TECHNICAL PREPRINT

Non-Cooperative Cyber-Electromagnetic Exploitation of ExpressLRS UAV C2 Links: Identity Reconstruction, FHSS Tracking, and Controlled Transmitter Substitution

Melik Lemariey

Electronic warfare consultant, France, https://meliklemariey.com/

Corresponding author: melik.e.lemariey@pm.me
ORCID: 0000-0002-1041-0113
Repository: `elrs-h44f-executable-evidence`

Abstract—Detecting a frequency-hopping command link is not sufficient to reconstruct its protocol, timing, and radio state. This study examines, within a cyber-electromagnetic exploitation framework, the extent to which the operational physical and logical state of an ExpressLRS link can be reconstructed from non-cooperative RF observations and then used for passive tracking and controlled validation of the link state.

Independent Python implementations specific to each version family were compared against a separately compiled C++ reference derived from selected rules in the pinned tags 1.2.1, 2.5.2, 3.6.4, 4.0.1, and 4.1.0 over 39 845 888 inputs, with no divergence. The H44F-A hardware campaign on ELRS 4.1.0 begins without a radio-profile or identity oracle, without a binding phrase, without supplied UID or seed values, and without a precomputed FHSS table. It passively selects a unique profile from six candidate profiles, confirms it after radio reset, and then reconstructs two FHSS-equivalent UID2 candidates, `3F|BF`, together with UID3–UID5 `35:59:F0`. From UID4 and UID5, it derives the base CRC initializer `0x5DF0`, and then obtains two seeds that produce the same 240-position FHSS table.

The reconstructed state enables tracking of 960/960 packets with no CRC error or channel divergence. After intentional interruption of the reference transmitter, a separately developed transmitter is accepted by the stock receiver. All 3 698 commands observed after the reference source returns remain attributed to the substitute source; after the latter is stopped, 439 of the 440 recovery commands are attributed to the reference source. The 5 671 RAW frames are reproduced without CRC, format, or sequence errors.

The binding phrase is not recovered: recovering it is unnecessary for the substitution demonstrated on the test bench. H44F-A shows that a state reconstructed from non-cooperative RF observations enables not only passive tracking and link-state validation, but also controlled source substitution on a stock receiver after interruption of the reference transmitter. These results demonstrate neither initial contention against a continuously active source, nor jamming capability, operational range, in-flight validation, or universal applicability to ExpressLRS.

Keywords—Mobile and wireless security, Network experimentation, Software reverse engineering, Embedded systems security, Cyberwarfare, Command and control

Preprint scope. The experiments use hardware owned by the experimenter in a controlled RF test bench, without flight or third-party links. A separate public review artifact brings together, for H44F-A and H44F-B, the anonymized logs, exact hashes of the selected artifacts, offline reconstruction and verification code, narrow upstream comparisons, and replay scripts. It enables offline reproduction of both verdicts without providing the active hardware chain. The `elrs-h44f-executable-evidence` repository distributes the original scripts under Apache-2.0 and the documentation and sanitized evidence under CC BY 4.0. It excludes the private binding phrase, any ready-to-flash firmware, directly usable injection tools, and any operational jamming procedure.

1. Introduction

Frequency-hopping spread-spectrum command links combine a variable carrier with short packets and stringent latency constraints. For a technical COMINT or electronic-support receiver, energy detection is only a first step: the PHY must be identified, the protocol state reconstructed or constrained, timing acquired, synchronization restored within a bounded error, and the consistency of decoded packets verified. Success at one stage does not imply success at the next.

ExpressLRS is an open-source, low-latency radio-control protocol implemented on several families of LoRa transceivers. Its openness enables exact code analysis and differential validation, but does not prove that a theoretical reconstruction is feasible for every version, integrated circuit, packet mode, or timing profile. Within a cyber-electromagnetic exploitation framework, this study therefore treats the reconstruction of PHY profiles from pinned sources, their passive identification through RF observation, protocol and identity reconstruction, FHSS tracking, controlled substitution, and attribution of the source retained by the receiver as an integrated chain of evidence.

The research question is as follows:

To what extent can the physical and logical state of a frequency-hopping ExpressLRS command link be reconstructed from non-cooperative RF observations, and with what accuracy can the reconstructed state support passive tracking and controlled validation of the link state?

The final H44F-A experimental campaign provides an integrated answer under the conditions of the test bench. It reconstructs from pinned sources the SX126x-compatible ExpressLRS radio profiles for the version and

FCC915 band under study, and then applies them successively in receive-only mode on their SYNC frequency. The blind detector selects a unique profile from coherent SYNC frames with correct structure and valid CRC, without a profile, identity, or binding-phrase oracle. After radio reset, its reconstruction core starts again from a fresh SYNC and reconstructs the operational logical state, the identity equivalence class, the seed, the FHSS table, and the synchronization state. The resulting state enables tracking of 960/960 packets without CRC error or channel divergence, followed by controlled source substitution on a stock receiver after intentional interruption of the reference source.

The deliberately bounded contributions are:

1. a source-pinned, cross-version reconstruction of selected rules governing OTA, CRC, UID, SYNC, and FHSS dependencies in the studied tags of ExpressLRS families 1 through 4.1;
2. reconstruction of the SX126x-compatible ExpressLRS radio profiles for the studied version and FCC915 band, followed by passive scanning until a unique profile is selected through detection of coherent SYNC frames with valid CRCs;
3. blind recovery of the operational radio derivatives of an ELRS 4.1 identity derived from 4096 bits of CSPRNG output, without recovering the binding phrase, including two UID2 candidates belonging to the same FHSS equivalence class;
4. embedded tracking across all 240 positions of the FHSS table, with 960/960 CRC-valid packets and no channel divergence in the final campaign;
5. controlled substitution and verified attribution of the reference and substitute sources, with retention of the substitute source after the reference returns, followed by recovery of the reference after the substitute source is stopped.

Earlier experimental work conducted from 2016 onward on a distinct FHSS link had already explored a related approach based on PHY characterization, exploitation of observable identity fields, local generation of candidate sequences, and their progressive elimination through comparison with observations. That work was not published at the time and does not constitute publicly available prior work concerning ExpressLRS. Its detailed description and the individual attribution of contributions are deliberately deferred in this version of the preprint pending validation by the participants in that work.

Several relevant properties of ExpressLRS were also discussed publicly from 2022 onward. No priority is claimed over those general principles. The contribution claimed here concerns their cross-version, quantitative, integrated, and reproducible treatment, from passive radio-profile identification to link-state reconstruction, full tracking, and controlled validation on a stock receiver.

2. State of the Art and Prior-Work Boundary

The general framework for digital radiocommunications, signal modeling, and the radio-frequency chain used in this study draws on the two volumes of the collective work edited respectively by Geneviève Baudoin and Martine Villegas [1, 2]. These works serve here as general theoretical references; they describe neither ExpressLRS nor a non-cooperative reconstruction of its link state. The present study starts from physical classification, or performs it jointly, and then evaluates the extent to which observable fields and public deterministic generators make it possible to reduce a discrete space of link states.

In the radio-control field, g3gg0 published a reverse engineering of the distinct TBS Crossfire 900 MHz link, based on SPI traces, recovery of PHY parameters, discovery of the hopping sequence, CRC analysis, reception on a Heltec board, and real-time timing tracking [3]. This work constitutes relevant prior methodological work. It is not asserted, however, that TBS Crossfire and ExpressLRS share an OTA architecture, an identity derivation method, a CRC initialization scheme, or software lineage.

The analysis published by NCC Group in 2022 focused mainly on ExpressLRS 1.x and 2.x [4]. It described the presence of three UID bytes in SYNC frames, UID-dependent CRC initialization, exhaustive search of one seed byte, reduction from 256 literal candidates to 128 distinct sequences, and a scenario for configuring a compatible transmitter. The present work reproduces some of these known principles where necessary and extends the software and hardware scope through version 4.1. It does not use the term “hijacking” as a result independent of the version under study and of the experimental conditions.

In public pull request #1411, opened by `redfiveau` and then closed without merge in 2022, `CapnBry` discussed direct observation of the FHSS sequence, exhaustive search of the 14-bit CRC initialization, replay of a static SYNC frame, and the distinction between collision avoidance and authentication [5]. `redfiveau` described the UID2 alias and then stated that they had written and successfully used hijacking code during tests. This statement is a claim of prior experimental work by its author; the corresponding code and test logs, however, do not appear in the currently available corpus.

Several security changes and their costs were also discussed, including a measurement of flash-memory usage by `pkendall64`, but the proposal was ultimately closed without merge. Later comments by `CapnBry` and `redfiveau` addressed protocol- and hardware-specific constraints. These statements are attributed to their respective authors and are not presented as an official position of ExpressLRS LLC.

Chronological boundary and earlier work. Earlier experimental work conducted from 2016 onward on a distinct FHSS link had already explored a related approach based on PHY characterization, exploitation of observable identity fields, local generation of candidate sequences, and their progressive elimination through comparison with observations. That work was not published at the time, does not constitute publicly available prior work concerning ExpressLRS, and establishes neither

protocol identity, software lineage, nor a shared OTA architecture.

