Fig. 7. The WirelessHART gateway queries the network manager for a list of active WirelessHART devices. Using the list of active devices from the network manager, the gateway queries the active devices for their tag names. Now the gateway can map the device network address to a Profinet IO slot.

The main advantage of our proposed integration method is that the already existing engineering tools in the DCS can be used to engineer and maintain the WirelessHART networks at a central location, in the same way as existing field devices. In addition, engineering and maintenance of the WirelessHART devices is simplified, as the configuration will be automatically downloaded after replacement of faulty components, thus reducing the down time. Moreover, the separation of HART commands, physical and logical units in the model simplifies both the design of the gateway and most important the usage of the gateway when considering safety and security. Other existing integration work or methods can be used as well, but will most probably not be beneficial to use with respect to safety, end-to-end security, as well as engineering and maintenance efforts of the latter.

B. On-demand Configuration Data

Fig. 8. An example where security modules protect the integrity and

To reduce the possibility that cryptographic keys are compromised, they should ideally be distributed once. In addition, the cryptographic keys should be updated on a regular basis.

Our solution transmits the keys on-demand in plain text from the engineering station to the WirelessHART gateway, by using the Discovery and Configuration Protocol (DCP) provided by Profinet IO. The keys are programmed in non-volatile memory in the WirelessHART gateway by using write-only Manufacturer Specific Parameters, and are distributed by the WirelessHART gateway in ciphertext to the WirelessHART devices. Doing it in this way, the cryptographic keys are assigned in the same way, using the same engineering tool, as IP-addresses for Profinet IO field devices without any changes in the Profinet IO standard. security modules use the same concept [41], and this enables a simple key distribution mechanism for Profinet IO and WirelessHART. Distribution of security-relevant data should in general be transmitted with additional protection compared to for example IP-addresses. However, this additional protection, e.g., encryption, needs major changes in the Profinet IO standard and has therefore neither been further investigated nor implemented. This approach supports the process of automatic key updates, by replacing the manual process with an automatic service that updates the keys on a regular basis. The join key and the Network ID of the WirelessHART Device must initially be configured via some local port for security reasons; otherwise the WirelessHART Device cannot join the network and create a secure channel for key updates. Key distribution is mostly the weakest link, even in this case, and is a general and known