Faulty Device Replacement for Industrial Networks

Markus Rentschler
Hirschmann Automation & Control GmbH
72654 Neckartenzlingen
Markus.Rentschler@belden.com

***Abstract*—In the case of failing equipment in industrial plants, the replacement time and effort must be kept at a minimum to increase the overall system availability. A well-designed Faulty Device Replacement (FDR) concept is therefore a central issue to the effective operation of industrial plants. Network enabled devices supporting FDR with minimum subsequent manual device configuration after replacement form a key requirement to improve repairability. To achieve this, several FDR techniques have been proposed and implemented by different vendors and organizations. In this work, a performance model for the time to repair and a taxonomy for existing FDR methods is provided. This can be used as a basis for comparative performance measurements to derive the most suitable method during the planning phase of an industrial network.**

***Keywords* — Availability, Fault, Repairability, Ethernet, DHCP, LLDP, TFTP, Relay Agent, Option 82**

I. INTRODUCTION

Industrial Ethernet networks [1] are usually composed of various devices, interconnected within complex wired and wireless topologies (Fig. 1). Initially, Network Engineers configure the TCP/IP capable infrastructure and end devices in these networks with the help of PC-based engineering tools such as network management software (NMS). After an industrial network has been setup and is operating productively, downtimes have to be avoided. In the case of unexpectedly failing network components, their replacement has to be performed in such a way to keep the downtime of the affected parts of the network at an absolute minimum. The physical replacement of a faulty device is a manual task, performed by maintenance personnel, whose time consumption can be significantly influenced by plant architecture, regulations and processes but also by the hard- and software design of the device to be replaced.

"Design for FDR" has therefore become an important issue for device vendors and network designers to meet customer needs. Although a range of mechanisms was already defined and available in commercial products at that time [1][2][3], the IAONA working group "JTWG System Aspects" still has in 2005 formulated the goal to "*Develop a strategy for faulty device replacement including IP address assignment and automatic application configuration.*" [4]. However, only very few publications on this subject have since emerged at all [5] [6].

The term "FDR" is commonly associated with the software- and network protocol based tasks of automatic IP and other configuration parameters assignment to devices in a communication network. Nonetheless it also strongly incorporates hardware and plant design aspects. The understanding of FDR in this context is therefore a more holistic one and incorporates the whole process of replacing a specific single device connected to an operational industrial network with an identical or equivalent spare part. In this respect, the FDR process consists of fault monitoring and notification, the physical replacement of the device, its start-up and configuration until it has returned operational condition.

The contribution of this work is the development of a generic FDR process and a time-to-repair timing model as basis for the objective comparison of different available FDR techniques, which are also summed up in this paper.

The structure of the paper is as follows: In chapter II, a generic FDR process model is defined and concisely modeled with UML diagrams. In chapter III, the taxonomy with brief furthermore overviews of different faulty device replacement mechanisms is given, their strengths and weaknesses highlighted. Finally in chapter IV, a conclusion on the findings is drawn.

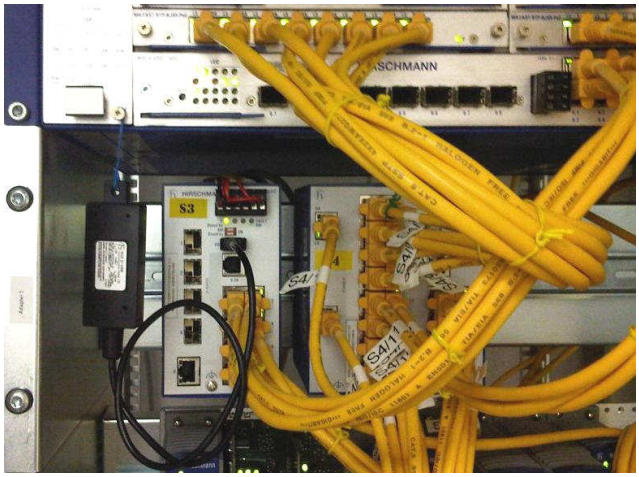

Figure 1. Industrial Network Devices

II. FAULTY DEVICE REPLACEMENT CONTEXT

The context of an Industrial Ethernet network in a factory plant is modeled in Fig. 2. The focus of FDR here lies on TCP/IP capable infrastructure (e.g. router, switch, gateway) and end devices. When one of these components in the factory communication network gets faulty, it needs to be replaced in a way to minimize downtime of the productive process of the

factory plant. In such an FDR process, commonly the following steps are involved:

1. A device becomes faulty.
2. The failure is detected and reported to the maintenance engineer.
3. The faulty device is identified and a suitable replacement device (identical or similar) is taken from maintenance stock.
4. The faulty device is accessed at its location and physically replaced with the replacement device.
5. The replacement device boots up and switches to operating.
6. The replacement device is configured with the same parameters as the faulty device.

