

Hirschmann. Simply a good Connection.

Future Industrial Wireless Concepts based on Thin Access Points

Future Industrial Wireless Concepts
based on Thin Access Points - Rev. 1.0



Contents

Future Industrial Wireless Concepts based on Thin Access Points

1	Introduction	3
2	Shifted intelligence as alternative to common wireless technologies	5
3	Advantages in terms of Cost and Technology	6
4	Security concerns	8
5	The big challenge: Roaming and Security	9
6	The future	11
7	References	12

Future Industrial Wireless Concepts based on Thin Access Points

1 Introduction

The installation of radio networks in the factory automation is still characterised by relatively expensive hardware and expensive planning and start-up costs. There are opinions to hear claiming to reduce both, the costs of hardware and the cost of installation. The solution of the problem will be as follows: An increase of intelligence will be shifted from the access point to the attached network. Following it will be possible to install more access points at the same costs. Intelligent mechanisms e.g. security mechanisms or roaming will be enabled by central units in the cable-based Backbone, and last but not least these mechanisms will also be accelerated. This model will be particularly successful in the factory automation if it will be possible to keep the existing cable based network unchanged, and if the shift of intelligence from the access points into the Backbone will be possible by adding the central intelligent instance only.

Today each individual access point has to render its economical right to exist, and the network is mainly designed for momentary needs only - in particular related to the number of expected mobile participants and thus related to the to be expected network load - in order to achieve the desired reliability in terms of quality of service. Understandably there are more and more opinions to hear claiming to reduce both, the cost of hardware and the cost of installation.

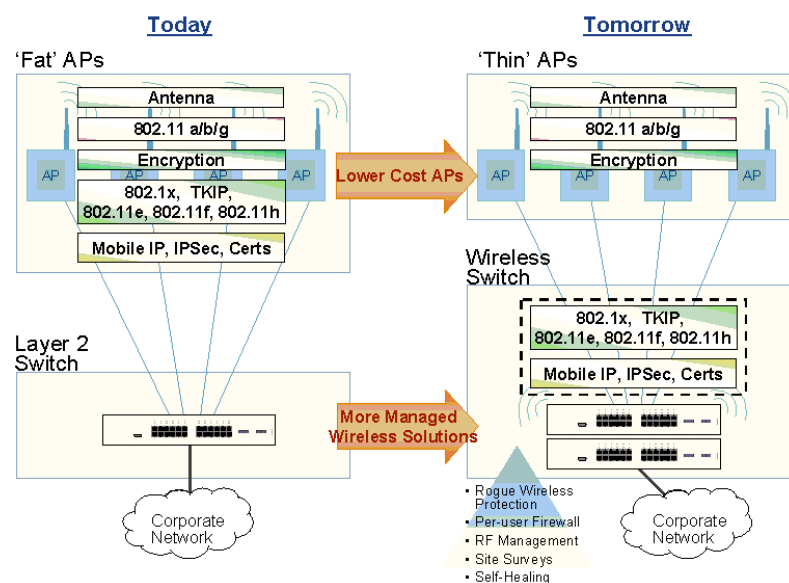


Figure 1: Comparison of Today's and Tomorrow's Wireless Architecture

The solution of the problem will probably appear in the near future as follows: An increase of intelligence will be shifted from the access point to the attached network (see figure 1), whereby first the importance and second also the costs of the access point will sink. Accordingly to that, it will be possible to install more access points at the same costs. Intelligent mechanisms e.g. security mechanisms (Authentication in accordance to IEEE 802.1x) or roaming will be enabled by central units in the cable-based Backbone, and last but not least these mechanisms will also be accelerated.

The described model offers two advantages:

Increased density of access point

The density of the access points is increased, whereby a higher system availability can be guaranteed. The choice of access clients to associate to different access points in the network cause an increase of redundancy. For example, with three available options to associate it is without any effect on the system availability if up to two of the access points fail.

Simplified installation

The installation is simplified, because the Site Survey is of smaller importance by the larger number of access points.

