermeasures

6.1 Physical

6.1.1 Construction Security

Later passive and active countermeasures are completely ineffective if the SCIF is breached during construction. Therefore meticulous preparation of and adherence to a Construction Security Plan (CSP) is required. The CSP covers construction personnel, site perimeter, site access, and construction materials.

6.1.1.1 Construction Personnel

Construction personnel must be vetted and monitored so that they do not pose an insider threat to the construction site and resulting facility. The IC Tech Spec-for ICD/ICS 705 (Office of the National Counterintelligence Executive 2012, pp. 23–27) provides for evaluation of construction workers by origin and clearance level. For example, it forbids the use of workers from SETL threat level "critical technical threat level." Furthermore, it requires biographical data (full name, current address, Social Security Number (SSN), date and place of birth (DPOB), proof of citizenship, etc.) and fingerprint cards for background checks of all non-cleared construction personnel. It requires finish work in high-threat countries to be carried out by SECRET-cleared U.S. personnel and requires access to the site to be withdrawn if adverse security, Counterintelligence (CI), or criminal activity is detected. It also sets various requirements for the monitoring/accompanying of non-cleared workers. As an example, for new facilities it allows non-cleared workers, monitored by Construction Surveillance Technicians (CSTs) - dedicated personnel that supplement site access controls, implement screening and inspection procedures, as well as monitor construction and personnel - to perform the installation of major utilities and feeder lines. It requires that all construction personnel receive a security briefing prior to entering the site, so they know which rules to follow and what suspicious activity to report. If a construction worker leaves the project under unusual circumstances, the ICD requires the event be documented and the approriate officer to be notified.

Not all these measures for the security vetting of construction personnel can be implemented by non-government actors. These actors should try to build a staff of long-term, trustworthy workers or employ a company that does so.

Video surveillance during the construction phase can supplement other monitoring efforts. However, it requires constant attention, just like any other non-technological security measure. Even with all the possible security mitigations and background checking, the human factor as an inside threat remains one of the most sensitive areas and the hardest to defend against.

Threats from construction personnel can also further be mitigated by careful inspection after each construction phase's completion and bug sweeping before commissioning of the SCIF.

6.1.1.2 Site Perimeter

Without a secure perimeter, access to and within the site cannot be controlled. A secure fencing or other form of perimeter should be errected, and continuously monitored for unauthorized penetration. For renovation projects, barriers should be installed to segregate construction workers from operational activities, providing protection against unauthorized access and visual observation. When expanding SCIF space into uncontrolled areas, maximum demolition of the uncontrolled areas should be carried out beforehand. This protects against existing threats and ensures a "clean slate" before building a new SCIF. (Office of the National Counterintelligence Executive 2012, p. 25).

6.1.1.3 Site Access

Access control using badges and other forms of identification should be required entry to the site. Guards should monitor these entry points to prevent tampering and penetration attempts. Possible site control measures like identity verification, random searches, signs listing prohibited items, and vehicle inspections should be considered and weighed against the SCIF threat model. (Office of the National Counterintelligence Executive 2012, p. 27)

The IC Tech Spec also requires the use of cleared American guards (CAGs) to supervise non-U.S. and non-cleared U.S. guards, as well as to directly protect the site in high-threat, SETL category I countries. No equivalent to CAGs exists in the private sector. Their loyalty is difficult to recreate for a private actor who can't offer the same long-term employment and ideoligical motivation. However, guards with a similar training level can be sourced from private suppliers and with organizational practices like supervision and vetting an adequate level of security can be ensured.

6.1.1.4 Construction Materials

Construction materials must be procured, transported, and stored in a secure way. If not, the entire security of the finished SCIF can be jeapordized by faulty or compromised materials. Inspectable materials are those that can be reasonably inspected with available measures. All other materials, as well as inspectable materials on which approved test methods were not carried out, are classified as non-inspectable and are subject to higher security requirements.

Inspectable materials can be procured from trusted suppliers without further security restrictions. Inspectable materials from non-trusted suppliers or shipped to the site in an unsecured manner should be inspected using approved methods and then moved to a secure storage area (SSA). If stored outside the SSA, a random selection of these materials should be inspected before use on the site. Non-inspectable materials should be procured from trusted suppliers or other approved channels and securely transported to the SSA. They can also be procured from untrusted suppliers if randomly chosen by trusted personnel from a suppliers shelf-stock without advance notice or indication of the intended use. No discernible purchasing patterns should be established while carrying out this randomized procurement procedure. (Office of the National Counterintelligence Executive 2012, pp. 27–29)

Secure transporation is not required for inspectable materials if they are inspected and then immediately placed in an SSA. If securely procured, shipped and stored inspectable materials may even be utilized without inspection. Non-inspectable materials, should be transported securely packaged or containerized and under the 24-hour control of an approved courier or escort officer. If this is not possible they should be securely shipped using approved transit security technical safeguards capable of detecting evidence of tampering or compromise. For government actors it may be interesting to require the transporation by military or flag carrying vessels. (Office of the National Counterintelligence Executive 2012, p. 30)

A secure storage area is a true floor to true ceiling, slab-to-slab construction of some substantial material, and a solid wood-core or steel-clad door equipped with a security lock. All inspected and securely shipped materials should be placed in the SSA immediately upon arrival and stored there until they are required for installation. Alternatively a shipping container located within a secure perimeter that is locked, alarmed, and monitored or a room or outside location enclosed by a secure perimeter that is under direct observation by cleared personnel can be used as an SSA. (Office of the National Counterintelligence Executive 2012, p. 31)

6.1.1.5 Inspection Methods

X-Ray, visual inspection, metal detectors and destructive tests can be used on inspectable materials to ensure their integrity. See (Office of the Director of National Intelligence 2020) for a detailed list of inspection methods and their uses.