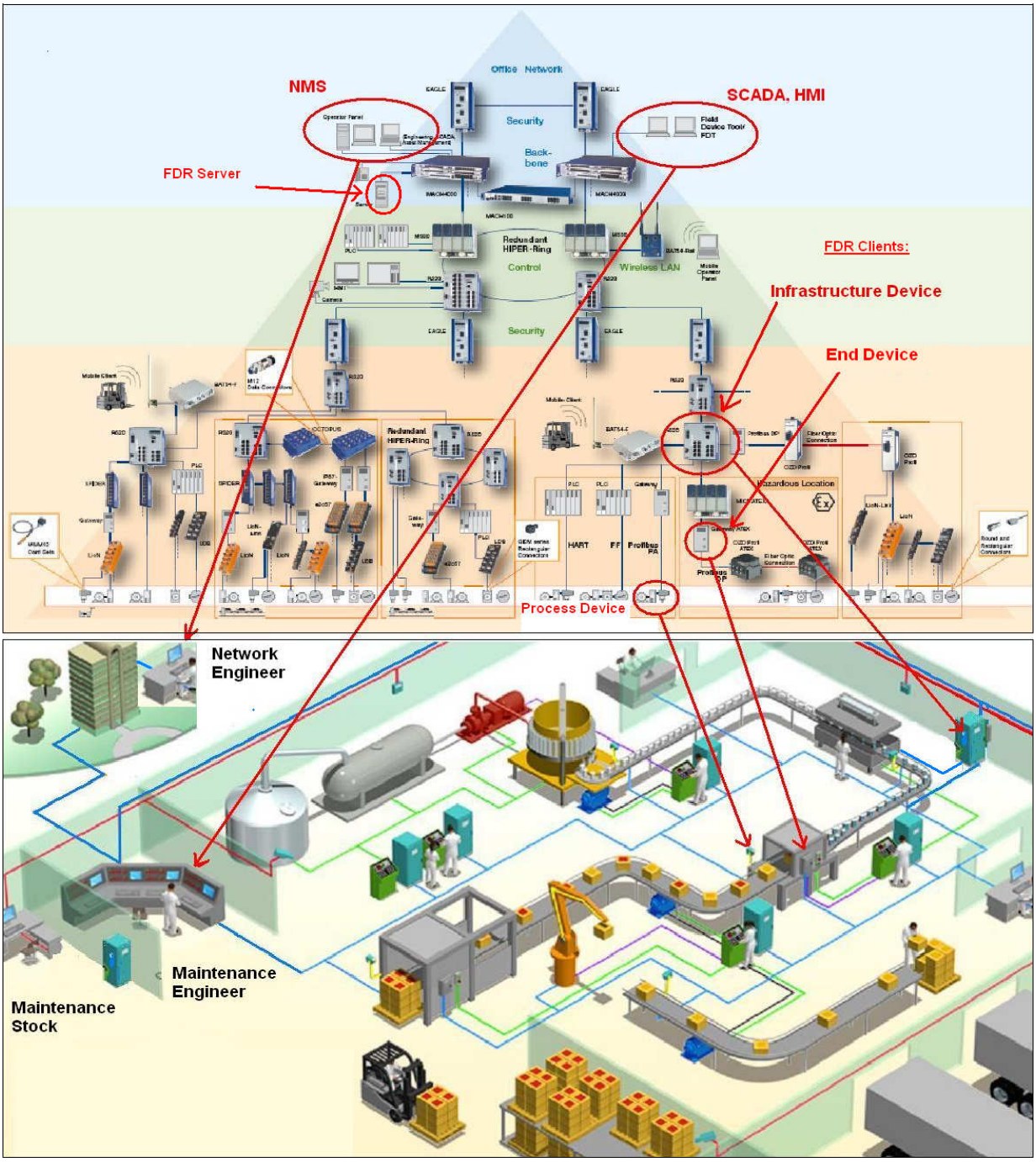

Figure 2. FDR context within automation pyramid and industrial plant.