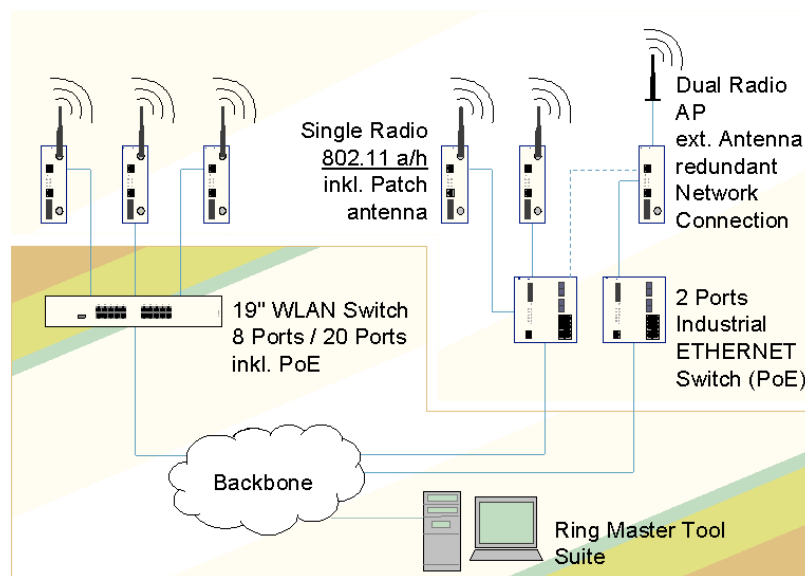


Figure 2: Typical Wireless Network Architectur based on Thin Access Points

In this context an increase of key words such as "self healing mechanism" and "automatic site survey" can be perceived. This discussion refers to another, the third component of the model: the management software. Besides the so called "Thin Access Points" and the central instance within the Backbone, it will also be possible to automate the service of site survey, as optimised topologies and preferred locations for the installation of the access points are thus automatically suggested and realised by the support of management software.

This model will be particularly successful in the factory automation if it will be possible to keep the existing cable based network unchanged, and if the shift of intelligence from the access points into the Backbone will be possible only by adding the central intelligent instance.

Regarding this approach a particularly side effect is of special interest: The importance of network infrastructure, which enables mobile communication on production floor, increases substantially - and this infrastructure is typically cable-based. The revolutionary forecast that wireless will replace cable takes time to wait for another evolution step (see figure 2).

2 Shifted intelligence as alternative to common wireless technologies

The concept of shifted intelligence involves a centrally installed wireless LAN switch and so called "thin" access ports. Compared to the traditional "thick" access point wireless technology, the "thin" approach profits from advantages like improved scalability and manageability, and will finally result in a decreased total cost of ownership.

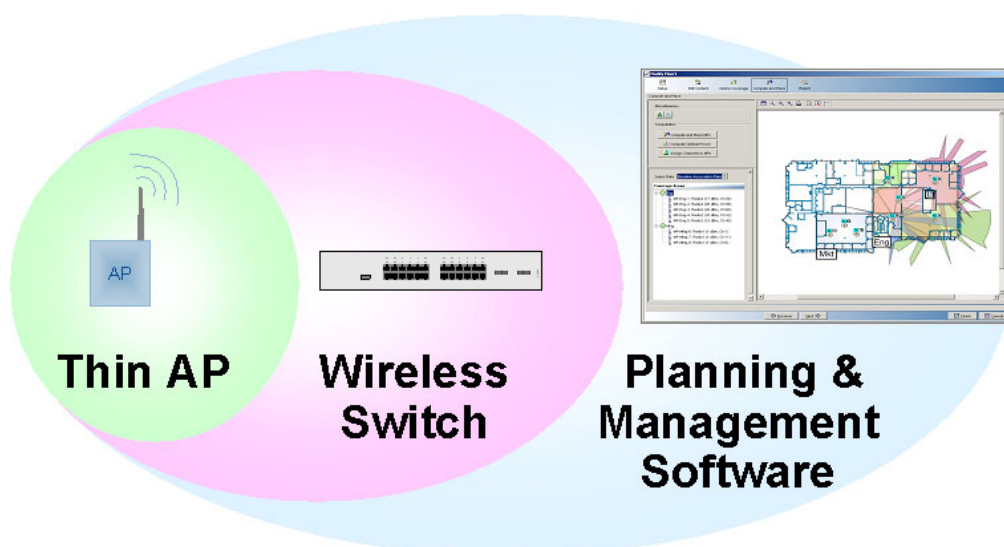


Figure 3: Three Elements of a Wireless Network Architectur based on Wireless Switch

Traditionally enterprise wireless LAN infrastructure uses intelligent thick wireless access points. These access points are attached to an existing wired Ethernet network. In this approach, the access points are dedicated to maintaining configuration data and performing client authentication. Since each access point is to be regarded as a separate, stand-alone device, a network administrator must manage each and every device. In the thin approach, there are access ports that simply provide wireless access. The intelligence in this architecture is consolidated in a central Wireless Switch. The network administrator is able to manage all wireless features by using the wireless switch (see figure 3). The model of thin access ports is more and more gaining acceptance since it is easier to manage and provides more flexibility.

