

Karlsruher Arbeitsgespräche Produktionsforschung 2010

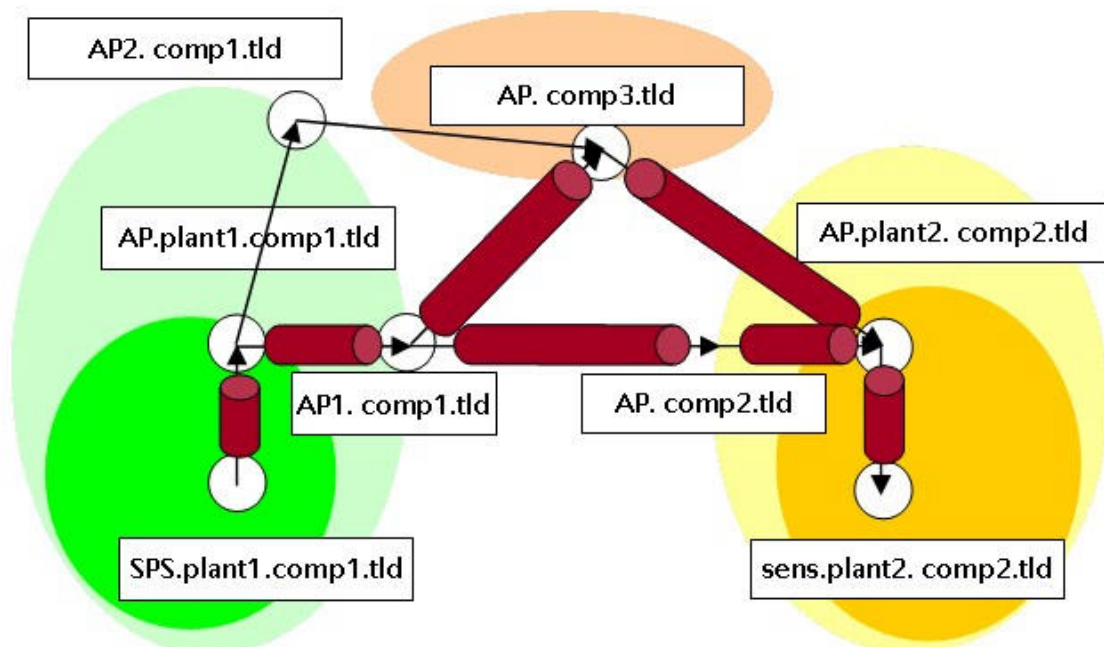
Presentation of Research Results / Challenges for Production Research

Virtual Automation Networks – a project sponsored by the EC with KIT as project manager

Embedded in the context of presenting research results from latest public projects during the conference “Karlsruher Arbeitsgespräche Produktionsforschung 2010” on March 9 and 10, an overview of the main results of the VAN project will be given in forum III, session 2 “Forward-looking International Cooperation”.