III. GENERIC FDR PROCESS AND TIMING MODEL

For a FDR model, the involved actors and their use cases are identified in Fig. 3. In the following, the FDR-capable replacement device will further be termed "**FDR Client**", the central instance responsible for assigning configuration parameters will be termed "**FDR Server**".

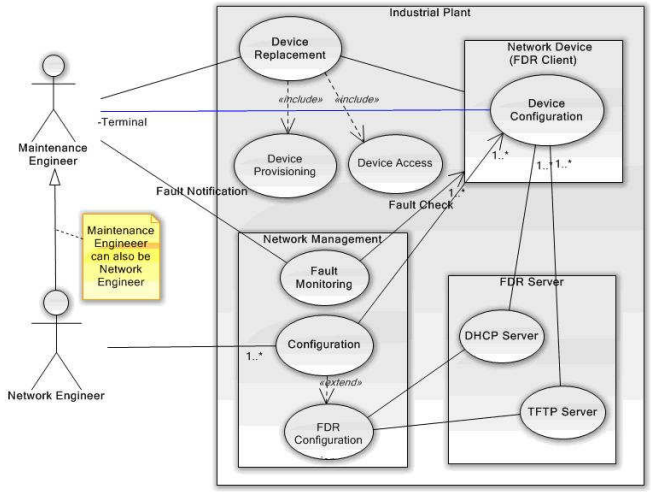

Figure 3. FDR Use Case model

The generic process steps are sequentially modeled in the activity diagram in Fig. 4, which can be utilized for FDR performance planning and measurement of different FDR techniques.

Figure 4. FDR Activity and Timing Model

These generic process steps and their influencing factors on the overall timing behavior T_{FDR} are defined as follows:

$$T_{FDR} = T_1 + T_2 + T_3 + T_4 + T_5 + T_6 + T_7 \quad (1)$$

1. **Fault Monitoring (T_1)**: The network devices must be constantly monitored by the NMS. When an error on a device occurs and requires replacement, the NMS must send a notification to the maintenance engineer. T_1 is the time from actual fault occurrence until reception of fault notification to the maintenance engineer. The cycle time T_{cycle} of the monitoring process (i.e. health check polling speed) determines the worst case detection time and subsequently the $T_{attention}$ reflects the duration until the network engineer has gotten attention of the notification.

$$T_1 = T_{cycle} + T_{attention} \quad (2)$$

2. **Device Identification (T_2)**: When the maintenance engineer has noticed the fault notification, the device type to be replaced and its location has to be identified. Influencing factors for T_2 are the informational content of the fault notification and the tooling available to locate the faulty device.

$$T_2 = T_{type\_identifiaction} + T_{location\_identifiaction} \quad (3)$$

3. **Device Provisioning (T_3)**: After identification, the replacement device must be taken from maintenance stock. T_3 is the time required for getting to maintenance stock and acquiring the device. Influencing factors are distance D_{stock} from the maintenance engineer's office and his moving speed v. The accessibility of the maintenance stock is mainly influenced by be the number of locked doors n_{doors} whose passage takes T_{door} each.

$$T_3 = (D_{stock} / v) + (n_{doors} * T_{door}) \quad (4)$$

4. **Device Access (T_4)**: After the replacement device has been provisioned, the faulty device must be physically accessed, so that the actual physical replacement can be performed. T_4 reflects the time required for walking to and accessing the location (i.e. network cabinet). This depends on distance, moving speed and accessibility to the place were the device is installed.

$$T_4 = (D_{location} / v) + (n_{doors} * T_{door}) \quad (5)$$

5. **Device Replacement (T_5)**: Remove the faulty device and install the replacement device. T_5 reflects the time required for unplugging connected cables, removing the faulty device, mounting the replacement device and reconnecting cables. Influencing factors are ease of access and the amount of wired connections to be processed (see Fig. 1).

$$T_5 = (n_{conns} * T_{unplug}) + T_{replace} + (n_{conns} * T_{plug}) \quad (6)$$

6. **Device Configuration (T_6)**: After reboot, the replacement device must be supplied with the identical configuration as on the previous faulty device. T_6 reflects the time required for this. Influencing factors are the FDR technique (manual vs. semi-automatic vs. fully-automatic) and the boot time of the device.