Typically thick access points typically provide as many features as possible – that is actually the reason why they are called “thick”. The huge feature set causes these devices to be more expensive and more difficult to maintain because each device must be managed individually. As a consequence, thick access points need to be configured, updated and monitored using third party software, which causes additional efforts.

The approach based on thin access points is different since the wireless switch centralizes and integrates network intelligence and management functions with the result that the access ports do not need to be intelligent. Additionally, the wireless switch system also provides an infrastructure for enforcing network policies, network security and Quality of Service.

3 Advantages in terms of Cost and Technology

The advantage and difference of a centralized wireless system in comparison to a standard access point/access client infrastructure is the ease of migration once network requirements and organizational needs are changing. As soon as an access point is connected to a wireless backbone, the centralized intelligence automatically identifies this new infrastructure component and configures it with the necessary parameters in accordance with the entire wireless system. In the end, the efforts managing and operating are reduced dramatically. Enterprises and industrial end users will immediately profit from reduced costs for skilled specialists during site survey and installation (see figure 6).

The centrally managed wireless switch architecture seamlessly integrates with existing wired networks to manage both thick access points and thin access ports, with virtually no disruption to existing network traffic. Wireless network management is simplified since the Wireless Switch serves as a central point of the WLAN for handling all wireless network activities. Through the Wireless Switch and a single IP address, network administrators can access all system management functions using a simple XML-based graphical

user interface. Administrators can control network access, provision and monitor all access ports, allocate wireless bandwidth, and manage all built-in WLAN connectivity services. [1]

Wireless Management

Automatic Site Survey & Deployment Tool

Configuration tool for setup & management of Wireless Switches

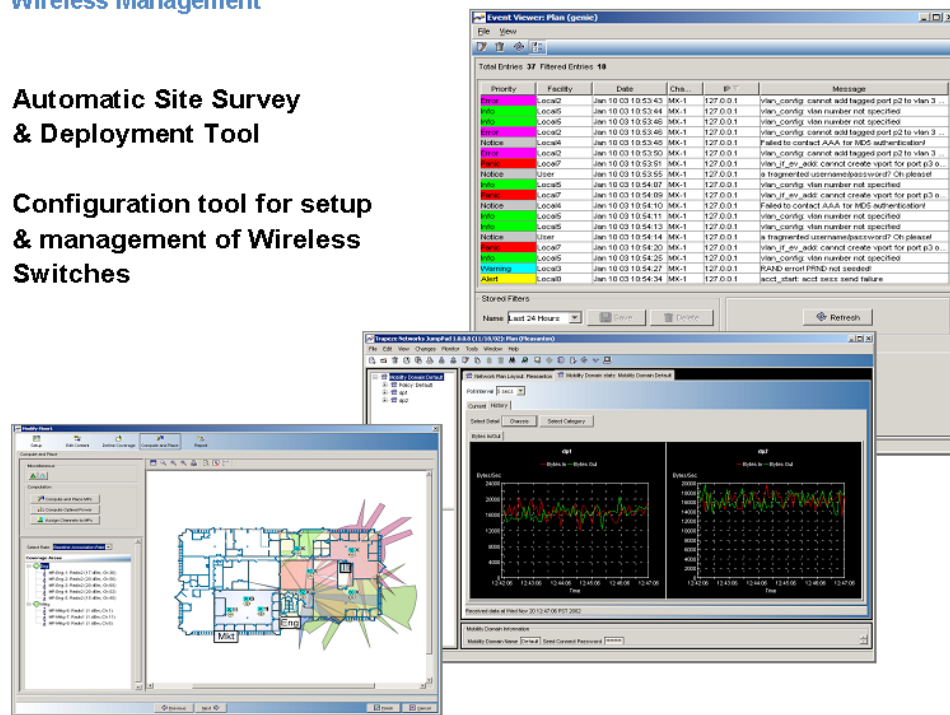


Figure 4: Necessary Tools for a management of a wireless system with shifted intelligence

