Das VdS-SecurIP-Protokoll zur Alarmaufschaltung – Hintergründe, Vorteile und Empfehlung des BHE-Fachausschusses Übertragungstechnik

Die Alarmübertragung auf eine NSL erfolgt inzwischen fast ausschließlich über eine IP-Verbindung, optional oder verpflichtend mit Funk-Ersatzweg.

Nachdem sich das Übertragungsprotokoll VdS 2465 in der Vergangenheit etabliert hatte und im Laufe der Jahre durch mehrere Erweiterungen um IP-Funktionalitäten ergänzt wurde, wurde aus den gewonnenen Erkenntnissen ein speziell für die Übertragung im IP-Bereich angepasstes Protokoll entwickelt: das **VdS-SecurIP-Protokoll**, welches das bisherige VdS 2465-Übertragungsprotokoll vollumfänglich ersetzt.

Grundlage des VdS-SecurIP-Protokolls

Mit der Weiterentwicklung des Protokolls VdS 2465 für den Einsatz in TCP/IP-Netzen wurden die Anforderungen und Prüfmethoden an das Protokoll in mehrere Teile aufgeteilt, von denen die beiden folgenden für den Errichter relevant sind:

- VdS 2465-2:2018-02 Übertragungsprozedur und Protokollprozedur
- VdS 2465-3:2018-02 Allgemeiner Satzaufbau und Satztypenbeschreibung

Um Verwechslungen mit den alten Fassungen der VdS 2465 auszuschließen, wurden die für den Errichter relevanten Teile der VdS 2465-2 und -3 unter dem Begriff VdS-SecurIP zusammengefasst.
Die Umstellungen auf das VdS-SecurIP-Protokoll befinden sich bereits in der Umsetzung. Neuaufschaltungen dürfen gemäß der aktuell gültigen VdS 2311:2021 ausschließlich mit dem VdS-SecurIP-Protokoll vorgenommen werden.
Auch die Richtlinien auf Leitstellenseite verweisen auf die Verwendung des SecurIP-Protokolls, um die Anforderungen der gesamten Sicherungskette umzusetzen, siehe hier auch die VdS 3534:2023.

Vorteile des VdS-SecurIP-Protokolls

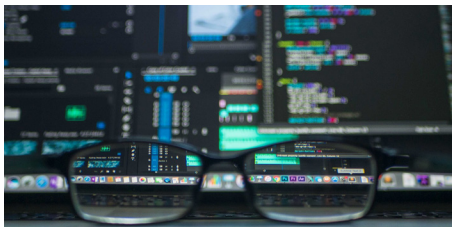
Wesentliche Vorteile sind neben der Übertragungssicherheit eine schnellere Alarmübertragung und weniger Traffic, was insbesondere bei der Alarmübertragung per Funk wichtig ist.

- Entspricht höchsten Sicherheitsanforderungen durch automatisierten regelmäßigen Schlüsselwechsel und hohe Verschlüsselung
  - Hohe Verschlüsselung AES 256bit für den Schlüsseltausch
  - „Init-Key“ ausschließlich für den ersten Verbindungsaufbau
  - Austausch des „Master-Key“ für weitere Verbindungsaufbauten
  - Wechsel des „Session-Key“ erfolgt zeitabhängig oder anhand der Anzahl der ausgetauschten Telegramme
  - Im Standard werden die „Init-Keys“ von der Leitstelle automatisiert erzeugt (PK03)
  - Im VS-Umfeld (PK04) werden die Init-Keys automatisiert durch BSI-geprüfte Verfahren von der Übertragungseinheit (ÜE) erzeugt („beliebig zufälliger Schlüssel“)
- Überwachungszyklus durch Service-Request flexibel gestaltbar
  - Durch zufällige Service-Requests sind (Alarm-)Meldungen nicht als solche erkennbar. Durch verlängertes Polling kann das Datenvolumen für die Wegeüberwachung stark reduziert werden.

- Es besteht die Möglichkeit, zeitkritische Informationen zu übermitteln, ohne das Pollingintervall abzuwarten.
- Reduziert die Abstimmungsproblematik zwischen NSL und Errichter bei Aufschaltungen nach SP4 bzw. DP4 (zentrale Einstellungen wie bspw. das Polling durch die NSL).

- Diverse Satztypen/Zeitstempel wurden überarbeitet und konkretisiert – Sicherstellung der herstellerübergreifenden Kompatibilität.

Contact-ID und VdS-SecurIP-Protokoll



Die Unterschiede zwischen einer Übertragung mit Contact-ID und VdS-SecurIP sind vielfältig und verdeutlichen unter anderem auch die sicherheitstechnischen Aspekte.
Der Schlüssel ist bei Contact-ID dem Errichter bekannt, bei VdS-SecurIP hat der dem Errichter bekannte Init-Key nach Inbetriebnahme keine weitere Relevanz, da dieser durch einen Master-Key / Session-Key ersetzt und zyklisch gewechselt wird.

Nachteile von Contact-ID im Sicherheitskontext

- Bei Contact-ID wird immer der gleiche Schlüssel verwendet (ÜE könnte ersetzt werden, wenn der Schlüssel bekannt geworden ist).
- Im VdS-SecurIP-Protokoll wird die Mehrfachnutzung eines Schlüssels verhindert, jede Verbindung erhält einen eigenen Schlüssel.
- Beim VdS-SecurIP-Protokoll ist eine Verschlüsselung verpflichtend, bei Contact-ID kann auch unverschlüsselt übertragen werden.
- Beim Contact-ID-Protokoll werden nur die Nutzdaten verschlüsselt, bei VdS-SecurIP erfolgt die Verschlüsselung komplett bis auf Kennung und Länge.
- Bei Contact-ID werden Meldungen spontan übertragen, jeder Teilnehmer kann ständig senden. In einem Telegramm können unterschiedliche Meldungsinhalte vorhanden sein, die gemeinsam quittiert werden.
- Die Telegrammlänge ist bei Contact-ID unterschiedlich, bei VdS-SecurIP immer gleich.
- Die Zeit, wann eine AÜA ausgelöst hat, wird bei Contact-ID nicht zwingend mit übertragen, sondern in der Regel nur der Zeitstempel, wann die Meldung übertragen wurde. Eine Laufzeitmessung ist daher nicht möglich.

Empfehlungen des BHE-Fachausschusses Übertragungstechnik

- ***Eine Alarmübertragung nach aktuellem Standard sollte möglichst mit dem VdS-SecurIP-Protokoll erfolgen – auch bei Bestandsgeräten.***
  - Vor allem die wesentlich aktuellere Verschlüsselungsart ist hier von Vorteil.
  - Die Messung von Übertragungszeiten ist elementar wichtig, um geforderte Standards wie Alarmübertragung nach DP4 auch umsetzen zu können.
- VdS-SecurIP ist zumindest im Bereich der Pflichtaufschaltungen von VdS-Anlagen der Standard und wird von allen nach VdS-geprüften und zertifizierten Leitstellen unterstützt.
- Übertragungseinrichtungen nach aktuellen VdS-Standards sind in der Lage, das VdS-SecurIP-Protokoll zu übertragen.
- Mit dem VdS-SecurIP-Protokoll steht ein Übertragungsprotokoll zur Verfügung, das höchste Anforderungen an die Cyber-Sicherheit erfüllt.

BHE Bundesverband Sicherheitstechnik e.V., Feldstraße 28, 66904 Brücken, Tel.: 06386 9214-0, Fax: 06386 9214-99, info@bhe.de, www.bhe.de