$$T_6 = T_{manual\_config} + T_{reboot} + T_{automatic\_config} \quad (7)$$

7. **Device Startup (T_7)**: After the device has received the identical configuration as the previous faulty device, T_7 reflects the time until fully operational state has been reached again and the fault is cleared in the NMS. T_{cycle} reflects the monitoring process worst case time and $T_{clearance}$ the time offset required to report completion of the FDR operation to the supervision system.

$$T_7 = T_{cycle} + T_{clearance} \quad (8)$$

Additionally, $T_{FDRConfig}$ reflects the required preparatory effort for the FDR configuration, incorporating mainly the FDR Server (i.e. DHCP, TFTP Server) and Relay Agents [13].

$$T_{FDRConfig} = (T_{DHCP} + T_{TFTP}) * n_{Clients} + T_{Relay} * n_{Relays} \quad (9)$$

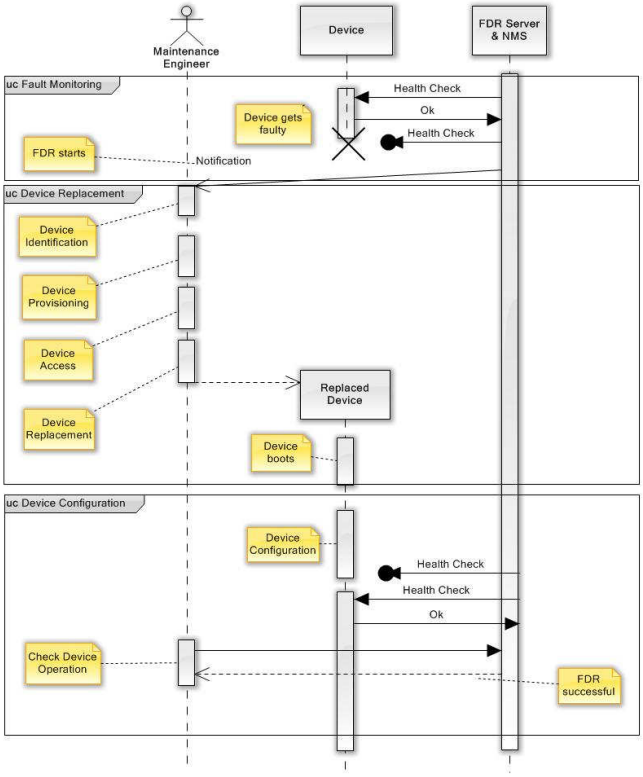

Figure 5. Generic FDR Sequence Diagram

The sequence diagram in Fig. 5 models the generic FDR process in another -more detailed- view that relates the sequential activities from Fig. 4 to the relevant use cases where the "Maintenance Engineer" is involved. This allows an easy substitution in the next sections of the different FDR techniques for device configuration.

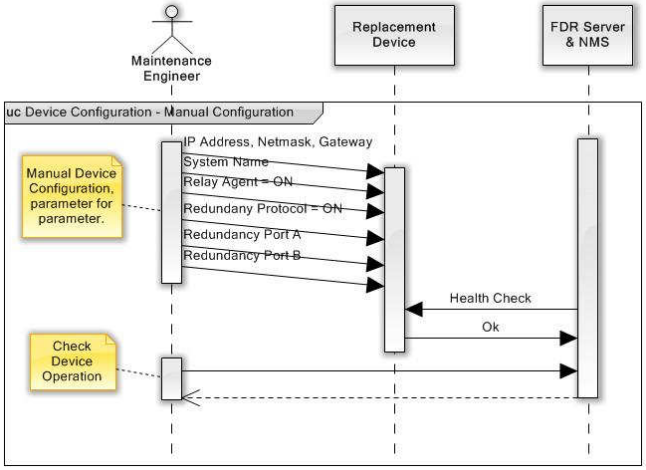

Figure 6. Manual Configuration

IV. FDR TAXONOMY

A classification of known FDR mechanisms for Industrial Ethernet networks is given in Fig. 7.