Its detailed description and the individual attribution of contributions are deliberately deferred in this version of the preprint pending validation by the participants in that work. This version therefore only records its existence and its general methodological continuity with the present experimental approach.

Public discussions concerning ExpressLRS from 2022 onward constitute relevant prior work and are attributed to their respective authors. No public priority is claimed over the general principles already discussed. The contribution claimed here concerns their cross-version, quantitative, integrated, and reproducible treatment, from passive radio-profile identification to link-state reconstruction, full tracking, and controlled validation on a stock receiver.

3. System and Threat Model

The system comprises a reference source, a stock ExpressLRS receiver, LoRa OTA packets whose format depends on the version and which are transmitted according to a deterministic FHSS cycle, and CRSF interfaces [6, 7]. A binding phrase is derived into UID bytes, but the official documentation distinguishes this mechanism from a password or encryption key and assigns it a collision-avoidance role [8]. A high-entropy binding phrase protects against guessing and preimage search, but does not constitute cryptographic frame authentication. FHSS likewise does not constitute an authentication mechanism. The CRC checks the consistency of a packet with a candidate state; it is not a keyed MAC.

The protected assets are command integrity, source authenticity, link availability, the FHSS synchronization state, command- and telemetry-channel states, the receiver acquisition state, and the operational radio identity. The actors considered are the legitimate operator, the non-cooperative RF observer, the authorized experimenter equipped with a programmable radio, and the defender.

For the H44F-A campaign, the model assumes knowledge of the ExpressLRS protocol, the version under study, the FCC915 band, SX126x compatibility, and the corresponding public source code. The OTA format, 14-bit CRC width, its `0x2E57` polynomial, and version-specific derivation rules are therefore known. The active radio profile is nevertheless neither supplied by an oracle nor fixed at compile time. The binding phrase and link-specific states—UID, base CRC initializer, current nonce, seed, FHSS table, and synchronization state—are not supplied. No guessing or preimage computation of the binding phrase is required.

Figure 1 separates the cross-version model derived from the sources from the integrated H44F-A hardware chain. Code coverage does not turn an untested version, band, radio, or profile into RF evidence.

H44F-A reconstructs from pinned sources the candidate radio profiles compatible with the studied configuration, then applies them successively to the SX1262 in receive-only mode on their respective SYNC frequencies. The scan dynamically selects at runtime the unique profile that produces a SYNC frame with correct structure and valid CRC. An independent acquisition then confirms the same packet rate and the same UID4/UID5 bytes.

H44F-A is executed without a profile or identity oracle and without a binding phrase; the three corresponding indicators are zero. During scanning, the Heltec/SX1262 platform remains strictly in receive mode and performs no RF transmission; only the reference source stimulated through CRSF transmits. If no valid profile is found or if several profiles remain ambiguous, the chain stops and Heltec RF transmission remains disabled.

After profile confirmation, the scan, classifier, and identity states are cleared, and the radio is reset. Only the selected profile is passed to the blind core; no identity byte is transferred between the two internal stages of the campaign.

The H44F-A reconstruction core begins without an identity oracle or binding phrase, and without compiled UID, base CRC initializer, seed, or FHSS table. From the selected profile, it acquires a new SYNC, reconstructs the operational radio identity, seed, FHSS table, and current synchronization state, and then validates passive tracking and the controlled active chain on a stock receiver.

The active phases of H44F-A use hardware owned and authorized by the experimenter, in a controlled RF environment, without third-party links or flight, and at the minimum practical power. The reference source is intentionally interrupted before substitute transmission and reactivated only after the stock receiver has acquired the substitute source.

No initial contention against a continuously active reference source and no jamming are tested. Operational range, in-flight validation, use of artificial intelligence for acquisition or classification, military systems, operational effectiveness, generalization to all hardware, bands, profiles, or versions, and general neutralization of an aircraft remain outside the experimental scope and, where applicable, are left to future work.

4. Cross-Version Reconstruction

The audit pins tags 1.2.1, 2.5.2, 3.3.2, 3.6.4, 4.0.1, and 4.1.0 of the official repository [6, 9]. Tag 4.1.0 corresponds locally to commit `a9d4a9c`, whose full hash is provided in the artifact. The scope of the audit and retained diffs is limited to files involved in the OTA, CRC, UID, SYNC, nonce, and FHSS rules, as well as the definition of the radio profiles used by H44F-A. The complete upstream repository is not redistributed; the artifact retains the URL, tag, commit, license hash, notices, narrow excerpts, and a deterministic retrieval script.

Cross-cutting invariants and version boundaries. The major version number does not by itself partition the algorithms. The pinned references share MD5-based UID derivation and the 50 Hz sub-GHz profile (BW500, SF8, CR4/7, preamble 10, 20 ms, one hop every four packets, and an 8-byte payload). The PRNG files have the same hash across the 37 tags from 2.0.0 through 4.0.1; version 4.1 retains the same LCG and bounded draw.

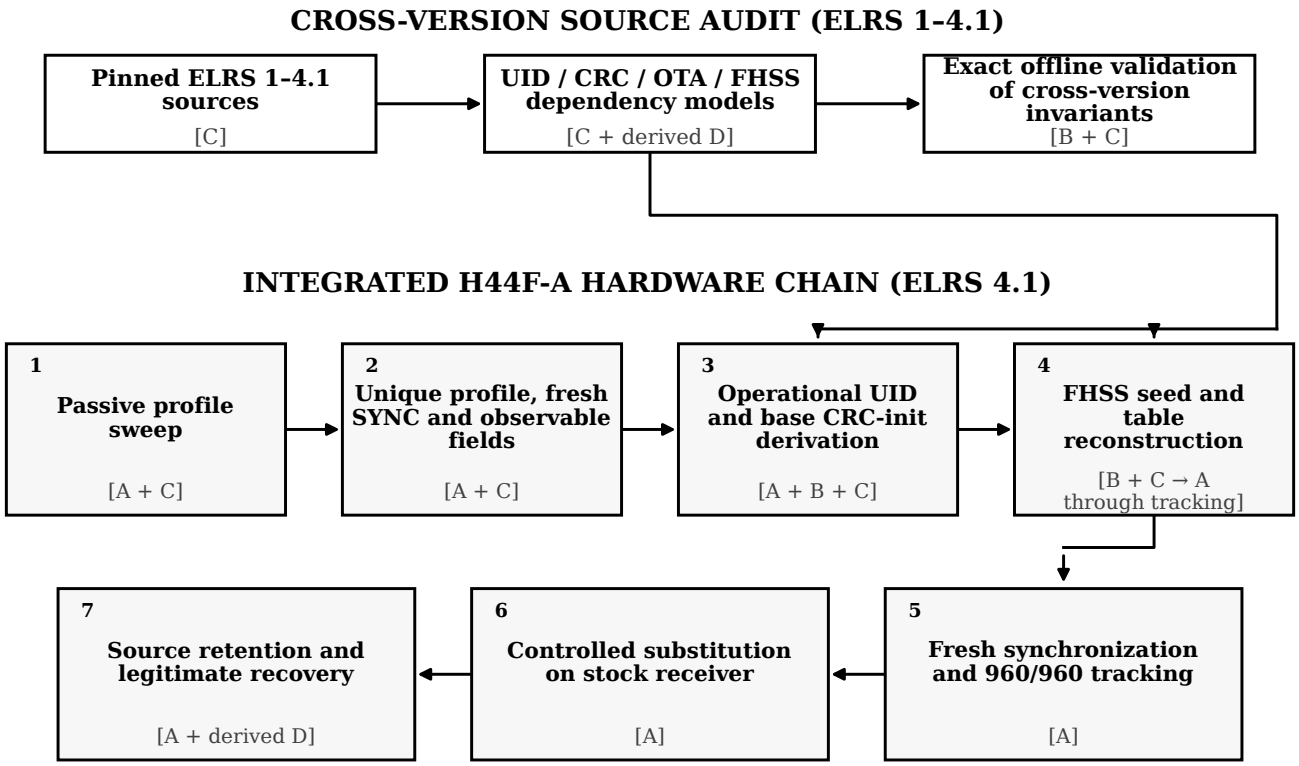


Figure 1: Cross-version and H44F-A hardware chain of evidence. The audit of pinned ExpressLRS 1 through 4.1 sources establishes the UID, OTA, CRC, and FHSS dependencies used by the offline reconstructors. H44F-A reconstructs from pinned sources the SX126x-compatible ExpressLRS 4.1 FCC915 radio profiles, applies them successively in receive-only mode, and dynamically selects at runtime a unique profile from SYNC frames with correct structure and valid CRC. After independent confirmation, state clearing, and radio reset, its blind core reconstructs the operational identity, seed, FHSS table, and synchronization state. It then validates tracking of 960/960 packets, controlled substitution on a stock receiver, retention of the substitute source after the reference returns, and recovery of the latter after the substitute is stopped. Each transition is assessed separately; the software audit does not imply universal RF validation of untested versions, bands, radios, or profiles.