6.1.1.6 Technical Security

The construction phase involves many different parties and material suppliers. It is almost impossible to defend against against down the entire supply chain. Security measures are only suitable to completely prevent the most primitive attacks and only serve to make advanced attacks more difficult. Therefore, a technical surveillance countermeasure (TSCM) inspection should be carried out at all major construction milestones and before commissioning of the SCIF. This can effectively mitigate the impact of security breaches in the construction phase.

6.1.2 Intrusion Resistance

A secure perimeter is the foundation of a SCIF's security. Only it can prevent brute-force entries into the protected space. Without it, no other access control or locking measures are effective.

A multi-layered approach, using security in depth (SID), is most effective in ensuring a SCIF's physical security. The multiple layers can be a controlled perimeter, a secure installation, a building perimeter, an area surrounding the SCIF, and/or the SCIF Perimeter itself. If one of these layers is not existant in a sufficient degree it may be possible to supplement by beefing up one of the other layers.

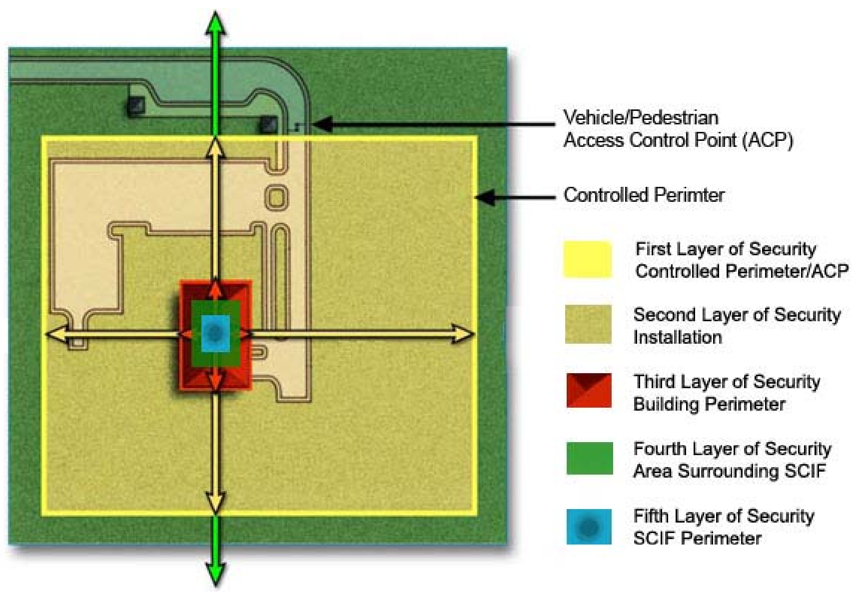


Figure 8: Map for Security in Depth of a Military Installation. Naval Facilities Engineering Systems Command Northwest (2012), p. 20

The SCIF perimeter itself should be made from a substantial material that is difficult to penetrate in a covert way. The IC Tech Spec-for ICD/ICS 705 (Office of the National Counterintelligence Executive 2012, pp. 8–10) proposes different wall makeups for varying mission demands. For example, an open storage facility - one in which sensitive information is stored openly and left out when not in use without further protection (Naval Facilities Engineering Systems Command

Northwest 2012, p. 16) - without SID requires a true-floor to true-ceiling wall made up of (from controlled to uncontrolled side) two 5/8" gipsum wall boards (GWB), ¾" #9 10 gauge expanded metal spot-welded or screwed every 6" to vertical studs, 16" metal studs and runners, acoustic fill, another 5/8" GWB. Specifically the combination of multiple GWBs and expanded metal makes for a very sturdy construction. Additionally, sheet metal laminated GWB, like Knauf Diamant Steel, can be used to further enhance the resistance capabilities of the GWB. Windows are highly discouraged for security reasons (Office of the National Counterintelligence Executive 2012, p. 12).

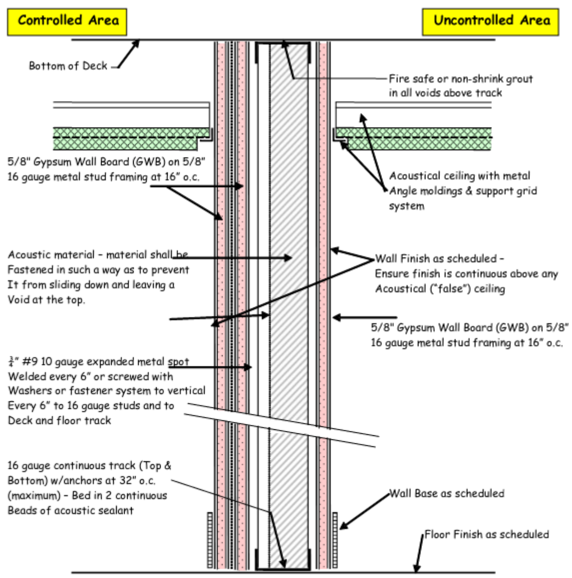


Figure 9: Wall B -Suggested Construction for Expanded Metal (Office of the National Counterintelligence Executive 2012, p. 17)