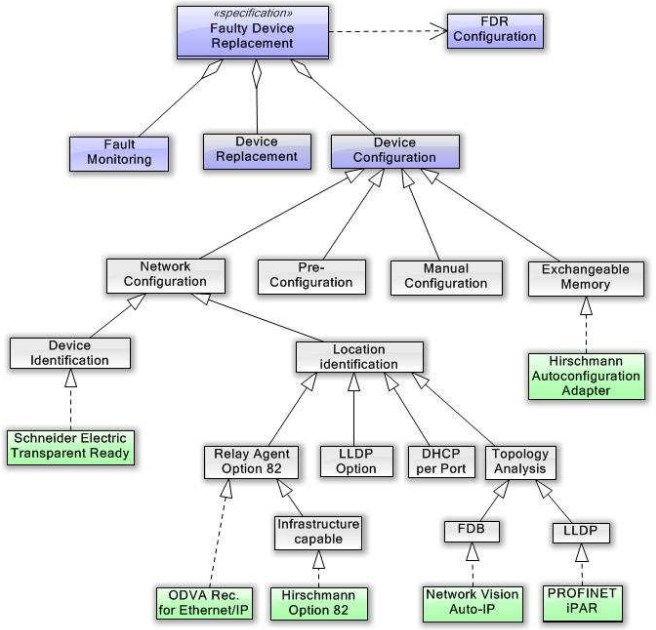

Figure 7. FDR Taxonomy

These different FDR techniques for device configuration are described in more detail in the following subchapters.

A. *Manual Configuration*

When no automatic FDR technique for device configuration is available, the replaced device has to be manually configured onsite e.g. with a portable computer that allows access to the replacement device via a serial interface.

The main obstacle to this approach is that the Maintenance Engineer must have the knowledge of the configuration details for the device and the required skills to enter them (see Fig. 6). For more complex configuration settings, the risk for misconfiguration rises quickly with this approach.

B. *Pre-Configuration*

A related approach is to have the devices kept in maintenance stock already preconfigured for their future role. In some cases they can even be delivered from the manufacturer with a customer-specific pre-configuration that fits the standardized device usage for this customer. Usually just the IP address parameter set needs to be configured at replacement time. Thus reducing the required time and risk of failure causes for replacement compared to a fully manual configuration.

C. *Exchangeable Memory Device*

Another FDR concept is based on exchangeable external nonvolatile memory (NVM) devices that are permanently connected to the network device. These external NVM devices are usually interfaced via RS232, USB port (Fig. 8, left side)

or SD card slot (Fig. 8, right side). Whenever the device configuration is saved to the embedded NVM of the device, a copy is also stored on the external NVM device. At boot time, when such an external NVM device is connected and contains valid configuration data, this data is loaded to configure the replacement device instead of the data in the embedded NVM. Simply connecting the external NVM from the faulty device to the replacement device prior to rebooting allows a fully automated device configuration transfer without further manual intervention from the maintenance engineer. This provides a very robust, fast and easy to handle FDR approach.

Figure 8. Autoconfiguration Adapter (ACA)

The external NVM devices and their respective connector slot on the device can be designed with the following properties:

- The connector slot is accessible without un-mounting the device, usually placed at the front or the bottom of the device (see Hirschmann's *ACA 21* [14] in Fig. 8, left side). This allows hot-plugging of the external NVM device.
- The connector slot is not accessible without removing the network device from its installation location, adding some security (i.e. theft prevention of the external NVM device). This can simply be achieved by placing the connector slot on the back of the network device (see Hirschmann's *ACA 31* [14] in Fig. 8, right side).
- The design of the external NVM device can allow its fixation to the installation location. This effectively prevents a potential mix-up of external NVM devices, when several device replacements take place at the same time in a plant. It also can achieve some theft prevention (see Fig. 1).

D. Network Configuration

A range of well-known FDR techniques are based on configuration retrieval from a remote configuration server via the network. Solutions like the PROFINET iPAR concept [6] fit in this category. Other solutions make use of standard network protocols like BOOTP or DHCP [7]. By utilizing the Option 67 (*boot filename*) [8], not only the IP parameters but also the complete configuration of a device can be transferred to the client device via FTP or TFTP [9].

The challenge with the network based approach is to assign the right configuration set to the replacement device. This must be achieved by precise identification of the replacement device, either based on ***Device Identification*** or ***Location Identification***.

