Virtual Private Infrastructure (VPI) Initiative – An Industry Consortium for Unified and Secure Web Control with Embedded Devices

Axel Sikora
Department of Information Technology
Steinbeis Transfer Centre Embedded Design and Networking
University of Cooperative Education Loerrach
Hangstrasse 46-50, D-79539 Loerrach
Germany

Peter Brügger
President of VPI initiative
IniNet AG

Seewenweg 5, CH-4153 Reinach
Switzerland

***Abstract* - Remote maintenance and control is already widely used in industrial automation and building automation and gains acceptance for many other applications, e.g. smart home appliances, consumer electronics, networking devices. Internet- and web-based connectivity is playing a major part in unifying network infrastructure and company information flow. However, a number of different implementations hinder a true interoperability of devices and exchangeability of suppliers in the different business levels.**
Virtual Private Infrastructure (VPI) Initiative [1] is an industry consortium providing basic guidelines for unified and secure web-based control with embedded devices.

I. INTRODUCTION

Remote maintenance and control is already widely used in industrial automation and building automation and gains acceptance for many other applications, e.g. smart home appliances, consumer electronics, networking devices. Internet- and web-based connectivity [2] is playing a major part in unifying network infrastructure and company information flow. It is a main stepping stone on the way to ubiquitous computing [3].

For embedded internet connectivity, various trends can be observed, which led to the foundation of Virtual Private Infrastructure (VPI) initiative as an industry consortium providing basic guidelines for unified and secure web-based control with embedded devices.

A. Maturing the products

The market for embedded internet is maturing rapidly. Being a research driven discipline for quite a while, internet protocol suites for embedded systems are widely available as stand-alone software packets or included in real-time operating systems. They are widely deployed and reliable. Performance is increased and cost is reduced as semiconductor device dimensions continue to scale.

B. Maturing the market

The market for embedded internet is rapidly following the technical advances. Maturity of the market can be identified by a broad variety of products and solutions, as well as by a fine differentiation of market players. However, this makes markets more complicated and interoperability is at stake.

C. Embedding and unifying internet connectivity and web services

Internet-connectivity gives access to a ubiquitous network of highest availability and reasonable performance at lowest cost. This especially holds true for target-oriented microcontroller-based embedded systems. However, connectivity infrastructure is only the starting point for interoperability and portability. A unified approach at application level (OSI level 7) is the next step. Its broad acceptance in the office and infotainment world, its flexible design and its efficient implementation makes *Hypertext Transfer Protocol* (HTTP) the main contender for automation and control.

D. Breaking the embedded isolation

Interoperability is even more questioned against the background of traditional dedication of embedded solutions, where optimized software hardware co-design and cost efficiency play a major role.

However, embedded internet calls for open systems and comprehensive interoperability through all levels of communication models. A unified data flow from enterprise resource planning (ERP) and management information systems (MIS) to production planning systems (PPS) and field control is envisaged.

E. Leveraging security

If security is of high value for desktop computing, this holds true for embedded computing, where production facilities and other hardware equipment is at risk. Therefore, security has to be at its maximum.

II. VPI – FOUNDATION AND GOALS

All these factors led to the foundation of Virtual Private Infrastructure (VPI) Initiative [1] in August 2002 with 13 founding members. From the very beginning, VPI combines companies of the various levels of value creation chain: There are engineering companies, device and system manufacturers, and service providers. All of them are interested in a common platform for their customers to withstand proprietary solutions in the embedded internet world. VPI Initiative is a non-profit organization registered in Switzerland. It is led by a six-head board.

VPI Initiative pursues several objectives on its way to a unified infrastructure for remote web services:

1) Baseline standards: In order to unify infrastructure, VPI Initiative develops baseline standards, described in paragraph IV. As unification of additional service is required, the standard will be evolved. This holds true for unification of data models, database access, etc. In its first version, the standard describes a basic communication model of a reasonable internet and web architecture.

2) Open certification: Standards are only useful if they can be understood and observed by market partners. Therefore, a certification authority within the VPI Initiative is required to test compatibility against the standard and interoperability between systems of different suppliers.

3) Marketing activities: VPI Initiative has the vision of deploying existing web technologies for many new and existing applications. To enable advances in technology, products, and markets, all members of the companies shall actively promote the VPI idea based on the same concepts.