There should be only one primary entrance door to simplify personnel and visitor controlled entry. This door should be of a substantial material, like 1 ¾ inch-thick solid wood core or 1 ¾ inch-thick face steel. Its hinge pins should be located inside the SCIF perimeter or modified to prevent removal of the door, e.g., welded or set screws. (Office of the National Counterintelligence Executive 2012, pp. 11–12)

The alarm response time criteria on (Office of the National Counterintelligence Executive 2012, p. 14) requires a maximum response time of 15 minutes. Assuming that the door should resist entry for the entire alarm response time, i.e. an attacker should be captured before he breaches the door, this requirement roughly translates to DIN EN 1627 Resistance Class 5. RC 5 entails that an experienced attacker using hand tools, power tools, such as a drill, jigsaw or reciprocating saw and an angle grinder with a max. disc diameter of 125 mm can't breach the door within 15 minutes. A SCIF door setup should meet or exceed this standard.

Closed storage of sensitive information in a security container is preferrable over open storage when the SCIF is not in use. Even better, sensitive information should be stored in a separate vault when the SCIF is not in use. A security container according to the IC Tech Spec-for ICD/ICS 705 (Office of the National Counterintelligence Executive 2012, p. 5) must be a General Services Administration (GSA) approved safe, which typically complies to GSA Class 6 for storage of classified information such as documents, maps, drawings, and plans (Naval Facilities Engineering Systems Command 2021). GSA Class 6 has no forced entry requirements, but requires 30 minutes resistance to covert entry and 20 hours resistance to surreptitious entry. Commercial cabinets meeting EN 14450 Grade S2 likely also fulfill the requirements of GSA Class 6.

Figure 10: Hamilton GSA Approved Class 6 4 Drawer Security Container

6.1.3 Intrusion Detection System

An intrusion detection system (IDS), also called alarm system, is essential in securing a SCIF against attackers. It allows quick detection and response to penetrations of the secured area. Multiple sensors are used in conjunction with a monitoring station to ensure round-the-clock alerts to unauthorized entry of any kind.

Mainly, the IDS is used to secure the SCIF when it is unoccupied. All interior areas through which access could be gained, including walls and doors, should be protected by IDS. Special attention should be given to detecting and responding to system outages and tampering. Limiting false alarms to a maximum of one per 30 days further ensures the reliability and effectiveness of the system, as too many false alarms cause fatigue and desensitization of security personnel. The

IDS should be stand-alone, i.e. independent of other facilities' alarm systems. It can be supplemented with audio or video monitoring if special attention is given not to inadvertently jeopardize the SCIFs information security. (Office of the National Counterintelligence Executive 2012, p. 53)

All components, i.e. the monitoring station, movement sensors, high security switches (HSS), premise control unit (PCU), and keypads should meet the internationally recognized Underwriters Laboratories (UL) Standards 2050, 639, 634, 1610 and/or 294 respectively. The UL, being an independent, international organization not complying to the standards of any one country, is most suitable for providing globally recognized and universal security standards for the purposes of this paper.

The IDS should allow for operating in access, secure, maintenance, and shunted/masked mode. Access mode is used during SCIF operation and should allow for normal entry without causing an alarm. Tampering or entry through a secondary point, like emergency exits, should continue to trigger an immediate alarm. Secure mode is used when the SCIF is unoccupied, i.e. the last person departs the SCIF. Any unauthorized entry into the SCIF should cause an alarm to be immediately transmitted to the monitoring station in secure mode. In general, there should be no remote capability to change between these modes. Maintenace mode is used during routine repairs and testing on the system. An signal for this condition should be automatically sent to the monitoring station and verified/recorded there. Generally speaking, there should be no remote access for diagnostics, maintenance or programming for security reasons. It might also become necessary to shunt/mask sensors and zones for other reasons, like unforeseen malfunctioning of specific components, however this must be displayed at the monitoring station through the period the condition exists and automatically limited in time to the next change from access to secure mode. (Office of the National Counterintelligence Executive 2012, pp. 57–58)

Electrical power supply of the IDS must be redundant, e.g. backed by 24 hours of uninterruptible power supply (UPS). On primary power failure, the IDS should be automatically transferred to emergency electrical power without causing an alarm. An indicator of the power source in use should be given at the PCU or monitoring station. (Office of the National Counterintelligence Executive 2012, p. 58)

The monitoring station must comply to UL 2050, which sets out standards for organizations monitoring, signal processing, investigating, servicing, and operating alarm systems in sensitive facilities (Convergint Technologies 2017). Governments themselves or private contractors can set up monitoring stations that meet these standards. These stations should be staffed by human operators trained in system theory and operation to effectively interpret system incidents and take appropriate response action. Any alarm event along with time of receipt, names of responding personnel, dispatch time, nature of the alarm, and follow up actions should be recorded there for at least two years. (Office of the National Counterintelligence Executive 2012, p. 59)

Sensors are the eyes and ears of an IDS. They detect breaches and trigger alarms. All sensors should be located inside the SCIF to prevent tampering and TEMPEST issues. Interior areas of a SCIF through which reasonable access could be gained should be monitored by motion sensors (UL 639) and high security switches (HSS) (UL 634 level 1 or 2). Motion sensors trigger alarms on detecting movements in their view. HSS split in two, one half mounted on moving components and the other on an adjacent rigid part. They trigger alarms when they lose internal contact between their two halfs, for example when a door is opened. SCIF perimeter doors should be protected by both an HSS and a motion sensor. Failed sensors should cause continuous alarm until repaired. (Office of the National Counterintelligence Executive 2012, pp. 54–55) Seismic detectors, sensors that trigger on vibrations such as those resulting from drilling and blastic, can further be used to supplement HSS and motion sensors. There are impressive innovations in the realm of motion sensors such as passive infrared detecting attacker's body temperature, doppler radar catching attacker's radar reflections, cloak and camouflage detection against intrudersattempting to cover their infrared signal, and anti-masking technology against attempts to obscure the field of view of the detector (Bosch Security 2021).