1) Identification Dependent Network Configuration

With the ***Device Identification*** approach, the FDR Client sends a unique device identifier with the BOOTP/DHCP-Request towards the FDR Server. Hardware identifiers, such as the MAC address or the serial number of the replacement device cannot be used because they will be different after replacement and thus unknown to the FDR server. Instead, the replacement device with factory settings has to be manually preconfigured with the same unique identifier in the local network context that the faulty device was associated with. This identifier can then be coded in a DHCP option field such as the Option 61 (*client identifier*) [8]. The FDR server is able upon reception of a DHCP request with this option to select the associated configuration parameter set and transfer it to the device via DHCP and subsequently TFTP. This approach is promoted in the "Transparent Ready®" concept by Schneider Electric [3]. The generation of a locally unique identifier can be achieved as follows:

HW Identifier: The device is equipped with DIP or rotary switches for selecting the device IP address or some other unique identifier code. Prior to replacement of the faulty device, the settings from the faulty device are just copied manually to the new device. At power-up, the device reads the hardware switches and codes the unique identifier into the DHCP option field.

SW Identifier: The unique identifier is manually configured after reboot. This can be simply the IP address or a locally unique *Role Name* or *System Name*. This approach is very similar to the Manual Configuration approach, but is then followed by a DHCP/TFTP sequence to retrieve the remaining configuration data from a remote FDR Server. This approach requires a minimum manual configuration intervention by the maintenance engineer. For easy handling of this approach, it is important that the locally unique identifier of the device is properly labeled on the outside of the faulty device.

2) Location Dependent Network Configuration

The ***Location Identification*** approaches require that the FDR server is informed about the precise position of the replacement device within the network topology. This allows a fully automatic device replacement without a manual pre-configuration of the replacement device. The challenge here is to reliably assign the origin of a FDR request to a certain position in the network topology. Several FDR methods dealing with this obstacle are described in the following.

3) DHCP per Port

This approach is based on peripherally located DHCP servers which are embedded in the infrastructure devices themselves. The FDR clients that are directly connected to the ports of these infrastructure devices are supplied with the parameters associated for the specific port (see Fig. 9). There is no manual pre-configuration on the replacement device. Even if the

infrastructure device cannot filter out the broadcasted DHCP requests, the directly connected DHCP server in this infrastructure device will always be the first one to answer to a DHCP client request and therefore win the lease before other DHCP servers in the network.

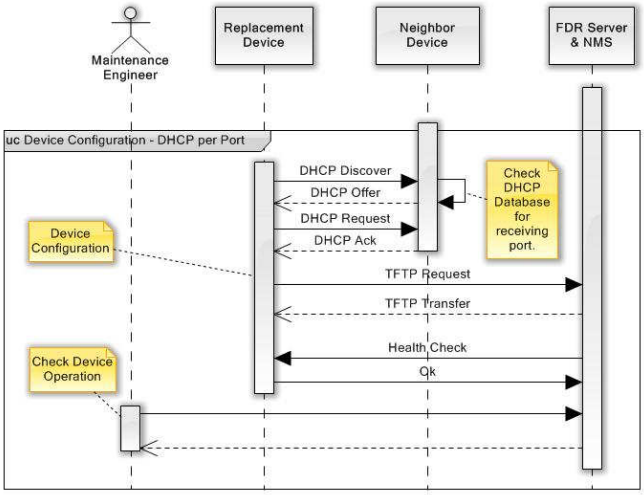

Figure 9. DHCP per Port

This approach has the limitation that only one client connected to a port can be reliably served.

4) Relay Agent Option

A popular approach is based on the Relay Agent Option 82 as defined in RFC3046 [13]. This method was selected by the *Open Device Vendor Association (ODVA)* as a preferred FDR method in "EtherNet/IP™" networks [1] and is supported by most available managed Industrial Ethernet switches.

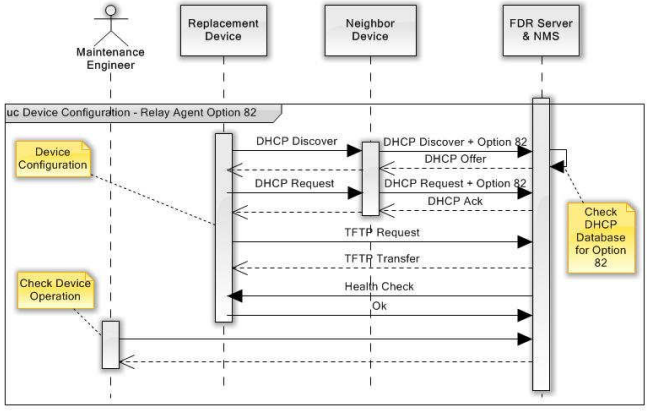

Figure 10. Relay Agent Option

Encoded in the DHCP Option 82, an *agent id* (Device Identifier) and a *circuit id* (Port Identifier) are added to the original DHCP request by the first infrastructure device where the FDR Client is connected (Fig. 10). This topological information is then used by the FDR server to assign the proper parameter set to the replacement device.