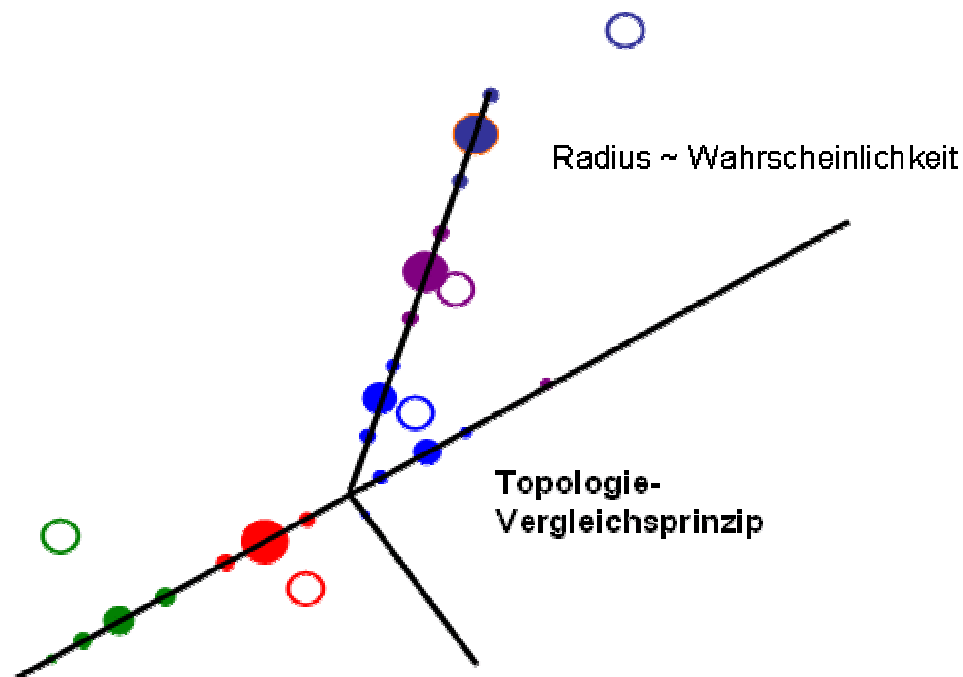
VAN Architecture

Beside the introduction of the consortium and the project structure, the in VAN used central architecture for industrial communication through public networks is central issue of the lecture of the technical project coordinator Ralf Greiner-Jacob. The flexible communication structure, which uses separate VPNs in sub-segments, the name-based access to devices and objects, which is also possible in private addressing areas. These VPN routes are with certain constraints in spite of this private IP addressing structure routable and usable for access via DMZ, too. Moreover, the structure offers security against industrial espionage, sabotage and incorrect applications as well as consequent integration of Industrial Safety.

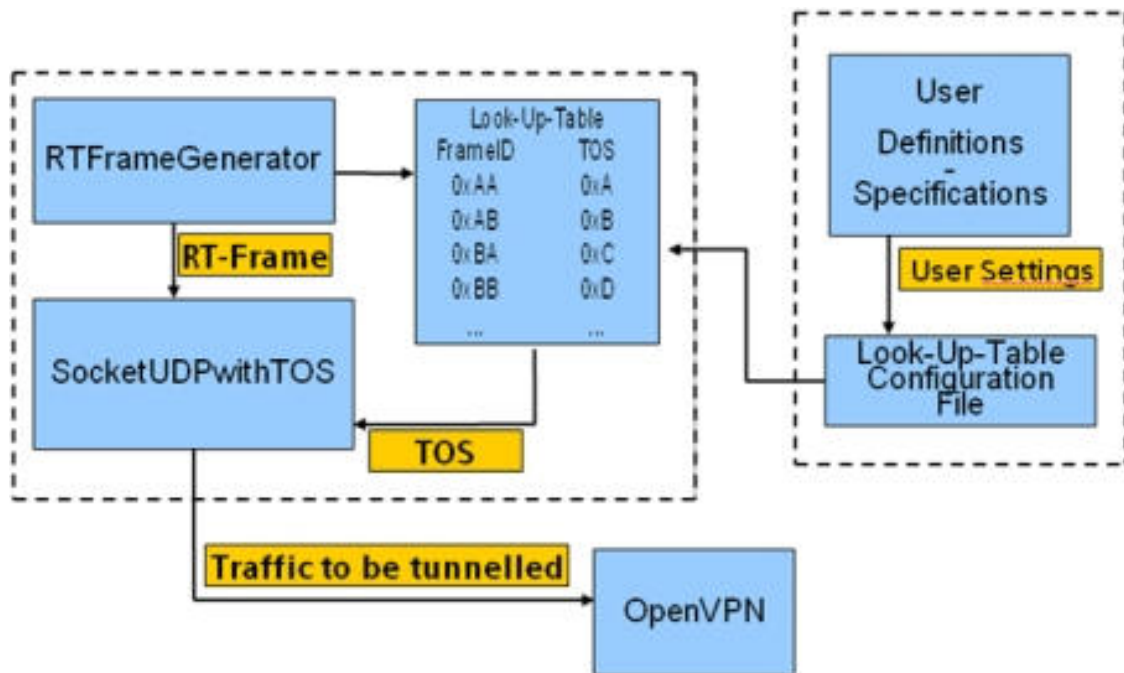


Wireless Communication

The attention of the wireless communication laid on coexistence research, real-time transmission and the positioning of subscribers in a WLAN. Marginal condition for the latter was the demand to use an existing WLAN without retroactive effect to commercially available wireless devices, which can be used in this network. Thus it is for example possible to locate persons carrying a WLAN mobile phone or to establish the positions of vehicles, which use a connection in the WLAN or are even controlled by this. Basing on frames or beacons being received by several industrial clients the server is analyzing the signals with suitable filtering methods and computes in that way the position. Further refinements could be achieved with help of a probabilistic process, which uses a topological data base.