Premise Control Units (PCU) serve as a first point of control inside the SCIF. They as well as any associated cabling should be fully located within the SCIF perimter. PCU should validate authorized use with an authentication technology, such as a keypad and/or card reader. Cabling between all sensors and PCU should be dedicated to the IDS and contained within SCIF. Otherwise "External Transmission Line Security" must be employed. The alarm status as well as power source in use should be continuously displayed at the PCU. A special indicator should alert to changed/failed power supply. The PCU should identify and display all activated sensors. The auto-alarm reset feature, if present, must be disabled as every security incident can only be resolved after an inspection of the SCIF and a determination for the cause of the alarm by trained personnel. Because of the sensitive nature of the information displayed, the PCU must be installed in a location that precludes observation by any unauthorized party. (Office of the National Counterintelligence Executive 2012, p. 55)

Immediate and continuous alarm must be given on any intrusion detection, failed sensor, tamper detection, or enabling of maintenance mode (maintenace message may be used in place of alarm). Alarms or maintenace messages should be displayed individually for all zones shunted or masked during maintenance mode. (Office of the National Counterintelligence Executive 2012, p. 55)

Once an IDS is set up to the above specifications, thorough acceptance testing should be carried out before the SCIF is commissioned. Motion sensors should be tested by moving at very slow speeds through the monitored area. This speed should not exceed 800 mm per second. The movements should be repeated throughout the SCIF and from different directions. The alarm must be activated at least three out of every four trials. HSS should be tested to ensure that an alarm activates before the non-hinged side of the door or window opens beyond its own thickness from the closed position. For example, this means that the HSS triggers an alarm before the door opens 5 cm for a 5 cm door. Tamper testing should be carried out by ensuring that alarms are triggered when IDS equiptment covers are opened, both in secure and access mode. These test procedures should be repeated at least semi-anually. (Office of the National Counterintelligence Executive 2012, pp. 60–61)

6.1.4 Access Control

An access control system (ACS) is employed while the SCIF is occupied to control and record personnel entry into the protected space. It is mounted in addition to the SCIF perimeter door lock to regulate access while the SCIF is in use. It does not replace this lock while the SCIF is unoccupied. (Office of the National Counterintelligence Executive 2012, p. 62)

Visual recognition of persons entering the SCIF by an authorized person at the entrance to a SCIF is the ideal access control. Should this not be possible an automated system can be used instead. (Office of the National Counterintelligence Executive 2012, p. 62)

An automated personnel ACS should use two different credentials, such as ID badge/card, PIN, and biometric identifier, to verify authorized personnel. The probability of an unauthorized individual gaining access must be no more than than one in ten thousand. Card readers, keypads, communication interface devices, and other access control equipment located outside the SCIF must be tamper-protected and securely fastened to a wall or other fixed structure. Electrical components, associated wiring, or mechanical links should only be accessible from inside SCIF. Otherwise transmission lines to and from outside SCIF must be FIPS-AES certified encrypted. Equipment containing access-control software used to program in authorized persons and remove no longer authorized individuals should be located fully inside the SCIF. Electric door strikes used to unlock the door and "buzz people in" must have a positive engagement, i.e. rest in a locked position and only unlock on entry authorization. The electric door strikes should comply to UL 1034 (Burglary-Resistant Electric Locking Mechanisms). (Office of the National Counterintelligence Executive 2012, p. 63)

Records should be kept of the active assignment of ID badge/card, PIN, level of access, recent entries, and other similar system-related information. Records of personnel removed from the authorized persons list should be retained for two years. Records of security incidents should be retained for five years from the date of the incident or until the corresponding investigation is resolved. (Office of the National Counterintelligence Executive 2012, p. 63)

If the number of personnel that require access is low and there is only one entrance a non-automated access control may be used. This can consist of a mechanical, eletric or electromechanical combination lock with combinations of four or more random digits. Mechanical access control devices should be installed to prevent manipulation or access to mechanisms used for setting the access combination from outside door. For all non-automated mechanisms, the control panel or keypad should be installed to preclude unauthorized observation of combination entry or actions of combination change. The control panel with combination, cabling and wiring should be located inside the SCIF with sufficient physical security to deny unauthorized access to its mechanisms. (Office of the National Counterintelligence Executive 2012, p. 64)

6.1.5 Locks

When not occupied, SCIFs should be alarmed and secured with a FF-L-2740A compliant combination lock and a pedestrian door deadbolt meeting Federal Specification FF-L-2890 (Office of the National Counterintelligence Executive 2012, p. 11). The combination lock is used to secure the door when the SCIF is unoccupied and the access control device is used when the SCIF is occupied (Office of the National Counterintelligence Executive 2012, p. 63). The equivalent international specifications for combination locks are UL 768 and DIN EN 1300. The lowest UL 768 rating, Group 2, is essentialy equivalent to FF-L-2740A (Locksmith Reference 2018).