Reduced Total Cost of Ownership

The wireless switch system significantly reduces the cost of deploying network infrastructure, with a lower cost of managing, maintaining and upgrading the wireless infrastructure. Installation, maintenance and troubleshooting costs are decreased because thin access ports do not need manual configuration, firmware installation or maintenance (see figure 4). The system's functionality, expandability, and centralized management eliminate all the administration time and costs associated with access point-based solutions. With the system's ability to support users, services and standards both today and tomorrow, a wireless switch system provides long-term protection of an enterprise's wireless technology investment. No need to rip and replace hundreds of access points to gain the benefits of essential new features. The system makes it easy to migrate wireless technologies by preserving legacy wireless network designs and facilitating the move from one generation of 802.11-based products to the next. [1]

4 Security concerns

Although wireless technology isn't new to industrial applications, it still carries a certain mystique. But even though industrial engineers seem more comfortable with the perceived security and reliability associated with a wired approach; some are seeing the benefit in wireless. Just compare the situation to Ethernet, a technology blooming in ubiquity because of its commercial communication applications and forcing the industrial community to take notice. Wired Ethernet's simplicity allows industry to more easily and cheaply deploy the technology. And newly developed standards allow quicker adoption, spurring more uses and further lowering cost. [16]

Wireless LANs should be no less secure than their wired counterparts, providing that appropriate techniques are used to implement a flexible and transparent solution. Thick access points are inherently vulnerable in that they are packed with sensitive data such as user IDs and passwords, IP addresses, access control lists and more. Hackers can not only steal sensitive data remotely, in some cases they can steal the access point itself and extract data in the comfort of their homes. The Wireless Switch System eliminates this security threat by providing centralized authentication and encryption that enables simpler and more cost-effective management of security functions and policies without compromising roaming performance. Many vendors provide its customers with today's most secure encryption system for mobile environments. Network management is another challenge. Network administrators aren't looking for greater complexity and demands on their time. Yet each thick access point requires individual care and attention, consuming precious administration time and talent. Conversely, with all management functions centralized in the Wireless Switch, managing a group of thin access ports is as simple as managing a single access port. Centralized configuration in the wireless switch allows distribution of configuration changes and updates to all access ports, eliminating the hours required for configuring and managing individual devices in an access point-based wireless LAN network. [1]

The Paradox: Secure Mobility

While mobility is virtually synonymous with wireless, ensuring secure mobility isn't a simple equation. Here's the paradox: Secure networks aren't mobile. Mobile networks aren't secure. Secure networks are not mobile. The problems of 802.11 WLAN security are well documented: The Wired Equivalent Privacy (WEP) keys, which secure the communication between the wireless client and the AP, are shared across different users associated with an access point (AP). A savvy hacker can crack a static 128-bit WEP key with off-the-shelf tools in a couple of hours. As a result, the IEEE developed new solutions for access control and encryption.

The IEEE 802.1x task group was formed to standardize network access control and to improve wireless encryption. 802.1X includes the Extensible Authentication Protocol (EAP), which permits the use of several authentication protocols (e.g. RADIUS) to control network access. 802.11i is the standard for encrypting the wireless transmissions between clients and APs. It offers two choices for encryption: the Temporal Key Integrity Protocol (TKIP) and the Advanced Encryption Standard (AES). TKIP addresses WEP's known vulnerabilities and provides per-packet key mixing, a message integrity check and a re-keying mechanism. AES, a cryptography algorithm from the U.S. government, delivers the strongest possible encryption, replacing 3DES and DES. [3]