The same limitation as with DHCP per Port exists: Only one single FDR client on each port of an infrastructure device is allowed, since ambiguity due to broadcast flooding cannot be resolved. Furthermore, the infrastructure devices must be configured as Relay Agents with a unique *agent-id*. The manual configuration of the FDR Server becomes elaborate and error prone in complex networks with redundant paths. Additionally, devices directly connected to the FDR server cannot use this approach, because there must be a Relay Agent capable device between FDR Client and the FDR Server.

5) Infrastructure capable Option 82 extension

The main disadvantage of the standard Relay Agent Option 82 approach is that the infrastructure devices themselves are not replaceable using this mechanism. The original DHCP broadcast requests are flooded on OSI layer 2 and subsequently relayed by every Relay Agent in their way and each tagged with a different Option 82 content. The FDR server receives all these DHCP requests and requires a means to select the right one. This works only when the FDR server database has only one parameter set assigned to any edge port in the network and will serve only the DHCP requests coming directly from these edge ports. All the other Option 82 tagged requests from non-edge ports must be ignored, because they are ambiguous. When an infrastructure device shall be the FDR client, this ambiguity cannot be resolved. To overcome this limitation, Hirschmann Automation & Control GmbH has implemented the following solution for its infrastructure devices (Fig. 11):

1. When acting as a FDR Client, the DHCP requests are not only broadcasted, but additionally sent to a private multicast destination MAC address.
2. A Hirschmann device acting as Relay Agent is capable of filtering these multicast requests and does not flood them further into the network.
3. The Hirschmann Relay Agent tags these multicast requests with an option 82 that contains the information that its origin was a multicast request (called "multicast flag").
4. The FDR server can now use this multicast flag in the received option 82 to distinguish FDR requests coming from infrastructure devices.

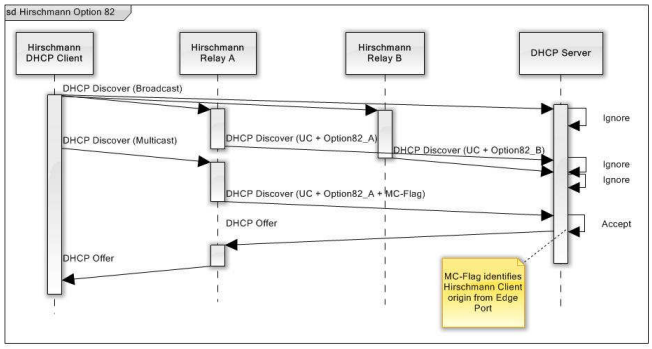

Figure 11. Hirschmann Option 82 Principle

This proprietary solution works quite well in networks containing only Hirschmann infrastructure devices. But still, the last device directly connected to the DHCP server cannot be identified with option 82 at all and all Relay Agents in the network must be pre-configured with a unique agent id that cannot be device hardware dependent (such as the MAC address or serial number).

6) LLDP option

LLDP according to IEEE 802.1AB [12] is a topology discovery protocol that distributes local topology information to its direct neighbors where this information is stored in tables for later retrieval via the LLDP-MIB from a Network Management Station (NMS), using SNMP.

LLDP can be utilized for FDR topology identification as follows: Prior to transmission on each FDR Client port, the DHCP request is tagged with a "*LLDP Option*" that contains the received neighbor topology information, similar to the *agent id* and *circuit id* of the Option 82. This approach works without the need for configured Relay Agents as in the Option 82 based topology identification mechanism, but both can coexist in the same network.

For this approach, all involved network devices must be LLDP capable and the FDR Clients able to transmit this new "LLDP option" which must be defined for BOOTP/DHCP. The Option 82 encoding scheme could be adopted for this approach, avoiding implementation changes in existing FDR servers. So far, no actual implementations of this promising approach are known.