Figure 11: Kaba X-10 Mounted Lock (FF-L-2740)

Combinations to locks installed on perimeter doors should be changed when a combination lock is first installed, when a combination has been compromised, and whenever a person knowing the combination no longer requires access to it unless other sufficient controls exist to prevent access to the lock. (Office of the National Counterintelligence Executive 2012, p. 83)

6.1.6 CCTV

Video surveillance, also known as CCTV, can be used to supplement the monitoring of SCIF entrances for the remote control of doors from within SCIF. Special attention should be given to a CCTV system to make sure that it presents no technical security hazard. (Office of the National Counterintelligence Executive 2012, p. 64). CCTV may be also used to supplement monitoring of the SCIF entrance and record events for investigation (Office of the National Counterintelligence Executive 2012, p. 75).

When CCTV is used to monitor a SCIF entrance for ACS purposes, the remote control device should be located within SCIF and should be monitored/operated by indoctrined personnel. The cameras should provide a clear view of SCIF entrance without enabling a viewer to observe classified information when the door is open nor external control pads or access control components that would enable them to identify PINs or access procedures. The CCTV communication lines should be fully located within SCIF. Any external communication lines should be installed to prevent tampering. (Office of the National Counterintelligence Executive 2012, p. 64)

When CCTV is used to monitor a SCIF entrance for security and record-keeping purposes the system and all its components, including communications and control lines, should be exterior to SCIF perimeter. In this case it must also not enable a viewer to observe any classified information or authentication procedures.

In both cases special attention must be given that the cameras present no further technical security risk. Chinese-made video surveillance systems can be reasonably suspected of leaking information back to their Chinese State owned/controlled manufacturers (Lehman-Ludwig 2020), like HikVision and Dahua, and suffer from general bad security practices (Cyber & Infrastrucutre Security Agency 2017). Their use has consequently been banned from U.S. government agencies and facilities (U.S. House. 115th Congress 2018). In general, proprietary products suffer from this kind of backdoor-risk and should only be sourced from trustworthy manufacturers. Even better, they should be built in-house with open hardware components.

Figure 12: Elphel 10393 Series Free Software and Open Hardware Camera

6.2 Visual

Visual insights into the SCIF space are the easiest attack vector to defend. It suffices to create a “water-tight” outer shell without gaps or holes. Every effort should be made to exclude windows from the SCIF (Office of the National Counterintelligence Executive 2012, p. 12). If they are unavoidable they must at least be treated for visual protection, i.e. darkened with external blinds and/or laser protection film (Wolfsperger 2008, p. 463). As noted above, video surveillance systems should be designed with special attention not to provide visual insights into the space. No cameras should be installed inside the SCIF (Office of the National Counterintelligence Executive 2012, p. 82).

To protect from visual insight into the SCIF during personnel entry, entrace points should incorporate a vestibule to preclude visual observation (Office of the National Counterintelligence Executive 2012, p. 11). Double doors should have an astragal strip attached to one door to prevent observation through the door crack (Office of the National Counterintelligence Executive 2012, p. 12).

6.3 Acoustic

To secure the discussions, information processing, and conferences carried out inside the SCIF it is essential to design an effective acoustic protection system. Sound waves have the habit of finding weakpoints in even the most well-designed systems and escaping to the outside where even the faintest emission can be captured and reconstructed with digital means. Therefore, it is necessary to pay meticulous attention to detail, both in the design and build phases, while building on multiple technologies to prevent capture of usable sound information from any point.

In most cases, passive sound attenuation, walls with strong sound isolation properties, must be combined with active sound masking, speakers that emit speech-like sounds to render useless escaping sound waves. Both out of room constraints and redundancy considerations passive sound attenuation most often doesn't suffice on its own. A sound masking system can reduce the wall thickness needed and mitigate any weakpoints that are inadvertently built into the attenuating shell.

Even protecting against attackers who manage to smuggle microphones into the SCIF space, as guests or intruders, should be considered in system design.

6.3.1 Sound Attenuation

Passive sound attenuation is the first step in reducing noise emissions from the SCIF space. Massive single-shell walls or double-shell components can be used to reduce sound transmission on all paths. Both direct transmission, sound forces on a wall to structure-borne sound in the wall to airborne sound outside the SCIF, and indirect transmission, airborne sound within the SCIF to structure-borne sound in the wall to airborne sound outside the SCIF, can be reduced with the right wall design both on primary and secondary paths. (Möser 2009, p. 253)

The sound insulation quality of building components is dependent on the frequency of the sound emission. Particularly low-frequency sound waves set walls into vibrations that they readily transmit as airborne sound to the outside. Higher frequencies are of less interest in system evaluation, because the insulation quality of walls for higher frequencies is almost always good. Problematically, the very sound emissions that need to be protected, those of the human voice, are in the low frequency range. (Möser 2009, p. 256)

A clear understanding of cut-off frequencies is essential to properly analyzing the frequency-dependent sound insulation of building components. The cut-off frequency is the frequency at which the wavelength of the airborne sound matches the length of a component's bending wave. In this frequency range, track matching occurs between the incoming airborne sound and the walls internal vibrations. They align and result in poorer airborne sound insulation. For single-shell components, sound attenuation increases with 6 dB/Octave below the cut-off frequency. This is known as Bergers' mass law. At the cut-off frequency the component's sound attenuation suffers a sharp drop and then rises with 7.5 dB/Octave. The drop is also described as the "cut-off slump" and entails significant decreases in sound attenuation at frequencies around cut-off frequency. The cut-off slump is more drastic the higher the cutoff frequency. Because of the higher sound attenuation increases above the cut-off frequency and lower cut-off slumps, it is of interest to design single-shell components with as low a cut-off frequency as possible. This can be accomplished by making the wall as rigid as possible and increasing its thickness. (Möser 2009, pp. 258–270)