III. VPI – OPEN STANDARD

The VPI Standard is an open standard enabling evolutionary compliance for many systems. Its main requirement says, that all transactions, which devices offer to the network, can be handled via HTTP 1.1, as described by RFC 2068 and 2616 [4]. Other protocols may be implemented. However, it is of vital importance, that their functionality is accessible via HTTP as well. HTTP is the common platform for all VPI-based transactions of components and systems provided by different suppliers. Thus, all services are accessible as web services via public internet. Integration into third-party applications is possible.

Additionally, VPI standard sets up rules for the highest possible portability of systems, e.g. no absolute links or addresses are allowed. And last but not least, security is a major stepping stone towards ubiquitous embedded computing.

The VPI Standard is currently under development. It is planned to get it developed and ratified within this year. Therefore, this paper covers only basic ideas and typical use cases.

III. VPI – ARCHITECTURE

Virtual Private Infrastructure (VPI) systems connect remote devices to the Internet via a VPI Portal. VPI uses HTTP from the VPI Portal to the VPI Agent to communicate with the remote device. The VPI Portal forwards the HTTP requests to the VPI Agent, which acts as relay station and forwards it to the VPI Device itself.

All those elements are called VPI Nodes and are explained in detail below.

A. VPI Client

The VPI Client is a HTTP Client. It works as a remote control or service station. It may be a custom web-browser but also an integrated application. Its hardware base may vary: It may be a PC, a so-called internet appliance (PDA, web tablet, smart phone), or a microcontroller-based embedded system.

Java applets may be understood and executed by VPI Clients. If Java applets are not supported, they shall be ignored, but shouldn't obstruct the VPI Client's operation.

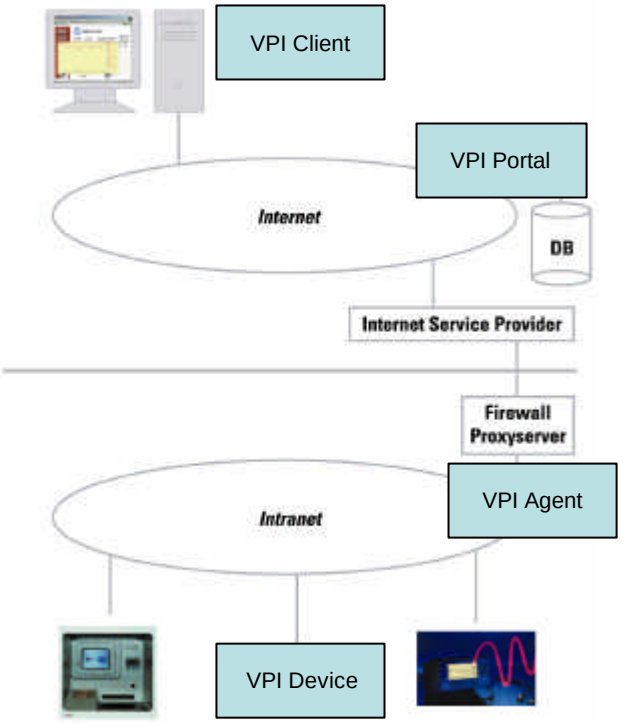

Fig.1 Architecture of a VPI System

B. VPI Portal

A VPI Portal is a communication platform that has to be transparent on HTTP-level. It receives requests from VPI Clients via TCP port 80 and relays them to VPI Agents. This also includes the transparent relay of remote procedure calls (RPC). In the same way, it relays the responses of VPI Agents to VPI Clients. VPI Agents may be reached via public internet facilities, but also via private dial-up or leased wired or wireless lines.

Thus, a VPI Portal is more than just a HTTP Proxy. It is the central administration platform for the all target devices in the system. It runs a list with the links of all target systems to which he has right of access. When a target is selected, a transparent HTTP connection is established to the VPI agent.

VPI Portals are mandatory in VPI Architecture: No VPI client is allowed to communicate directly with VPI Devices. Thus, availability, flexibility and security is enhanced.

Availability and flexibility is provided, as VPI Portals are located with an Internet Service Provider (ISP), or at any location in the public Internet. It may be implemented with redundancy, as well concerning the VPI Portal itself, but also with regard to the connection to VPI Devices. A VPI Portal provides access security, as the user has to authenticate against a user/password database.