5 The big challenge: Roaming and Security

One of the biggest challenges for IT departments that secure the WLAN with IPsec VPNs is enabling applications to run while users roam. While roaming, they may associate with an AP on another subnet. If the wireless interface loses three sequential packets while a user roams, the IPsec client is forced to reauthenticate. Forcing client re-authentication breaks the sessions of delay-sensitive applications—everything from hot synchronizing a PDA while walking down the hall to voice-over-wireless-IP (VoWIP) calls. To maintain IPsec VPN sessions, some systems perform network address translation (NAT) to allow the client's IP address to remain the same. If the IP address changes, the IPsec client must re-authenticate since the session is dependent on the specific IP address. The vendor's implementation of NAT will vary widely in support for "special" protocols such as the File Transfer Protocol (FTP), H.323 videoconferencing or voice-over-IP (VoIP). With 802.1x, the mobile enforcement of policies, such as VLAN membership, becomes possible. Users may roam across subnet boundaries while retaining their VLAN memberships and IP addresses. When IPsec VPNs are combined with an 802.1x-enabled WLAN, the VPN session can be maintained more reliably as the user roams. [15]

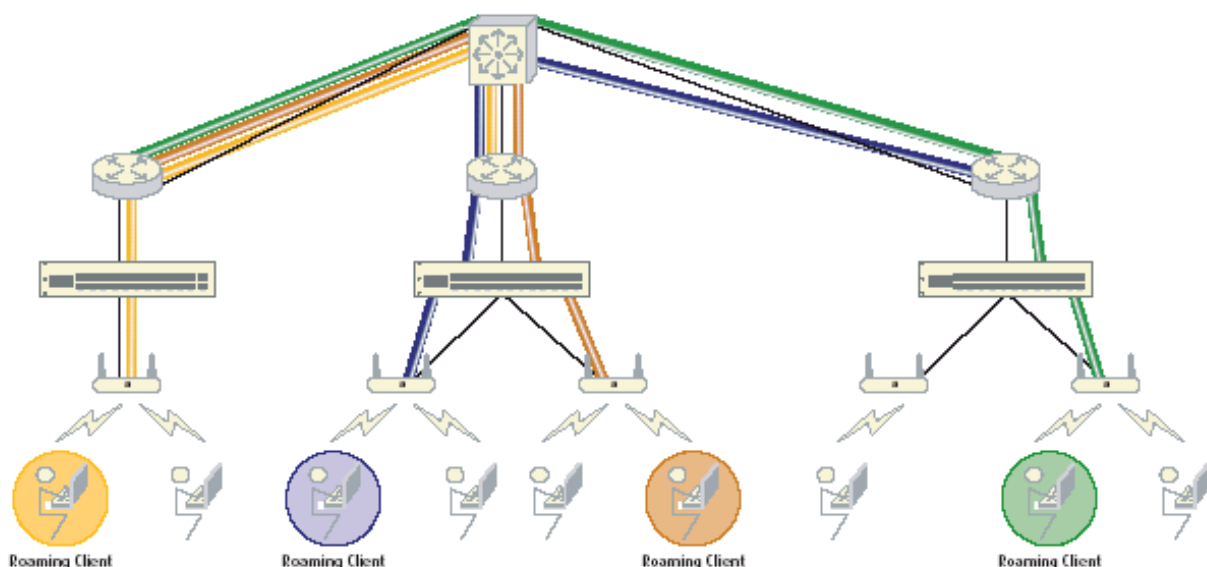


Figure 5: Roaming in a wireless system with shifted intelligence [3]

Deploying standards-based 802.1x authentication as an overlay to Ipsec VPNs is an excellent security solution when IPsec VPNs are a requirement. Together, they secure the enterprise end-to-end and over the air, no matter where users roam. 802.1x gives you Layer 2 protection that cannot be provided by Layer 3 Ipsec VPNs. 802.1X patches the holes with IPsec authentication, in particular the use of the non-standard XAUTH shim to authenticate users to a RADIUS server. IPsec solves the end-to-end security problem and it can be FIPS compliant with the right implementation of a PKI. Deploying 802.1X with IPsec VPNs can provide your users with the most secure, seamless mobility. [15]

Secure Roaming

There are systems available eliminating the security risk most IT directors in enterprise and factory automation are concerned about deploying wireless technology. Unlike traditional switches, the new systems are designed to track an extensive amount of user information to ensure security throughout the wireless deployment. They store such data as user name, authentication information, roaming history, and access rights. This collection of data ensures appropriate network access even as users roam. As a result, users can maintain a single network logon, without the need to reauthenticate or re-logon wherever they roam throughout the enterprise or factory floor (see figure 5). [14]



Figure 6: Picture: support for third-party APs includes the ability to model the RF signal contours of those APs. This view shows two third-party APs modeled on the left and three mobility points on the right. [12]