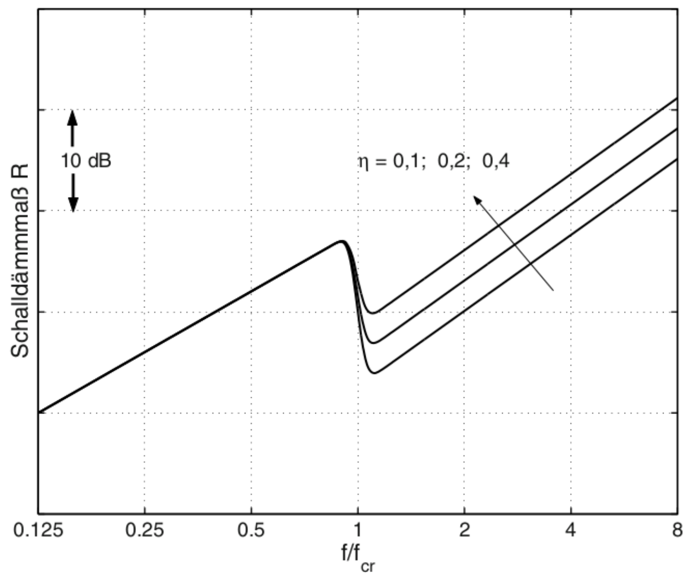


Figure 13: Principle curve of the sound reduction index frequency response of a single shell wall. Eta = loss factor derived from the loss mechanisms actually occurring, such as internal damping and vibration energy dissipation to adjacent components, f = frequency of emission, f_{cr}= cut-off frequency (Möser 2009, p. 267)

Increasing wall rigidity and thickness might not always be possible due to space, weight, and cost constraints. Thankfully, a better method for building attenuating walls exists, double-shell components with flexurally soft facing-shells. These make use of the propensity of the two walls to swing at different frequencies when not connected, making use of the cavity in between to create a mass-spring-mass system. No connections or cross-coupling may exist between the two shells as these destroy the spring function of the hollow space and jeopardize the entire system's effectiveness. (Möser 2009, pp. 270–276)

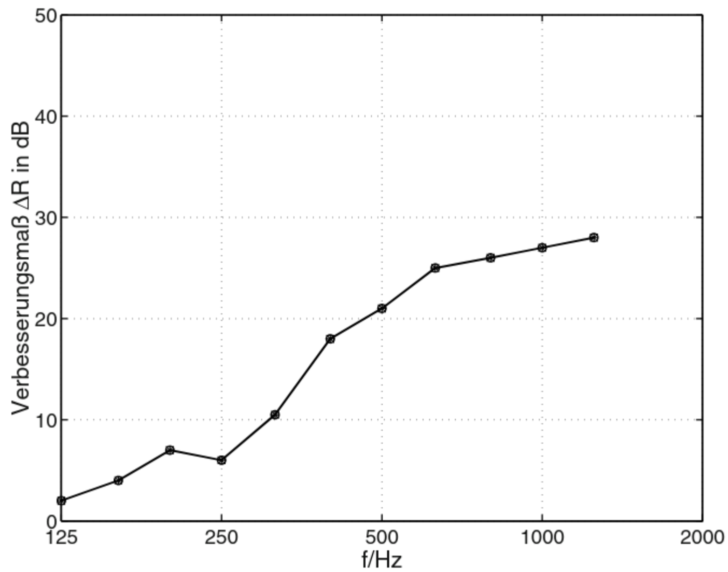


Figure 14: Improvement of the sound insulation delta R of a 80 mm plaster wall by a flexible facing shell with m”$_2$ = 4 kg/m^2 and cavity depth d = 65 mm, filled with mineral wool

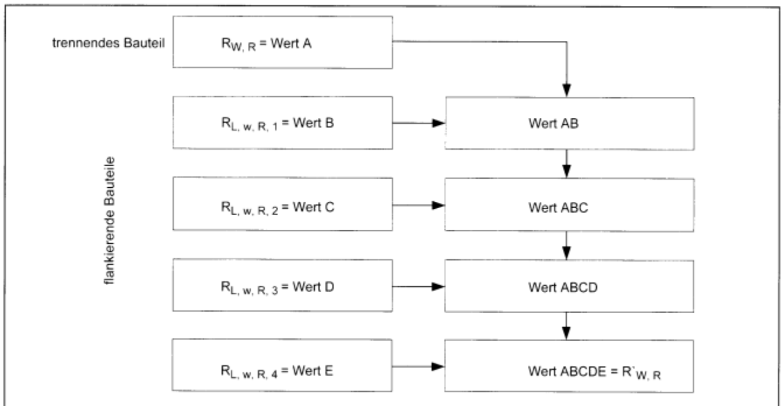
Below the cut-off frequency the additional shell has no effect, however, above it the sound attenuation increases with 12 dB/octave. At the cut-off frequency there is again a slump in attenuation performance. The cut-off frequency should be engineered to be as low as possible to make use of the steep attenuation increases. According to

$$f_o \approx \frac{60Hz}{\sqrt{\frac{m_2''}{kg/m^2}\frac{d}{m}}}$$

a cut-off frequency of 60 Hz (well below the building acoustics frequency range beginning at 100 Hz) can be reached with a facing shell with a mass per unit area of m”$_2$ = 10 kg/m^2 (heavy gypsum wall board) and a hollow space of d = 10 cm. From here we can see that sufficiently low cut-off frequencies can be achieved without excessively heavy facing shells or massive hollow spaces. (Möser 2009, p. 273)