Versions 2–4 also share block-based FHSS shuffling, but not all of its parameters.

Within 3.x, extraction distinguishes three FHSS code organizations: 3.0.0–3.2.1, 3.3.0–3.3.2, and 3.4.0–3.6.4. The native FCC915 harness nevertheless classifies 3.2.1, 3.3.2, and 3.6.4 in the same behavioral family for ten reserved seeds. Likewise, 4.0 and 4.1 are identical for the selected OTA/FHSS rules, not as complete firmware images. Discontinuities remain property-specific: a 256-position allocator in 1.x; a 240-position block table in 2.x; seed, CRC, and SYNC changes in 3.x; and new SYNC frames and nonce-dependent CRC state in 4.x. A common invariant therefore extends only the software evidence for that invariant, never RF evidence for an untested version.

Bounding and reconstruction of the profile space. The profile space must be distinguished according to the level considered. In ExpressLRS 4.1, the upstream tables for the SX127x, SX128x, and LR1121 families contain a total of 36 compilable entries. After entries corresponding to the same logical profile are removed, 24 distinct profiles remain. The 900 MHz subset formed by the union of the SX127x and LR1121 tables contains nine logical profiles:

$$\left|\mathcal{P}_{4.1}^{\text{entries}}\right| = 36, \qquad \left|\mathcal{P}_{4.1}^{\text{logical}}\right| = 24, \qquad \left|\mathcal{P}_{4.1}^{900}\right| = 9. \quad (1)$$

These nine 900 MHz profiles include the following logical rates:

- `FSK_900_1000HZ_8CH`;
- `LORA_900_250HZ`;
- `LORA_900_200HZ_8CH`;
- `LORA_900_200HZ`;
- `LORA_900_100HZ_8CH`;
- `LORA_900_100HZ`;
- `LORA_900_50HZ`;
- `LORA_900_25HZ`;
- `LORA_900_50HZ_DVDA`.

The H44F-A campaign does not scan this global space. The reference source uses the SX127x radio family at 900 MHz; the relevant subset therefore consists of the six logical profiles defined in the corresponding upstream table:

$$\mathcal{P}_{\text{H44F-A}} = \mathcal{P}_{4.1}^{\text{SX127x,900}}, \qquad |\mathcal{P}_{\text{H44F-A}}| = 6. \quad (2)$$

Table 1: Pinned FCC915 family dependencies used by the reconstruction. Concatenation is denoted by ‖. ELRS 4 non-SYNC CRC state also includes the OTA nonce.

Reference	OTA ID	Base CRC init.	FHSS seed	Generator	L	Sync ch.
1.2.1	none	$u_4 \| u_5$	$u_2 \| u_3 \| u_4 \| u_5$	legacy balanced	256	0
2.5.2	none	$u_4 \| u_5$	$u_2 \| u_3 \| u_4 \| u_5$	block shuffle	240	20
3.3.2/3.6.4	3	$(u_4 \| u_5) \oplus 3$	$u_2 \| u_3 \| u_4 \| (u_5 \oplus 3)$	block shuffle	240	21
4.0.1/4.1.0	4	$(u_4 \| u_5) \oplus (4 \ll 8)$	$u_2 \| u_3 \| u_4 \| (u_5 \oplus 4)$	block shuffle	240	20

The three 900 MHz profiles not included in this subset belong to the LR1121 table:

$$\mathcal{P}^{900}_{4.1} \setminus \mathcal{P}_{\text{H44F-A}} = \left\{ \begin{array}{l} \texttt{FSK\_900\_1000HZ\_8CH}, \\ \texttt{LORA\_900\_250HZ}, \\ \texttt{LORA\_900\_200HZ\_8CH} \end{array} \right\}. \quad (3)$$

The six logical H44F-A profiles nevertheless correspond to only five distinct hardware receive configurations on the SX1262. The `LORA_900_200HZ` and `LORA_900_50HZ_DVDA` profiles share the same receive PHY tuple: spreading factor 6, 500 kHz bandwidth, coding rate 4/7, an 8-symbol preamble, and an 8-byte payload.

Let ϕ denote the mapping that associates each logical profile with its SX1262 hardware receive configuration:

$$|\phi(\mathcal{P}_{\text{H44F-A}})| = 5. \quad (4)$$

The mapping ϕ is therefore not injective: two logical profiles share the same receive PHY configuration. Their logical distinction then depends on the enumerated rate carried by the SYNC frame and on the timing constraints associated with the profile, rather than solely on the SX1262 tuple.

A naive combinatorial bound can be obtained by independently considering all values encountered in the fields of the six profiles:

$$\begin{aligned} N_{\text{naive}} &= 6_{\text{enum}} \times 4_{\text{SF}} \times 1_{\text{BW}} \times 2_{\text{CR}} \times 2_{\text{preamble}} \times 4_{\text{interval}} \\ &\quad \times 2_{\text{hop}} \times 2_{\text{payload}} \times 2_{\text{sends}} \times 5_{\text{ToA}} \times 1_{\text{frequency}} \\ &= 15\,360. \end{aligned} \quad (5)$$

This value is artificial and does not constitute a useful operational bound. The enumerated rate, spreading factor, coding rate, preamble length, packet interval, hop interval, number of transmissions, and time on air are not independent: they are grouped into coherent tuples in the upstream code.

Retaining only the main PHY dimensions encountered in the six profiles, four spreading factors, one bandwidth, two coding rates, two preamble lengths, and two payload lengths would produce at most

$$N_{\text{PHY,theoretical}} = 4 \times 1 \times 2 \times 2 \times 2 = 32 \quad (6)$$

theoretical PHY combinations.

If both IQ orientations were treated as an independent dimension, this bound would become

$$N_{\text{PHY+IQ,theoretical}} = 32 \times 2 = 64. \quad (7)$$

Adding two CRC-format hypotheses, for example CRC-8 and CRC-14, would yield a relaxed bound of

$$N_{\text{PHY+IQ+CRC,theoretical}} = 32 \times 2 \times 2 = 128. \quad (8)$$

This last value describes a hypothetical PHY–OTA space. It does not correspond to the space actually tested by H44F-A, because IQ orientation, CRC width, OTA format, and payload are constrained by the version and by the tuples defined in the sources.

The operational bound for H44F-A therefore remains

$$\begin{gathered} N_{\text{logical}} = 6, \qquad N_{\text{RX,distinct}} = 5, \\ N_{\text{expected,winners}} = 1. \end{gathered} \quad (9)$$

H44F-A reconstructs from pinned sources the six logical profiles of the SX127x 900 MHz family, translates them into SX1262 receive parameters, and applies them successively in receive-only mode. The active profile is neither provided by an oracle nor fixed at compile time: it is dynamically selected at runtime from RF observations and then confirmed by an independent acquisition before transition to the blind core.

Profile selection transfers no identity state. After confirmation, the scan, classifier, and identity states are cleared, and the radio is reset. The blind core then acquires a new SYNC using only the selected radio profile.

UID, OTA, and CRC dependencies. Let $u_i = \text{UID}_i$, $v = \text{OTA\_VERSION\_ID}$, ‖ denote byte concatenation, and n the OTA nonce. Code review yields

$$I_{1,2} = (u_4 \ll 8) \mid u_5, \quad (10)$$

$$I_3 = \big((u_4 \ll 8) \mid u_5\big) \oplus v, \quad v = 3, \quad (11)$$

$$I_4 = \big((u_4 \ll 8) \mid u_5\big) \oplus (v \ll 8), \quad v = 4. \quad (12)$$

For ExpressLRS 4.x, the effective initialization is

$$I'_4(p, n) = I_4 \oplus \begin{cases} 0, & p = \texttt{SYNC}, \\ n, & \text{otherwise}. \end{cases} \quad (13)$$

The selected standard path implements a CRC-14 with polynomial `0x2E57`. The OTA format, CRC width, and this polynomial are known from the pinned public sources; they are not reconstructed by the campaign. These equations describe an error-detection state and consistency with a candidate state. They describe neither authentication, encryption, nor a confidentiality mechanism. The CRC is not a keyed MAC.

Generation and length of FHSS tables. The FHSS seeds are

$$s_{1,2} = (u_2 \ll 24) \mid (u_3 \ll 16) \mid (u_4 \ll 8) \mid u_5, \tag{14}$$
$$s_{3,4} = (u_2 \ll 24) \mid (u_3 \ll 16) \mid (u_4 \ll 8) \mid (u_5 \oplus v). \tag{15}$$

In H44F-A, the final `F4` byte of the ELRS 4 seeds is thus derived, not directly observed: `UID5` $\oplus$ `OTA_VERSION_ID` = `F0` $\oplus$ `04` = `F4`.