With this method test implementations could reach a minimal error of 1.7 to 1.9 meters in the 5 GHz band, the maximum error lied between 3.9 to 5.8 meters, in the 2.4 GHz band appeared a minimal error of 1.8 to 2.8 meters, maximally from 3.59 to 9.01 meters. The reason for the differences in the frequency band could not be identified.



Real-Time

The investigation of real-time communication beard fruits in some noteworthy results. The responsible teams compiled a test implementation for the extension of the existing PROFINET protocol by the service RTOverUDP. By means of a board for comparative measurements the resulting values for latency, jitter, bit error rate and packet loss could be established. The results show that under certain conditions a resistant real-time communication in a public network is possible. Some of these conditions are dealt in more detail below in the paragraph for Telecontrol.

An absolutely necessary condition for that is the improvement of VPN mechanisms when using these real-time protocols by means of TOS mapping. With this the priorities of the real-time frames are mapped to the priorities (TOS parameters) of the VPN frames.

Safety

In the work packets of Safety the usage of the existing safety layer technology PROFISave was verified for public networks. The safety demands required an additional IT security analysis, which was compiled in context of this project. Owing to missing standards for analysis of infrastructure, danger and risk in this area, the analysis was compiled according the VDI/VDE Guideline 2182 "IT Security in industrial automation". Especially the constraints for real-time communication required by the applications limit the usage in the Safety sphere. It could be shown that a broad pallet of possible applications is possible with the reached times. The usage of UMTS however showed that the measured maximal time delays are still not sufficient for a lot of applications to use Safety on this media.

Security

Three essential pillars define the security concept of VAN.

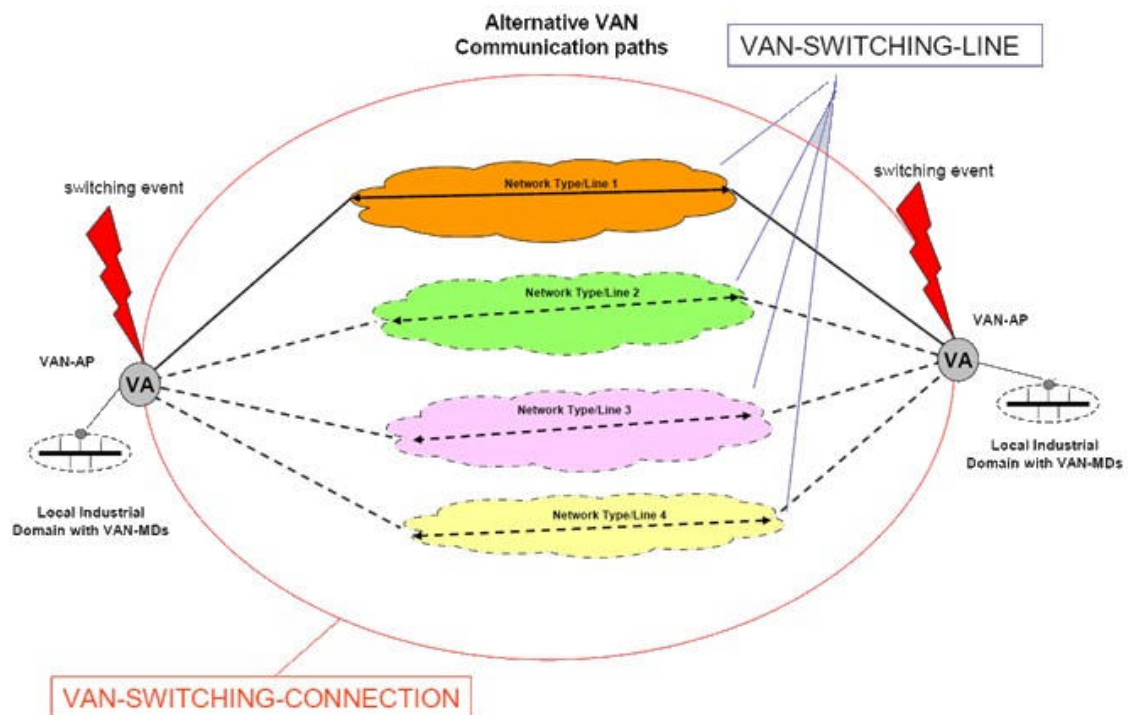
- Administration of the security policy over a separate channel
- Advanced software packets to protect the applications against DoS attacks
- Depth protection by means of numerous security protocols

Some containers with authentication over a separate channel for the administration of the policy make it impossible to manipulate via the request channel. In addition, the implementation of security mechanisms in the application can be dropped and reduce incorrect implementation or application too, or rather enable independent applications. The entire renunciation of write access during evaluation of the policy reduces potential security bugs by another factor.