Many enterprises and industrial end users have installed wireless LANs using the traditional access point-based architecture while using add-on products to provide additional management and security features. The problem is that none of these add-ons deliver a complete, integrated solution for managing and securing a wireless LAN - nor do they provide switching functionality to integrate the wired and wireless network. Although a traditional wireless network with thick access points may look like a switched-wireless network with thin access points on paper, it does not work the same. Thick access points are still “smart” entities that require configuration, management and support. In addition, the few additional services that these devices provide adds significant time and labor costs because of the installation, configuration and administration that they require. [1]

6 The future

Wireless networking is one of the fastest growing sectors in technology. Wireless-enabled LANs are rapidly replacing wired local area networks in all areas like business and home application as well as on factory floor. The technology is leading the way to a new “always on” world where people, businesses and machines will be able to connect at any time, anywhere. In the last few years, the global market for wireless Internet devices has skyrocketed, projected to reach \$73 billion by 2005, according to a study conducted by Strategy Analytics Inc. Today, individuals, businesses and industrial end users are accessing networks and the Internet through a wide variety of mobile devices. Wireless services such as location-based services tied to GPS satellites and instant messaging using cell phones and personal digital devices are becoming increasingly vital to keeping employees and remote machinery connected. This new reality is empowering individuals, enterprises and end users in industrial environment to access information and communicate faster and easier than ever before possible. [1]

Summary

The wireless switch with shifted intelligence offers a superior approach to wireless local area networking. This technology centralizes intelligence, control and management functions for the wireless network and provides an easy and cost effective way to add users and features. Intelligence previously designed into the access points of a WLAN is now integrated within the central switch enabling significant improvements in functionality, scalability, flexibility and extensibility. The wireless switch system is the optimum way for industrial end users, too, to unify network access, security, policy management, roaming control and QoS at the switch level, while delivering the highest level of wireless security to protect network, data and devices without compromising service. [1] As a consequence, the industrial end user will profit from a higher system availability due to reduced failure rate of access points – according to reduced complexity - in combination with a centrally managed wireless control mechanism.

7 References

- [1] What is a Wireless Switch and the value of the Overlay Architecture? Symbol Technologies, Technical White Paper January 2005.
- [2] Securing Enterprise Air: Understanding and Achieving next-generation Wireless Security with Symbol Technologies and 802.11i. Symbol Technologies, Technical White Paper February 2005.
- [3] Achieving Secure Mobility for the Wireless LAN. Trapeze Networks, Technical White Paper 2005
- [4] AP Architecture Impact on the WLAN, Part 1: Security and Manageability. Trapeze Networks, Technical White Paper 2004
- [5] AP Architecture Impact on the WLAN, Part 2: Scalability, Performance and Resiliency. Trapeze Networks, Technical White Paper 2004
- [6] Detecting Rogue Users and APs in a Wireless LAN. Trapeze Networks, Technical White Paper 2004
- [7] WLAN Total Cost of Ownership: Comparing Centralized and Distributed Architectures. Farpoint Group, Technical White Paper January 2004.
- [8] J. Yee and H. Pezeskhi-Esfahani, "Understanding Wireless LAN Performance Tradeoffs," Communication Systems Design, November 1, 2002,
- [9] J. Andersen, T. Rappaport, and S. Yoshida, "Propagation Measurements and Models for Wireless Communications Channels," IEEE Communications Magazine, pp. 42-49, January 1995.
- [10] V. Erceg et al, "An Empirically Based Path Loss Model for Wireless Channels in Suburban Environments." IEEE Journal on Selected Areas in Communications, pp. 1205-1211, July 1999.
- [11] S. Arnesen and K . Haland, "Modeling of Coverage in WLAN," PhD Thesis , Agder University, 2001.
- [12] Multivendor Interoperability. Trapeze Networks, Technical White Paper 2004
- [13] WLAN Security and Identity Awareness. Trapeze Networks, Technical White Paper 2005
- [14] Defining a Mobility Switch. Trapeze Networks, Technical White Paper 2004

[15] The Illusion of Security: Using IPsec VPNs to Secure the Air. Trapeze Networks, Technical White Paper 2003

[16] Be vigilant - Don't make a hacker's job easy. Frank Williams, ELPRO Technologies, California, August 2005.

Frank Seufert
Hirschmann Automation and Control
Neckartenzlingen, Germany