ExpressLRS 1 uses a balanced allocation of length 256, with channel 0 for SYNC. Later families use block-based shuffling:

$$L = F \left\lfloor \frac{256}{F} \right\rfloor, \tag{16}$$

where F is the number of frequencies in the domain. For FCC915, $F = 40$ and $L = 240$. The SYNC index is 20 for ExpressLRS 2 and 4, and 21 for ExpressLRS 3.

Table 1 provides a compact synthesis of these pinned dependencies. ExpressLRS 4.0 and 4.1 are equivalent for the selected rules, but not for the complete firmware.

4.1 Binding-Phrase Search and Observation-Guided Reconstruction

The role of MD5 must be distinguished from a collision or a generic preimage attack. In the tested implementation, MD5 is a fast, deterministic, unsalted identity-derivation mechanism. The first six bytes of the digest form the radio UID from the compilation definition

```
-DMY_BINDING_PHRASE="<binding phrase>"
```

For a candidate phrase p, let

$$U(p) = \mathrm{Trunc}_{48}(\mathrm{MD5}(\texttt{-DMY\_BINDING\_PHRASE="}p\texttt{"})) \,. \tag{17}$$

A human-generated, predictable, or reused phrase can therefore be tested offline by dictionary: each candidate is converted into the compilation preimage, hashed and truncated, and then compared with the UID bytes reconstructed through RF observation. If only UID2 through UID5 are reconstructed, the comparison can be limited to those four bytes. The absence of a salt also allows the same computations to be reused across devices configured with the same phrase. The relevant properties here are determinism, speed, absence of salt, and truncation; an MD5 collision is not required for this search.

Conversely, a uniformly random 128- or 256-bit phrase makes dictionary recovery impractical. H44F-A uses an even longer random input. A subsequent private verification yields the nominal UID `E9:79:3F:35:59:F0`, while the blind reconstruction obtains `UID2=3F|BF`, UID3–UID5 `35:59:F0`, the base CRC initializer `0x5DF0` derived from UID4/UID5, and seeds `0x3F3559F4`/`0xBF3559F4`. The original phrase is not recovered. Its recovery is unnecessary for the demonstrated controlled substitution: the campaign directly reconstructs the operational derivatives needed for tracking and radio acceptance.

FHSS equivalence classes. Let c be an identity candidate or, equivalently for FHSS generation, a seed candidate. Let $h_c(j)$ denote the frequency predicted by that candidate at table position j. Literal identity values are grouped into FHSS equivalence classes by

$$\begin{aligned} c_a \sim c_b \iff & \big(h_{c_a}(0), \ldots, h_{c_a}(L-1)\big) \\ & = \big(h_{c_b}(0), \ldots, h_{c_b}(L-1)\big). \end{aligned} \tag{18}$$

This relation concerns complete equality of the radio tables, not literal equality of the UIDs. Two distinct UID values can therefore belong to the same FHSS equivalence class and remain indistinguishable from observation of the hopping sequence alone. The nominal UID and the FHSS equivalence class are thus distinct objects. A subsequent private verification may identify the nominal UID, but it is excluded from the blind reconstruction verdict.

FHSS is here a deterministic frequency-distribution mechanism. Knowledge or reconstruction of its table does not constitute source authentication.

In the tested generation path, the most significant bit of UID2 does not distinguish the FHSS table: `UID2`=x and `UID2`=$x \oplus$ `0x80` belong to the same effective class. Once UID4 and UID5 have been obtained from a valid SYNC, the useful space over the seven least significant bits of UID2, denoted `UID2[6:0]` or `UID2 & 0x7F`, and over UID3 therefore contains

$$2^7 \times 2^8 = 32\,768 \tag{19}$$

classes, rather than 65 536 nominal byte pairs. A corpus containing a 240-position table for each class represents

$$32\,768 \times 240 = 7\,864\,320 \tag{20}$$

raw channel bytes, or approximately 7.5 MiB before metadata and indexing. This size permits deterministic preconstruction of the table corpus.

Reduction of the candidate space. For an observed frequency f_k at position i_k, the compatible candidate set is reduced by

$$\mathcal{C}_{k+1} = \{c \in \mathcal{C}_k \mid h_c(i_k) = f_k\} \,. \tag{21}$$

Each positive observation thus eliminates candidates whose predicted frequency differs from the observed frequency.

The offline implementation constructs the inverted index

$$(i_k, f_k) \longmapsto \{c \mid h_c(i_k) = f_k\}. \tag{22}$$

Each candidate set is represented by a bit vector stored in an arbitrary- precision Python integer; pruning then reduces to successive `AND` operations. Only positive observations are used as hard constraints. A missing packet may result from timing error, channel loss, a telemetry slot, or a receiver state unrelated to the candidate; it is therefore not interpreted as evidence of invalidity.

If the cyclic offset τ is not fixed, an alignment score can be defined as

$$S(c, \tau) = \sum_{k=1}^{N} \mathbf{1}\big[h_c\big((i_k + \tau) \bmod L\big) = f_k\big] \,. \tag{23}$$

The table index is thus evaluated modulo its cyclic length L. H10, H12, and H44F-A nevertheless use exact intersection of constraints followed by validation on independent observations, rather than a verdict based on a threshold applied to S.

5. Experimental Method

Evidence is classified as A (hardware measurement), B (exact offline result), C (pinned upstream source), D (documented derived analysis), E (interpretation), or F (not demonstrated). Class E and F items are never presented as experimental results. Each quantitative value points to a primary file, a locator, a verifier, and a SHA-256 hash. Figures are regenerated from read-only working copies. Original code, upstream material, their anchors, and narrow semantic comparisons are kept separate and are not relicensed.

The ExpressLRS 3 tests use a Heltec WiFi LoRa 32 V3 board equipped with an SX1262 as a receiver and, only during protected active phases, as a laboratory transmitter [10]. The ExpressLRS 4.1 tests use an EMAX NANO 900TX module as the reference source, an unmodified stock receiver, a Heltec/SX1262 board as the programmable source, and an independent CRSF monitor. In the logs and RAW data, the labels *Aeris* and *Heltec* respectively denote the reference source and the substitute source.

H37C, which predates the final campaigns, characterizes in read-only mode the module, software version 4.1.0, and its normal CRSF interface at 400000 baud. It does not initialize the SX1262, does not transmit over RF, and provides neither an OTA profile, identity, nor FHSS table to the final chain.

Selection of the cross-version hardware scope. The inventory of firmware images available for the test bench includes 4.0.0, 4.0.1, and 4.1.0; a 3.x subset extending from 3.0.0 to 3.6.4; and 2.5.0, 2.5.1, and 2.5.2. It includes neither a 1.x image nor a 2.0–2.4 image. The presence of an image is nevertheless insufficient to constitute hardware evidence: a compatible and restorable TX/RX pair, a pinned compilation target, a radio path observable by the instrumentation, and a family-specific verification protocol are also required.

Versions 3 and 4 were selected for the RF campaigns because these conditions were established on the test bench: the ELRS 3 chain had SX127x/SX1262 targets already characterized in H8B and H15/H16, while the ELRS 4.1 chain had a stock pair, the passive selector, and the integrated H44F-A chain. The level of evidence differs: the 3.x campaigns separate FHSS reconstruction (H8B/H10/H12) from controlled substitution (H15), whereas 4.1 combines both with blind profile selection in an integrated chain.

This choice does not assume four disjoint algorithms. The audit in Section 4 instead shows cross-cutting invariants: a common UID and 50 Hz PHY, an identical PRNG from 2.0.0 through 4.0.1, block-based shuffling common to versions 2–4, and the same FHSS behavior at the three 3.x milestones. Seed, CRC, SYNC, nonce, and OTA format remain treated separately.

The available 2.5.x images did not undergo, in this study, the full hardware preflight required for a comparable blind campaign. Because the selected 4.0 and 4.1 rules are identical in the pinned diff, the complete hardware campaign was executed on 4.1; this source-level equivalence does not turn 4.0 into an RF validation. Selection of the 3.x and 4.1 configurations therefore constitutes reasoned sampling of two instrumentable hardware paths. Shared invariants broaden the scope of the software audit, but not that of the RF evidence.

Development chronology and final campaign. The fixed-profile reconstruction core was first validated in the intermediate H43 runs, after which the passive selector was developed separately under the H44 alias. These identifiers describe the development chronology and remain attached to their historical artifacts. The final H44F-A campaign then combines both stages in a single firmware image, serial protocol, log, and verdict. Its execution order is profile selection, clearing and reset, followed by blind reconstruction from a fresh SYNC. Counters from the intermediate campaigns are not aggregated with those of H44F-A.

H44F-B is subsequently executed as a complementary and independent passive hardware validation. It repeats blind profile selection and UID2/UID3 reconstruction, but bounds probing to five observations and reserved tracking to five hops. It remains receive-only and performs neither substitution, retention, nor source recovery. Its log and verdict are not aggregated with those of H44F-A.