To achieve a high sound attenuation level it is advantageous to use heavy total masses and to distribute them unequally among the shells if possible avoding shells of equal weight. One should also maximize the distance d between the two shells, dampen the cavity as fully as possible with absorber material, and avoid leaks or structure-borne sound bridges. (Möser 2009, p. 276)

In order to evaluate the solution on a whole system level, including floors and ceilings, one combines the walls R_W value as described in Chapter 4.2 with the longitudinal sound transmission $R_{L,w}$ of the four flanking components (two walls, ceiling, and floor) in a stepwise addition scheme specified in DIN 4109-1. The result is a total resulting sound reduction index $R'_{w,R}$ expressed in dB. (Tichelmann, Pfau 2000, p. 34)



Dabei gilt beispielhaft für alle Stufen:

wenn Wert A ≥ Wert B:	wenn Wert B ≥ Wert A:
Werte-Differenz = Wert A – Wert B ablesen von ΔR aus Tabelle Wert AB = Wert B – ΔR	Werte-Differenz = Wert B – Wert A ablesen von ΔR aus Tabelle Wert AB = Wert A – ΔR

Werte-Differenz [dB]	0,0	0,5	1,0	1,5	2,0	2,5	3,0	3,5	4,0	4,5	5,0
ΔR [dB]	3,0	2,8	2,5	2,3	2,1	1,9	1,8	1,6	1,5	1,3	1,2

Werte-Differenz [dB]	5,5	6,0	6,5	7,0	7,5	8,0	9,0	10,0	11,0	13,0	15,0
ΔR [dB]	1,1	1,0	0,9	0,8	0,7	0,6	0,5	0,4	0,3	0,2	0,1

Figure 15: Stepwise addition scheme DIN 4109-1 (Tichelmann, Pfau 2000, p. 34)

Walls and flanking components aren't the only transmission paths for sound out of the SCIF. Air ducts and vents also present a significant challenge in sound attenuation. If untreated they can serve as direct transmission paths for sound waves out of the SCIF and eliminate all benefits gained from a carefully designed shell system. In order to treat air ducts and vents it is necessary to insert some type of silencer. These can be reflection mufflers, wall mufflers or active noise cancelling systems. Reflection mufflers work eclusively through reflection. Cross-section changes, branch-offs and inserted chambers reflect sound waves internally and decrease their energy. Wall mufflers Work through absorption *and* reflection. Absorbant wall lining or slim absorbant channels are used to reflect sound waves internally. Additionally, these sound waves lose energy into the mufflers absorbant surfaces. (Möser 2009, pp. 285–328)

Active noise cancelling systems produce anti-sound, amplitude inverted sound waves, to cancel out sound. They are limited in frequency range and aereal effectivity. Large levels of sound reduction require very high replication accuracy in the secondary, cancelling field. (Möser 2009, pp. 405–427) Because of their complexity and relative novelty they are not the go-to solution for air vent treatment.

For reflection and wall muflers either achieve high attenuation performance in narrow bands or moderate attenuation in wider bands. Knowing the frequency range of sound to be cancelled is essential in optimizing the mufflers. Specialized air vent mufflers for the human voice, called cross-talk sound attenuators, are readily available on the market. They achieve relatively high performance values around the frequency spectrum of the human voice and come in a box shape optimized for installation inside drywall. An off-the-shelf product from german manufacturer SHAKO KG, the cross-talk sound attenuator box AUDIX® achieves a weighted sound reduction index of R_w 38 dB at 508 mm length and 300 mm height. Normalised sound level difference, $D_{n,e}$ at the male fundamental frequency 125 Hz is 54 dB. (SCHAKO KG 2021)

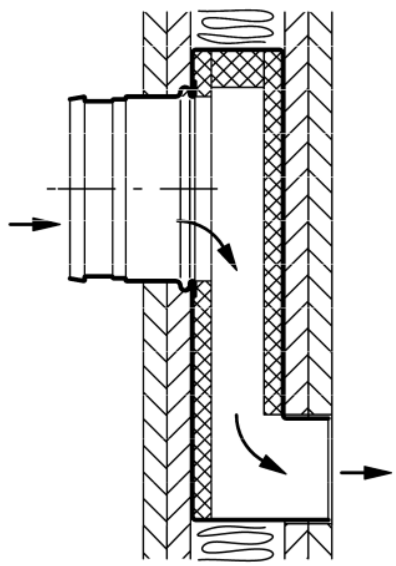


Figure 16: SCHAKO Cross-talk Sound Attenuator Box AUDIX® Installation Schematic

6.3.2 Sound Masking

6.3.3 Microphone Jamming

6.4 Electromagnetic/TEMPEST

6.4.1 Electromagnetic Shielding

6.4.2 System Monitoring

6.4.3 Signal Jamming

6.5 Bug Sweeping

7 Example Module

This section will propose an example solution for a Sensitive Compartmented Information Facility (SCIF). It will employ the above passive and active countermeasures in a shipping container sized (~ 6 x 2.4 x 2.7 m) module to reach the quantitative limits on information source leaks defined above.

