network.

2) An access point: Is usually part of the gateway and acts as the radio interface, and multiple AP’s are making it possible to communicate on different channels in parallel.

3) A network manager: Is normally part of the gateway and is responsible for managing the wireless network.

4) A security manager: Manages and distributes security encryption keys, and also holds the list of devices authorized to join the network.

5) Field devices: These are devices directly connected to the process (measurement and control), or equipment (asset monitoring) or adapters which connects wired HART devices to the wireless network (retrofit).

WirelessHART is a secure and reliable protocol, which uses the Advanced Encryption Standard (AES) with 128 bit block ciphers. A counter with Cipher Block Chaining Message Authentication Code mode (CCM) is used to encrypt messages and calculate the message integrity code (MIC). The standard supports end-to-end, per-hop, and peer-to-peer security. End-to-end security is provided on the network layer, while the data link layer provides per-hop security between the two neighboring devices. Peer-to-peer security is provided for secure one-to-one sessions between field devices and handhelds during configuration. WirelessHART devices need a join key to join the network securely. The join key can be individual, or the same for the complete network. When a device joins the network for the first time, the join key needs to be programmed via a local port.

C. Black Channel and Profisafe

Most industrial safety protocols for fieldbus communication are based on the principle of the black channel [36], using the experience from the railway signaling domain [27], [37]. Safe applications and non-safe applications share the same standard communication system, the black channel, at the same time. The safe transmission function, e.g., the safety layer, comprises all measures to deterministically discover all possible faults and hazards that could be infiltrated by the black channel, or to keep the residual error probability under a certain limit without relying on services provided by the network. Therefore, the black channel principle limits the certification effort to the safe transmission functions, i.e., the safety nodes and their safety layers, as they do not rely on the standard transmission system which includes switches, routers, gateways, transmission protocols, etc. The principle of the black channel is visualized in Fig. 2. In comparison, a White Channel approach requires all components, including network components, involved in the safety function to be subject to safety certification, and is therefore a less attractive alternative with respect to cost and life cycle management.

Profisafe [38] is one of four safety protocols described in the IEC 61784-3 standard [36]. Profisafe, or functional