Dynamic radio-profile selection. The first stage of H44F-A replaces the radio profile previously fixed at compile time with dynamic runtime selection. The six logical ExpressLRS 4.1 SX127x/900 MHz profiles are reconstructed from pinned sources, translated into SX1262 receive parameters, and then applied successively in receive-only mode on their respective SYNC frequencies.

For each candidate profile ρ_j, H44F-A records, among other values, the radio rate, spreading factor, bandwidth, coding rate, preamble, payload length, packet interval, hop interval, time on air, number of completed receptions, SYNC candidates, and valid SYNC frames. A profile passes the first stage when it produces a SYNC frame with correct structure and valid CRC.

The scan must produce exactly one winner. No valid profile or multiple winners cause the chain to stop without enabling RF transmission by the Heltec platform. The selected profile is then subjected to an independent acquisition that confirms the same radio rate and the same UID4/UID5 bytes.

After confirmation, the scan, classifier, and identity states are cleared, and the radio is reset. No identity byte is passed to the blind core. Only the dynamically selected radio profile is retained.

The first part of the preregistered chain is therefore

profiles derived from sources → receive-only scan
↓
unique profile → independent confirmation
↓
state clearing and reset
↓
transfer of the profile alone to the blind core.

H44F-A is executed without a profile or identity oracle and without a binding phrase. During scanning, the Heltec/SX1262 remains in receive-only mode and does not transmit; the reference source emits the observed SYNC frames. Guard criteria include the absence of any call placing the Heltec in transmit mode, state clearing, absence of identity transfer, and acquisition of a new SYNC by the core after reset.

Blind reconstruction and FHSS tracking. Starting from the selected profile, the H44F-A blind core begins without a compiled UID, CRC initialization, seed, or FHSS table, and without a binding phrase or identity oracle. The preregistered integrated chain is

blind SYNC → (u_4, u_5, I_4) → probing
↓
(u_2, u_3) → FHSS table → fresh SYNC
↓
960/960 tracking; CRC/channel errors: 0
RX–TX transition→substitution
↓
return of reference → retention of substitute
↓
stop substitute → recovery of reference.

UID4/UID5 are read from each candidate SYNC; the public version-specific rule derives a base CRC initializer from them, after which the recomputed CRC validates or rejects the candidate. This initializer is therefore not an independent measurement. Positive observations associating a table index with a frequency channel then constrain UID2/UID3. Two candidates differing only in bit 7 of UID2 are retained when their 240-position tables are strictly identical. They then constitute the same FHSS equivalence class, without by themselves determining the nominal UID.

Tracking requires a complete traversal of the table, at least 500 valid packets, no CRC error, no divergence between the predicted and observed channel, and no use of an identity oracle. The final campaign uses 960 slots, corresponding to 240 hops and coverage of all 240 table positions.

After tracking, a new SYNC is acquired before the RX–TX transition. The reference source is then intentionally interrupted before substitute transmission begins. It is reactivated only after the stock receiver acquires the substitute source. The final phase successively verifies substitution, retention of the substitute source after the reference returns, and recovery of the latter after the substitute source is stopped.

Source attribution. The reference and substitute sources generate distinct, preregistered, multichannel CRSF signatures. The offline parser verifies each 26-byte RC frame, its CRSF CRC-8 with polynomial `0xD5`, its format, sequence continuity, and its 16 channels before attributing it to the reference source, the substitute source, or the `unknown` class.

This CRC-8 applies to the CRSF serial layer; it is distinct from the CRC-14 `0x2E57` of the OTA radio packets and does not authenticate their source.

Source attribution is independent of the RF demodulation used for reconstruction. It verifies which source effectively controls the receiver during the reference-only, substitution, simultaneous-presence, and recovery phases.

The binding phrase remains separate from the blind protocol. It is never provided to the firmware, reconstructor, or primary verifier. It is used only for a subsequent private check of the nominal UID, explicitly excluded from the blind verdict.

Metrics. The conditional tracking rate and scheduling residual are defined as

$$P_{\text{track}} = \frac{N_{\text{matched}}}{N_{\text{observed}}}, \qquad r_k = t_k - (t_0 + kT_s). \tag{24}$$

The reported maximum residual is

$$r_{\max} = \max_k |r_k|. \tag{25}$$

P_{track} is conditioned on the slots actually observed during the tracking window. It is neither a universal estimate of the link delivery rate, nor a range measurement, nor evidence of RF dominance.

The hardware verdict is supplemented by offline verification of the logs and RAW captures. This verification checks the blind contracts, scan uniqueness, profile confirmation, state clearing, reconstruction, tracking, operator events, complete capture, absence of binding-phrase disclosure, and final safe state. A run is declared PASS only if the embedded and offline verdicts agree and no mandatory check fails.

6. Results

The offline validations compare the independent Python implementations with separately compiled C++ references derived from the pinned upstream sources over 39 845 888 inputs and 32 768 `UID2[6:0]`/UID3 classes per reference, without divergence. The initial multi-version validator covers 31 981 568 inputs; its negative control passes and all 64/64 deterministic round trips are exact. A complementary validation specific to the pinned ExpressLRS 4.1.0 tag then compares 7 864 320 positions directly with upstream commit `a9d4a9cb5b5687c4c9d7e9e7fbdf44ad93651da6`, also without divergence. ExpressLRS 1 accounts for 8 388 608 length-256 inputs; ExpressLRS 2, 3, 4.0, and 4.1 each account for 7 864 320 length-240 inputs. The selected 4.0 and 4.1 matrices are identical, but their comparisons with the two pinned upstream references were executed and are counted separately. These results concern the

selected software models; they are not RF validations of complete firmware families.

Earlier campaigns separately establish the elementary stages. H8B records 44 877 valid-CRC matches over 44 902 slots, without channel divergence, across all 240 table positions and 46 cycles. H10 and H12 independently reduce 128 radio classes to one and respectively validate 30/30 and 48/48 reserved positions. Figure 2 places these reductions alongside the complementary H8B, H15, H28, and H44F-A validations without aggregating their metrics of different kinds.

H15 performs six controlled ExpressLRS 3 cycles and 5 574/5 574 `TxDone` events. Its 16-state sequence varies CH1–CH4, with throttle at minimum and safe AUX channels held low; it therefore does not demonstrate arbitrary control of the entire AUX space.

H28 performs five ExpressLRS 4.1 runs with known identity, totaling 4 800 tracking windows and all 240 table indices per run, with a maximum residual of 409 μs. Conversely, H29F validates no blind candidate, H38F observes 148 `RxDone` events without a valid SYNC, and H39 fails before capture. These negative results remain valid for their respective experimental paths; H44F-A uses a distinct integrated chain and does not retroactively reclassify them.

6.1 H42B_R2: Preparatory Characterization of Attribution and Retention

H42B_R2 is a preparatory source-characterization campaign; it does not perform the integrated blind reconstruction of H44F-A. Its parser reproduces 4 875/4 875 RAW RC frames without CRC, format, or sequence errors and without an unknown source.

In `BOTH_ON_1`, the reference source is established first: 1 253/1 253 frames are attributed to Aeris and none to Heltec. After the reference is interrupted, all 1 334/1 334 frames in `AERIS_OFF_1` are attributed to Heltec. Approximately 5.98 s separate the last Aeris frame from the first Heltec frame.

After the reference returns, all 1 287/1 287 frames in `BOTH_ON_2` remain attributed to Heltec, without alternation, merging, or unknown source. Finally, all 1 001/1 001 frames in `AERIS_OFF_2` remain attributed to Heltec. H42B_R2 thus establishes multichannel attribution and continuity in favor of the already acquired source; it does not demonstrate initial preemption of a continuously active source.

6.2 H44F-A: Integrated Blind Campaign

H44F-A combines in a single firmware image and a single log passive profile selection, blind reconstruction of the operational identity, FHSS tracking, and controlled active validation. The campaign is identified by the public UUID `5e47158c-14cb-4395-a803-47ea468e8e8a`; no absolute timestamp is used as an alias in the article.

Wired CRSF stimulation of the reference module sends 9 459 frames without a write error. During scanning, the Heltec SX1262 remains in receive-only mode: `heltec_rf_tx=0`, and no call places it in transmit mode. The six logical ExpressLRS 4.1 SX127x/900 MHz profiles reconstructed from pinned sources are tested. Only one produces a SYNC that simultaneously satisfies structure, enumerated-rate, and CRC checks: `LORA_900_50HZ`. It uses SF8, 500 kHz, coding rate 4/7, a 10-symbol preamble, an 8-byte payload, a 20 000 μs interval, and one hop every four frames.