The depth protection contains filters with white lists (e.g. of addresses). Moreover, a dedicated concept for PKI certificates with machine based communication was elaborated, as well as a guideline for bootstrapping and the associated take-over of the key.

Telecontrol

The increased usage of public networks is accompanied by the fact that certain techniques of Telecontrol have to be included into the common communication. For example a static connection is not necessary between sporadic communicating machines. Possibly a connection can be limited to a few minutes per day for exchange of archives or statistical data, or a connection is only necessary on certain events. This affords communication, which can be dynamically initiated from both sides, as well as a connection specific storage of values during an offline phase. With it come filters in order not to need catching each intermediate value, e.g. to fix an interesting interval of values. Basing on a real-time peer-to-peer communication protocol a minimal Telecontrol profile was implemented, which covers the mentioned requirements and which can be integrated into the communication of the application, if required.



Moreover, a constant measurement of the communication quality offers the possibility of a dynamical swap of the provider access, as soon as a no longer acceptable level of a certain critical parameter is reached, like jitter, delay or packet loss.

Configuration

The configuration of the VAN devices was done by Web Services. Basing on the XML technology a tool was programmed, which can load certain VAN device descriptions and offers then resulting facets during a certain commissioning project. The device description defines the selection of the relevant functionalities of a device; the description a functionalities contains an input mask for the corresponding parameters. Together with these actions a stand alone tool was developed, which can independently be used in addition to a device specific engineering and an implementation, which is integrated into Step7 that shows, how the VAN functionality can be integrated into existing engineering tools as a packet.

Validation And Test

Accompanying Trend and Technology Screening

One factor of success of the project was the parallel running screenings of the topics handled in the work packets. With this, an immediate feedback was given, whether the current trends and continuously new publications of automation products evolve in a comparable direction, which is quite necessary for a project with an appropriate long life-span. Moreover, the technology screening offered itself as a fountain of ideas to find solutions for open issues in the all over VAN architecture.

Prototypes in Real Families

Relatively early in the project the activities concentrated towards two prototype implementations each in one facility for manufacture automation and for process automation.



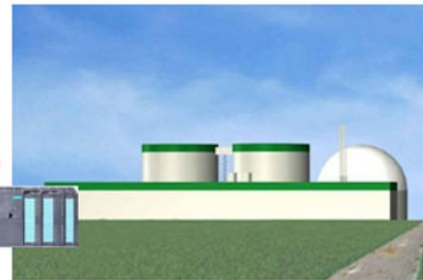
Thus out of the machinery of the parallel ongoing IST project Pabadis Promise a subset machinery for motor fabrication consisting of a central controlling element (JFMX) of the consortium's partner Fidia, a milling machine, a conveyor belt and a robot arm, which lifted machine parts from the conveyor belt in order to put it on the milling machine and vice versa. The VAN specific enhancements in the connected PLCs enabled swapping the location of the JFMX from the local floor to a remote. Accordingly the control of the plant could be overtaken on a breakdown of the local control unit by a different location or, as part of an activated guarantee, by the manufacturer of the device without the need of interrupting the current production. In order to demonstrate this, the test plant in Modugno/Bari/Italy was equipped by a local JFMS, which had the job to transfer the control to a second device, identical in construction, which was located in the about 1000 kilometre distant Vigolzone/Milano/Italy.

The prototype for process automation is a biogas power plant of the company Wabio being in Neukirchen/Saxony/Germany. Wabio plans in Gera/Thuringa/Germany a central control site for this and other facilities, like e.g. the facility under construction in Brieselang/Brandenburg/Germany and others still to be commissioned. One central supervisor controller evaluates the various measurement values from the prevailing bio reactor in order to gain optimal efficiency by adding appropriate raw materials.

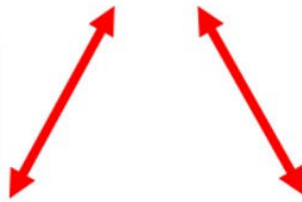
Gera



Neukirchen (in Betrieb)



Briselang (in Planung)



Based on the VAN communication the measure instruments for ethanoic acid concentration are connected via PLCs with the VAN enhancements on both sites to transfer the values in that way. In order to demonstrate the security of the facility, after commissioning of the security packets with PKI certificates a hacker access was simulated. At the same time in the control centre at Gera a notification appeared about the indented intrusion into the Virtual Automation Network.