7.1 Physical

7.2 Visual

7.3 Sound

7.4 Electromagnetic/TEMPEST

References

BOSCH SECURITY, 2021. *Commercial Series TriTech AM Motion Detectors with Anti-mask*. March 2021. https://resources-boschsecurity-cdn.azureedge.net/public/documents/Commercial_Series_Tr_Data_sheet_enUS_75201763083.pdf.

CONVERGINT TECHNOLOGIES, 2017. *Meet UL 2050 Standards for Closed Rooms and SCIFs*. September 2017. https://www.convergint.com/meet-ul-2050-standards-for-closed-rooms-and-scifs/.

CYBER & INFRASTRUCUTRE SECURITY AGENCY, 2017. *Hikvision Cameras* [online]. May 2017. ICS Advisory (ICSA-17-124-01). Available from: https://us-cert.cisa.gov/ics/advisories/ICSA-17-124-01

DEUTSCHES INSTITUT FÜR NORMUNG, 2018. DIN 4109-1:2018-01: *Sound Insulation in Buildings - Part 1: Minimum Requirements*. Berlin: Beuth Verlag.

EMCTEST TECHNOLOGIES, 2018. *NSA 94-106 Effectiveness Testing RF Shielded Enclosures*. 2018. https://www.shieldingtests.com/?standard=NSA-94-106.

GENKIN, Daniel, PACHMANOV, Lev, PIPMAN, Itamar and TROMER, Eran, 2015. Stealing Keys from PCs using a Radio: Cheap Electromagnetic Attacks on Windowed Exponentiation. *Tel Aviv University*. February 2015.

GÖSELE, K. and SCHRÖDER, E., 2004. Schalldämmung in Gebäuden. In: *Taschenbuch der Technischen Akustik*. Berlin, Heidelberg: Springer-Verlag.

KRIEGER PRODUCTS, 2015. *Radio Frequency Interference (RFI) Shielding Principles*. 2015. https://www.kriegerproducts.com/downloads/general/RFI-Shielding-Principles.pdf.

LEHMAN-LUDWIG, Anna, 2020. *Hikvision, Corporate Governance, and the Risks of Chinese Technology*. August 2020. https://www.csis.org/blogs/technology-policy-blog/hikvision-corporate-governance-and-risks-chinese-technology.

LIU, Zhuoran, SAMWEL, Niels, WEISSBART, Léo, ZHAO, Zhengyu, LAURET, Dirk, BATINA, Lejla and LARSON, Martha, 2020. Screen Gleaning: A Screen Reading TEMPEST Attack on Mobile Devices Exploiting an Electromagnetic Side Channel. *Radboud University*. November 2020.

LOCKSMITH REFERENCE, 2018. *Ratings for Safe Locks*. October 2018. https://lockreference.com/ratings-for-safe-locks/.

MÖSER, Michael, 2009. *Technische Akustik*. Berlin, Heidelberg: Springer-Verlag.

NAVAL FACILITIES ENGINEERING SYSTEMS COMMAND, 2021. *Introduction to GSA-approved Security Containers*. January 2021. https://www.navfac.navy.mil/navfac_worldwide/specialty_centers/exwc/products_and_services/capital_improvements/dod_lock/SecurityHardware/SecurityContainers.html.

NAVAL FACILITIES ENGINEERING SYSTEMS COMMAND NORTHWEST, 2012. *Physical Security of Sensitive Compartmented Information Facilities (SCIF)*. November 2012. https://www.washingtonpost.com/news/politics/wp-content/uploads/sites/11/2017/02/navfac_scif_ho.pdf.

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, 2020. *Inspectable Construction Materials Checklist*. July 2020. https://www.dni.gov/files/Governance/Inspectable-Materials-Checklist-V15.pdf.

OFFICE OF THE NATIONAL COUNTERINTELLIGENCE EXECUTIVE, 2012. *Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities Version 1.2 - IC Tech Spec-for ICD/ICS 705*. 2012. https://fas.org/irp/dni/icd/ics-705-ts.pdf.

RTL-SDR.COM, 2017. *TempestSDR: An SDR tool for Eavesdropping on Computer Screens via Unintentionally Radiated RF*. November 2017. https://www.rtl-sdr.com/tempestsdr-a-sdr-tool-for-eavesdropping-on-computer-screens-via-unintentionally-radiated-rf/.

SCHAKO KG, 2021. *Technical Documentation for Cross-talk Sound Attenuator Box AUDIX®*. March 2021. https://schako.com/wp-content/uploads/audix_en.pdf.

TICHELMANN, Karsten and PFAU, Jochen, 2000. *Entwicklungswandel Wohnungsbau: Neue Gebäudekonzepte in Trocken- und Leichtbauweise*. Wiesbaden: Vieweg+Teubner Verlag.

U.S. HOUSE. 115TH CONGRESS, 2018. *John S. McCain National Defense Authorization Act for Fiscal Year 2019*. August 2018. H.R.5515.

U.S. NATIONAL SECURITY AGENCY, 1972. *TEMPEST: A Signal Problem*. 1972. http://www.jproc.ca/crypto/tempest.pdf.

U.S. NATIONAL SECURITY AGENCY, 1994. *NSA 94-106 National Security Agency Specification for Shielded Enclosures*. 1994. http://cryptome.info/0001/nsa-94-106.htm.

WOLFSPERGER, Hans A., 2008. *Elektromagnetische Schirmung: Theorie und Praxisbeispiele*. Berlin, Heidelberg: Springer-Verlag.