An acquisition after a complete reset independently confirms the same rate and the same UID4/UID5 bytes. The scan, classifier, and identity states are then cleared; the stimulus is stopped, GPIO47 is returned to input mode, and no identity byte is passed to the blind core. The four selection gates are

$$\begin{aligned} &\texttt{profile\_sweep\_pass} = 1, && \texttt{profile\_lock\_pass} = 1,\\ &\texttt{profile\_confirm\_pass} = 1, && \texttt{handoff\_pass} = 1. \end{aligned} \tag{26}$$

The core starts again from a fresh SYNC, without a compiled UID, base CRC initializer, seed, or FHSS table, without a binding phrase, and without an identity oracle. Probing over 3 000 slots records 64 positive observations. The reconstruction obtains UID2 `3F|BF`, UID3–UID5 `35:59:F0`, the base CRC initializer `0x5DF0` derived from UID4/UID5, and seeds `0x3F3559F4`/`0xBF3559F4`, whose 240-position tables are identical. The `F4` suffix of the seeds results from `F0` $\oplus$ `04`. All embedded criteria are satisfied:

$$\begin{aligned} &\texttt{blind\_sync\_pass} = 1, && \texttt{probe\_pass} = 1,\\ &\texttt{reconstruction\_pass} = 1, && \texttt{fhss\_follow\_pass} = 1,\\ &\texttt{takeover\_pass} = 1, && \texttt{incumbent\_lock\_pass} = 1,\\ &\texttt{aeris\_recovery\_pass} = 1, && \texttt{raw\_pass} = 1,\\ & && \texttt{final\_safe} = 1. \end{aligned} \tag{27}$$

Tracking covers 960 slots, 240 hops, and all 240 table positions. It produces 960 `RxDone` events and 960 valid packets, without a CRC error or channel divergence; the maximum residual is 2 327 μs. After acquiring a new SYNC and physically interrupting the reference, the bounded TX phase covers 6 000 slots: 5 625 transmissions result in 5 625 `TxDone` events, with 375 telemetry slots, no timeout, no resynchronization failure, and zero final radio errors.

The parser attributes 1 533/1 533 commands to Heltec during source substitution and 3 698/3 698 to the same source after Aeris returns, with no Aeris frame or unknown source in either phase. After Heltec is stopped, the recovery phase contains 439 Aeris frames and one final Heltec frame, without an unknown source and with a single transition. Approximately 5.584 s separate the last Heltec frame from the first Aeris frame.

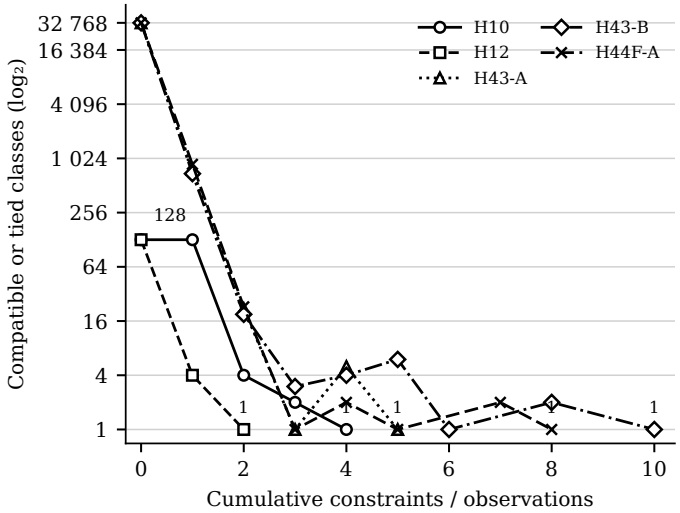
The core verdict, overall verdict, and their offline verifications are all `PASS`. The capture contains 5 671 RAW lines without CRC, format, or sequence errors and without overflow. Final shutdown disables RF transmission and returns GPIO47 and GPIO42 to input mode. The SHA-256 hash of the sanitized and verified public log is `e8e4a73a0d802861cec98e5ef0a34aaf2366cd9e5624b872626d3cb764fc4aff` . The combined package also provides a normalized replay copy obtained by removing only binary startup noise; its hash is `bf9f6e041be81515d1c5c9a996f68fc804ff9fa129a5324f5dc11ab3c23f818e`. The manifest retains both hashes and explicitly documents this derivation.

H44F-A therefore constitutes the integrated validation of the complete chain:

Table 2: Evidence-bounded validation of the tested tags and configurations. Host/source validation covers selected reconstruction rules, not a complete firmware family. The ELRS 3 hardware row identifies the actual H8B bench versions. "Substitution" denotes controlled source acceptance on a stock receiver, not arbitrary AUX control or initial preemption of a continuously active source.

Tested tag/configuration	Offline/source validation	Passive RF	Real-time tracking	Substitution
1.2.1	HOST VALIDATED	NOT TESTED	NOT TESTED	NOT TESTED
2.5.2	HOST VALIDATED	NOT TESTED	NOT TESTED	NOT TESTED
3.3.0 TX / 3.3.2 RX	SOURCE VALIDATED	DEMONSTRATED	DEMONSTRATED	DEMONSTRATED
3.6.4	HOST VALIDATED	NOT TESTED	NOT TESTED	NOT TESTED
4.0.1	HOST VALIDATED	NOT TESTED	NOT TESTED	NOT TESTED
4.1.0	HOST/UPSTREAM VALIDATED	DEMONSTRATED	DEMONSTRATED	DEMONSTRATED

(a) Reduction and convergence



(b) Complementary validations

Campaign	Measure	Coverage / errors
H8B	44,877 / 44,902	240 pos.; mism. 0
H10	30/30 held out	30 chan.; mism. 0
H12	48/48 held out	27 chan.; mism. 0
H15	5,574/5,574 TxDone	6 cycles
H28	4,800 windows	5 runs; 240 idx/run
H44F-A	960/960 packets	240/240 pos.; errors 0

Figure 2: Reduction of FHSS classes and complementary experimental validations. On the left, H10 and H12 apply exact intersection to 128 classes. H43-A, H43-B, and H44F-A start from 32 768 canonical `UID2[6:0]`/UID3 classes; their curves show the number of classes tied for the best cumulative score until a unique class stabilizes. A temporary increase therefore represents a new tie, not the reintroduction of a class eliminated by exact intersection. On the right, metrics remain expressed in their own units for H8B, H10, H12, H15, H28, and H44F-A; they are not aggregated. Counts denote radio-table classes, not literal UIDs.

dynamic profile selection
↓
blind reconstruction → 960/960 FHSS tracking
↓
controlled substitution
↓
retention after return of reference
↓
recovery after substitute is stopped.

The intermediate development campaigns remain preserved in the historical artifact with their own verdicts. They separately validated the fixed-profile blind core and then the passive selector. They are not aggregated with the H44F-A counters and do not carry the verdict of the final campaign.

6.3 H44F-B: Passive Five-Hop FAST Validation

H44F-B is a distinct passive hardware repetition identified by public UUID `583431a1-9948-4173-9b9b-14954169cb33`. It selects and cold-confirms the same `LORA_900_50HZ` profile, clears identity state, and then acquires a new CRC-valid SYNC. Probing stops after five positive observations at five distinct FHSS indices.

The exhaustive search over 32 768 canonical `UID2[6:0]`/UID3 classes leaves a unique class: UID2 `3F|BF`, UID3 `35`, with UID4/UID5 `59:F0` and seeds `0x3F3559F4`/`0xBF3559F4`. Four observations match the table exactly and one uses the bounded tolerance of an adjacent channel. A fresh acquisition then validates the table without tolerance over five hops and 20/20 CRC-valid packets, with zero channel divergence and a maximum residual of 2 006 μs.

The embedded verdict and offline replay are both `PASS`. The hash of the anonymized replay log is `fefe06180f79758c58160a60110ebeab99e778eea659a21b36feca105e9fc83b`. The Heltec SX1262 remains in receive-only mode throughout the campaign, and final shutdown returns GPIO47 to input mode. H44F-B therefore provides hardware confirmation of fast passive reconstruction in this session; it demonstrates neither substitution, retention, nor source recovery and does not replace H44F-A.

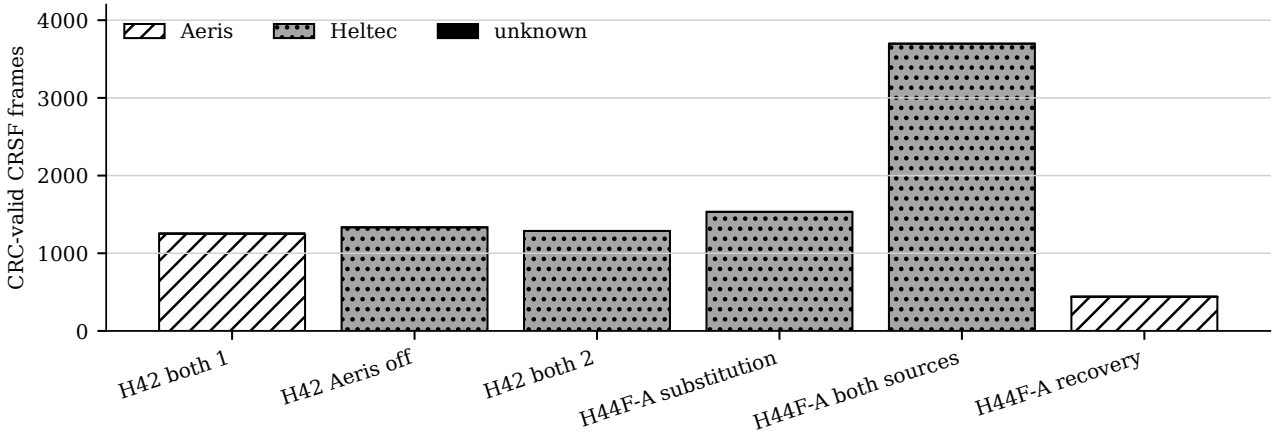


Figure 3: Source attribution regenerated from the H42B_R2 and H44F-A RAW captures. H44F-A transmission begins after intentional interruption of the reference; the "both on" phase measures retention of the substitute source, not initial contention against a continuously active source. The terminal `AERIS_OFF_2` phase of H42B_R2 is not shown.