7) Topology Analysis

FDR approaches exist that are based on topological analysis of the network data prior and during the FDR phase performed by the FDR Server. The FDR Server receives a request for parametrization from a replacement device which is until then unknown. The FDR server then starts a lookup of the topological information in the infrastructure devices to determine the location of the new replacement device and subsequently selects the associated parameter set in its database for assignment to the new device.

"Auto-IP" by *Network Vision Inc.* is based on BOOTP/DHCP and utilizes SNMP [10] to collect topological information of the Forwarding Database (FDB) as displayed in the network device's *Bridge MIB* according to RFC1493 [11]. This approach is described in great detail in [2].

The PROFINET iPAR-Server concept [6] utilizes the topology information in the LLDP MIB tables [12] of the network devices for the FDR procedure. For parametrization, the PROFINET Discovery and Configuration Protocol (DCP) is used.

These approaches based on topology analysis require a rather complex knowledge engine in the FDR Server and are likely to fail when the network is in an undefined state and delivers ambiguous topology information.

V. SUMMARY AND CONCLUSION

In this work, a generic performance model for FDR was developed. This can be used as a basis for development of a related network planning tool. A taxonomy of known FDR mechanism was presented. The required initial configuration effort for these FDR mechanisms was also discussed.

The result is that the semi-automatic approaches requiring manual configuration might work acceptable fast when there is not much configuration data to enter, thus limited to the IP parameter or a role name and the rest of the device configuration is subsequently retrieved via DHCP and TFTP.

The major shortcoming of the approaches based on network configuration is the setup of the FDR Server instance(s) – which can even be distributed as in the "*DHCP per Port*" approach. For the Option 82 based methods the Relay Agent functionality has to be configured on the infrastructure devices. Furthermore, all the topology based approaches are unsuitable for the replacement of faulty mobile wireless devices with no wired connection into the network topology.

The approach using exchangeable memory devices does not have any of these limitations and can even be used for mobile devices. It was found to be the fastest, most flexible, robust and reliable FDR method, which can even work without a central instance such as a NMS or a FDR Server. This method is therefore highly recommendable for use in Industrial Ethernet networks.

REFERENCES

[1] ODVA; "Recommended IP Addressing Methods for EtherNet/IP™ Devices"; Version: 1.0, 10-June-2003, available at http://www.odva.org

[2] Network Vision Inc.; "Comparison between Auto-IP and DHCP Option 82", 2004, available at http://www.intravue.net/productsAutoIP.asp

[3] Schneider Electric; "Transparent Ready - User guide"; Rev.1.0/0.2, Doc. 31006929, October 2009, available at http://www.global-download.schneider-electric.com

[4] IAONA; "Work Plan JTWG System Aspects"; Release No 1.3 - DRAFT, Date 2005/09/07, available at http://www.iaona-eu.com/pdf/Work_Plan.JTWG-System_Aspects.V13.050907.pdf

[5] Henrici, de Waha; "Vereinfachung der Administration von IP-Netzwerken mit dynamischer Hostkonfiguration"; DFN 2007; available at http://dspace.icsy.de:12000/dspace/bitstream/ 123456789/ 205/1/20_DFN_DHCP.pdf

[6] PNO, Profibus User Organisation; "The iPAR Server Concept", 2012; available at http://www.profibus.com/ technology/functional-safety/how-to-implement/

[7] Droms, R.; "Dynamic Host Configuration Protocol"; RFC 2131, March 1997;

[8] Alexander, Droms; "DHCP Options and BOOTP Vendor Extensions"; RFC 2132, March 1997;

[9] Sollins, K.; "The TFTP Protocol (Revision 2)"; RFC 1350, July 1992;

[10] Case, Fedor, Schoffstall, Davin; "Simple Network Management Protocol", RFC 1157, May 1990;

[11] Decker, Langille, Rijsinghani, McCloghrie; "Definitions of Managed Objects for Bridges", RFC 1493, July 1993;

[12] IEEE 802.1AB-2005 - IEEE Standard for Local and metropolitan area networks Station and Media Access Control Connectivity Discovery

[13] Patrick, M., "DHCP Relay Agent Information Option"; RFC 3046, January 2001;

[14] Hirschmann Product Catalogue 2012 ; available at http://www.beldensolutions.com