Table 3: Compact result summary. Primary evidence and derived interpretation are separated; levels are defined in Section 5.

Campaign	Tag/profile	Result and boundary	Primary evidence	Derived interpretation
Offline	1.2.1/2.5.2/3.6.4/ 4.0.1/4.1.0	Independent Python/C++ comparisons: 39,845,888 entries, 0 mismatch	B, C	–
H8B/H10/H12	3.3.0 TX/3.3.2 RX	44,877 packet/channel matches; one held-out FHSS class	A, B, C	D
H15	3.3.x	6/6 cycles; minimum throttle and safe AUX unchanged	A	–
H42B_R2	4.1.0	4,875 clean attributed frames; acquired-source retention	A, B	D
H44F-A	4.1.0 / selected 50-Hz profile	Unique blind profile; reconstruction; 960/960 following; substitution, retention, and recovery on stock RX; 5,671 integral RAW frames	A, B, C	D
H44F-B	4.1.0 / selected 50-Hz profile	Separate RX-only validation; one class after five observations; held-out five-hop follow and 20/20 valid packets, without mismatch	A, B, C	D

7. Security Implications and Countermeasures

7.1 Protocol Positioning and Scope of the Analysis

ExpressLRS is an open-source protocol designed primarily as a high-performance radio-control link for FPV use: low latency, range, radio robustness, spectral efficiency, and compatibility with constrained hardware [6, 8]. Within that scope, its architecture is coherent and particularly effective.

ExpressLRS is nevertheless neither presented nor evaluated by the project as a secure command-and-control system hardened against an active adversary, or as a certified military link. The present study therefore does not show that the protocol fails to fulfill its primary function. It examines what occurs when a civilian, performance-oriented link is placed within a cyber-electromagnetic threat model more demanding than that of its intended use.

Potential use of ExpressLRS in a contested, safety-critical, or military environment changes the threat model without retroactively changing the protocol's design goals. The results presented should therefore be understood as an analysis of the gap between these two contexts, not as an attack on the project, its developers, or the quality of its engineering.

7.2 Binding Phrase, Entropy, and Authentication

A strong binding phrase remains necessary. It should be generated by a CSPRNG, be unique to each link, and contain no name, date, predictable pattern, or value reused across devices or fleets. A min-entropy of at least 128 bits is a reasonable baseline; a random 256-bit value also remains practical [11, 12, 13].

Such a value primarily protects against direct guessing, dictionary attacks, and reuse of predictable secrets. It remains useful for configuration, coordination, and radio identification. H44F-A does not, however, recover the binding phrase: the campaign directly reconstructs the operational derivatives required for the tested radio state.

The distinction is essential:

> *FHSS is not authentication; a CRC is not a MAC; a strong binding phrase protects against guessing the phrase, but does not necessarily authenticate all operational radio states derived from it.*

The nominal UID and the effective FHSS equivalence class are likewise distinct objects. Several literal values may lead to the same FHSS table and remain indistinguishable from observation of the hopping sequence alone. High input entropy therefore replaces neither cryptographic source authentication, command integrity, nor an authenticated notion of freshness.

The observed issue is not reducible to the use of MD5 for configuration derivation. Replacing only the hash function, without changing the authentication structure of frames and synchronization states, would not be sufficient to prevent reconstruction of operational derivatives or acceptance of a compatible radio source.

7.3 Configuration and Protocol Evolution

In current deployments, users should generate and securely retain a unique random value for each link. Reusing the same phrase across several devices or an entire fleet increases the scope of a compromise and facilitates identity correlation.

A salt can prevent global reuse of some precomputations, but it does not turn a weak phrase into a strong secret. Nor does it authenticate commands, SYNC frames, or state transitions.

For a more demanding security profile, a public radio identity should be separated from an independent authentication secret. A modern, context-specific KDF with domain separation could derive distinct keys for authentication, synchronization, and, where necessary, confidentiality.

Commands, critical states, and SYNC transitions should carry authenticated integrity evidence associated with a counter or nonce that is itself authenticated. The protocol should then explicitly define:

- replay protection;
- persistence of counters across restarts;
- recovery after packet loss;
- secure key renewal;
- behavior during desynchronization;
- absence of a trust reset through unauthenticated resynchronization.

The experimental result primarily identifies a need to authenticate integrity and freshness; it does not demonstrate a need for confidentiality. A MAC, for example CMAC or HMAC, associated with an authenticated counter or nonce is therefore a minimal conceptual response [14, 15]. An evaluated AEAD mode such as ChaCha20-Poly1305 becomes relevant only if confidentiality of commands or telemetry is also sought [16].

SYNC frames, counters, and resynchronization transitions must themselves be authenticated; encrypting only the commands would not be sufficient. Given the eight-byte payload of the studied profile, these mechanisms cannot be added as a simple option. They would require a distinct OTA format and experimental evaluation of tag and nonce lengths, throughput, latency, time on air, memory, power consumption, recovery after loss, and backward compatibility.

These proposals correspond to a possible *Secure C2* profile distinct from the nominal FPV profile. They should not impose on the original civilian protocol goals it did not claim, but rather provide a basis for a variant intended for adversarial environments.

7.4 Detection and Defense in Depth

In the absence of complete cryptographic authentication, a complementary defense can monitor:

- discontinuities in SYNC or nonce values;
- unexpected returns to an earlier synchronization state;
- duplicate logical identities associated with different RF fingerprints;
- rapid variations in power, frequency, or origin;
- source changes observed on the command interface;
- unexpected source recoveries or reacquisitions.

These indicators may help detect an anomaly, but they do not constitute cryptographic evidence. Propagation variations, packet loss, legitimate restarts, and power changes can produce false positives. Detection should therefore be considered a defense-in-depth measure, not a substitute for authentication of commands and synchronization states.

Limitations, Ethics, and Disclosure

Disclosure status. Some relevant general properties had already been the subject of public discussion before the present study. No private coordinated-disclosure process with the project maintainers preceded preparation of the manuscript. Relevant stakeholders were nevertheless informed of the identified risks before publication. This statement describes only the disclosure timeline and implies neither validation nor endorsement of the results by the maintainers.

Anonymization and artifact publication. The body of the article identifies campaigns by stable aliases, notably `H42B_R2`, `H44F-A`, and `H44F-B`, rather than by their absolute timestamps. The public manifest associates each alias with a public UUID, the corresponding verdict, the list of its files, and the SHA-256 hashes of the published copies. The UUID serves only as an identifier; integrity is provided by the cryptographic hashes.

Public copies of the logs replace absolute dates with relative times or slot numbers, local paths with relative paths, and machine or session names with generic identifiers. The mapping to the original timestamps and raw logs is retained in a private manifest. Because anonymization modifies the files, the public hashes apply to the sanitized copies, not to the private originals.

The specialized public H44F-A/H44F-B artifact provides both sanitized replay logs, their UUIDs and SHA-256 hashes, the captures and derived tables, and the offline reconstructors, parsers, and verifiers. It provides exact anchors to the upstream commit and a narrow semantic comparison of the six profiles, without reproducing the ExpressLRS sources. The general manuscript package separately retains the historical campaigns and figure-regeneration scripts. The specialized artifact does not publish the binding phrase, directly usable injection tools, ready-to-flash firmware, or operational jamming or neutralization procedures.

This choice enables verification of the passive, logical, and experimental claims from the logs, but limits direct public reproduction of the active phase. This restriction

is part of the stated reproducibility limitations of the public package.

Local availability of a firmware image must not be confused with hardware validation of its family. The inventoried 2.5.x and 4.0.x images did not receive the same preflight, blind campaign, and RF verification as the tested 3.x and 4.1 configurations. Hardware results therefore remain tied to the explicitly reported tags, targets, and TX/RX pairs; they do not extend either to intermediate versions or to all available images.

Conversely, code overlap should not be ignored: an identical PRNG hash or identical FHSS behavior extends software validation of that specific property to the audited tags. This component-by-component extension does not constitute global firmware equivalence and does not replace a configuration-specific RF campaign.

Future work. Future work concerns only properties not demonstrated in the present study: extending the selector to the other 900 MHz profiles and other radio families, implementing GFSK paths, measuring acquisition and recovery thresholds under controlled attenuation, and instrumentally characterizing timing and RF margins.

Further work may study defensive detection of source changes, improvements to PHY acquisition, tracking, sensor fusion, and calibration of confidence scores. Artificial-intelligence assistance for classification or acquisition, controlled jamming, and any form of neutralization remain prospective directions. They are neither implemented, evaluated, nor claimed as results of this article.

8. Conclusion

Within the experimental scope, the answer to the research question is affirmative: the operational physical and logical state of an ExpressLRS link can be reconstructed to a degree sufficient to enable passive tracking followed by controlled source substitution after interruption of the reference.

The integrated H44F-A campaign first establishes, without a profile oracle and in receive-only mode, dynamic selection of the active radio profile among the six ExpressLRS 4.1 SX127x/900 MHz profiles reconstructed from pinned sources. After independent confirmation, state clearing, and radio reset, its blind core starts again from a new SYNC, without a supplied binding phrase, UID, base CRC initializer, seed, or FHSS table.

The non-cooperative RF observations then make it possible to reconstruct the PHY and timing profile, the base CRC initializer derived from UID4/UID5, an FHSS equivalence class of the UID, the seed, the FHSS table, and the current synchronization state. Reconstruction relies on 64 positive frequency observations collected during a 3 000-slot probe.

Passive tracking then validates 960/960 RF packets, corresponding to 240 hops and complete coverage of all 240 positions of the FHSS table, without a CRC failure or channel divergence. This number describes the window dedicated to tracking validation; it does not by itself summarize the entire campaign.

After intentional interruption of the reference source, a separately developed transmitter performs 5 625/5 625 RF transmissions, without a timeout or resynchronization failure, and establishes a link accepted by an unmodified stock receiver. The offline parser then analyzes 5 671 RC frames without CRC, format, or sequence errors: 1 533 are attributed to the substitute source during source substitution, 3 698 remain attributed to that source after the reference returns, and the recovery phase then contains 439 frames from the reference and one final frame from the substitute, with a single transition between the two sources.

The stock receiver therefore retains the substitute source for as long as it remains active, including after the reference is reactivated, and then recovers the reference after the substitute is stopped. The result thus goes beyond the question of reconstruction and tracking alone: it demonstrates controlled source substitution after interruption of the reference, and then experimentally characterizes source retention and recovery.

Dynamic radio-profile selection	YES
Reconstruction of physical state	YES
Operational logical reconstruction	YES
Frequency probing (3 000 slots; 64 positive observations)	YES
FHSS tracking (960/960; 240/240 positions)	YES
CRC errors or channel divergences during tracking	0
Substitute RF transmissions (5 625/5 625)	YES
Validation on a stock receiver	YES
Retention of the already acquired source after the other source reappears	YES
Recovery of the reference after the substitute is stopped	YES
RC frames analyzed (5 671; errors: 0)	YES
Recovery of the original binding phrase	NO, and not required
Source substitution without prior interruption of the already acquired source	NOT TESTED

These conclusions are experimental and bounded to the protocol, version, band, profiles, and hardware tested. The receiver empirically favors continuity of the already acquired source, without automatically returning to the previous source when it reappears. The campaign does not, however, test source substitution without prior interruption of the already acquired source.

The results demonstrate neither recovery of the binding phrase, breaking of encryption, nor a universal capability applicable to all versions, bands, radios, or propagation conditions.

Nor do they constitute a claim of operational range, jamming, or general neutralization. They characterize the gap between a civilian link designed for FPV performance and the properties expected of a secure command-and-control system in an adversarial environment.

Author Contribution and Attribution of Earlier Work

Melik Lemariey: conceptualization of the present ExpressLRS study; methodology; software; firmware; validation; formal analysis; investigation; data curation; visualization; original drafting; review and approval of this preprint.

The ExpressLRS campaigns reported in this manuscript were designed, conducted, and analyzed by Melik Lemariey.

Part of the methodological reasoning continues earlier experimental work conducted collaboratively from 2016 onward on a distinct radio link. Its detailed description and the individual attribution of contributions are deferred in this version pending validation by the participants concerned.

Conflicts of Interest

The author declares no known conflict of interest that could have influenced the conduct, analysis, or presentation of this study.

Data and Code Availability

The associated public repository is `https://github.com/Melik159/elrs-h44f-executable-evidence`.

The specialized public artifact contains the anonymized H44F-A and H44F-B logs, captures and extracted data, reconstructed FHSS tables, verification reports, traceability manifests, and SHA-256 hashes of the published copies. Absolute time identifiers, local paths, and machine names are replaced with stable aliases, public UUIDs, and relative times. The historical H42B_R2 evidence and figure-generation scripts remain distributed separately in the general manuscript package.

The specialized artifact also contains the offline reconstruction and validation code, locators and anchors for the pinned upstream sources, a narrow semantic comparison of the profiles, and a deterministic replay protocol. The original scripts are distributed under Apache-2.0; documentation and sanitized evidence are distributed under CC BY 4.0. Upstream material remains separate, retains its own license, and is not relicensed.

The private binding phrase, the mapping between public identifiers and the original logs, ready-to-use active firmware, and directly operational transmission or injection tools are not distributed. This restriction limits direct public reproduction of the active phases, but does not prevent offline verification of the reported results from the sanitized artifacts.

Declaration of Artificial-Intelligence Use

Generative artificial-intelligence tools assisted with artifact inventory, generation and revision of scripts, preparation of the LaTeX document, consistency checks, and some drafting stages.

These tools produced no experimental measurement and were not used as a source of evidence. The results derive exclusively from the selected captures, logs, programs, and verifiers. Melik Lemariey reviewed the outputs used, verified the claims, and remains solely responsible for the content and approval of the manuscript.

Stakeholder Notification

Relevant stakeholders were informed of the identified risks before publication of this study.

References

[1] Geneviève Baudoin, Martine Villegas, Jean-François Bercher, Corinne Berland, Jean-Marc Brossier, Daniel Courivaud, Nicolas Gresset, Pascale Jardin, Gaëlle Lissorgues, Christian Ripoll, and Olivier Venard. *Radiocommunications numériques. Tome 1 : Principes, modélisation et simulation.* Technique et ingénierie. Dunod, Paris, 2013. 2e édition.

[2] Martine Villegas, Corinne Berland, Daniel Courivaud, Gaëlle Lissorgues, Christian Ripoll, and Odile Picon. *Radiocommunications numériques. Tome 2 : Conception de circuits intégrés RF et micro-ondes.* Technique et ingénierie. Dunod, Paris, 2007. 2e édition.

[3] g3gg0. Analysis of TBS Crossfire, Reverse Engineering the Air Link. Online technical report, August 2021. Separate 900-MHz RC link; accessed 30 July 2026.

[4] Richard Appleby. Technical advisory—ExpressLRS vulnerabilities allow for hijack of control link. NCC Group Research, June 2022. Online advisory, published 30 June 2022; accessed 30 July 2026.

[5] redfiveau and ExpressLRS contributors. Security Improvements, ExpressLRS Pull Request 1411. GitHub, 2022. Closed unmerged; accessed 30 July 2026.

[6] ExpressLRS Project. ExpressLRS Source Repository. GitHub, 2026. Pinned revisions are listed in the artifact; accessed 30 July 2026.

[7] TBS Avionics Co. Ltd. CRSF Protocol Specification. GitHub, 2026. Pinned revision recorded in the artifact; accessed 30 July 2026.

[8] ExpressLRS Project. Binding ExpressLRS. Official documentation, 2026. Accessed 30 July 2026.

[9] ExpressLRS Project. ExpressLRS version 4.1.0 source tree. GitHub source release, 2026. Tag 4.1.0, commit a9d4a9cb5b5687c4c9d7e9e7fbdf44ad93651da6; accessed 31 July 2026.

[10] Semtech Corporation. *SX1261/SX1262 Long Range, Low Power, Sub-GHz RF Transceivers.* Semtech Corporation, 2025. Data sheet; accessed 31 July 2026.

[11] Donald E. Eastlake, 3rd, Jeffrey I. Schiller, and Steve Crocker. Randomness requirements for security. RFC 4086, RFC Editor, June 2005.

[12] Elaine Barker and John Kelsey. Recommendation for random number generation using deterministic random bit generators. NIST Special Publication 800-90A Revision 1, National Institute of Standards and Technology, 2015.

[13] Niels Ferguson, Bruce Schneier, and Tadayoshi Kohno. *Cryptography Engineering: Design Principles and Practical Applications.* Wiley, 2010.

[14] Morris J. Dworkin. Recommendation for block cipher modes of operation: The CMAC mode for authentication. NIST Special Publication 800-38B, National Institute of Standards and Technology, 2016.

[15] Hugo Krawczyk, Mihir Bellare, and Ran Canetti. HMAC: Keyed-hashing for message authentication. RFC 2104, RFC Editor, 1997.

[16] Yoav Nir and Adam Langley. ChaCha20 and Poly1305 for IETF protocols. RFC 8439, RFC Editor, 2018.