A VPI Portal can handle additional tasks, such as event-driven messaging or escalation of error cases. It might also be the interface to enterprise resource planning (ERP) systems, helping to provide a unified and complete supply chain management. All functionality that is added to a VPI Portal has to be independent from the transparent communication flow.

C. VPI Agent

The VPI Agent is used to make devices within an intranet accessible from the VPI Portal. The operator of the intranet has control over the VPI Agent and can define at any time which target systems should be visible on the Internet. Additionally, the available procedures, variables and devices are provided as process points.

In most cases the VPI Agent is a software module which can be deployed on any system within the intranet, e.g. a PC, a server or a suitable embedded device. For operability behind firewalls, it is required, that the VPI Agent's HTTP Server works via TCP Port 80.

The VPI Agent is optional. The VPI Portal may directly access VPI devices. This is important for direct dial-in connectivity. However, if a VPI Device is assigned to a VPI Agent, the access to the VPI Device is limited to this VPI Agent only. VPI Agents allow the access to VPI Devices in networks with private IP addressing schemes. A VPI Agent can also be a gateway to other, non-IP based networks.

D. VPI Device

Any device with an embedded Web server can be used as a VPI Device, as long as the requirements, provided by the VPI standard are fulfilled. The implementation technique of the web server is of no importance to VPI compliance. It may be software or hardware, or even a gateway-based solution, depending on the requirements.

Remote control of VPI Devices is performed via process points.

IV. VPI – HTTP USE CASES

The following examples demonstrate the use of HTTP for the different use cases.

1) Information Download: For information that is downloaded from a VPI Device to a VPI Agent, from a VPI Agent to a VPI Portal or from a VPI Port to a VPI Client, the HTTP GET-method is used.

2) Information and Command: If information or commands shall be sent from the VPI Client to the VPI Device via VPI Portal and VPI Agent, the HTTP POST-method is used.

3) File Upload: If any element in the VPI hierarchy offers a file-upload, e.g. via FTP, then the same service must be offered using the HTTP POST-method.

4) Remote Procedure Calls: A VPI Agent may offer remote procedure calls (RPC) either within an HTML-page or via a RPC-standard such as OPC, RMI, DCOM, or Corba. Thus, read or write access to the connected process points may be established. If this is the case, the same functionality must be accessible via HTTP and TCP port 80. It may be realized via a function call (cgi-bin), a servlet or a SOAP command.

5) Process Point Relaying: If process points, which are requested, are not within the range of one VPI Agent, it may forward the request to another VPI Agent. It is essential, that this forwarding procedure is accessible via HTTP and TCP port 80. Additionally, no absolute addressing is allowed.

6) Event-Driven Messaging: The VPI Agent may wish to send messages to another system, e.g. with an SMTP client. If this is the case, the same functionality must be accessible via HTTP and TCP port 80. In order to accomplish this, a VPI Agent can access other VPI Nodes with HTTP methods GET and POST.

V. VPI – SECURITY LEVELS

The basic idea behind VPI is that security has to be provided by applications, not by networks. This certainly is a lesson learnt from office data network administrators, where port scanning allows an easy access to networks with only port-based firewalls. But also stateful firewalls provide a low security level towards public internet, when applications show security risks. With all functionality being accessed via TCP port 80, most firewalls systems should transmit VPI traffic. This eases portability of VPI systems, as they can be located in company's networks without implications to standard network security administration. This holds true as well for large and ingenious networks as for simple small office / home office networks. However, additional counter-measures against attacks and eavesdropping from within the company's network and from the outside internet have to be taken. Security is provided in various steps:

1) Correctness by Construction: VPI systems are robust against erroneous or unauthorized operation, as all commands for the remote devices are generated within the system. All commands for the devices stem from a VPI Portal or a VPI Agent. Therefore, the access to VPI Portals and VPI Agents must be made as secure as possible.

2) Authentication: A VPI Portal asks the VPI Client to authenticate at least against a user / password database. Challenge response mechanisms are to be used to ensure secure transaction and to avoid denial-of-service attacks.

3) Encryption: The traffic between any two VPI Nodes may be encrypted. VPI compatible systems use HTTPS via TCP port 81 or SSL for encryption [4]. This approach is similar to Virtual Private Networking (VPN). However, as intermediate relay-points such as a VPI Portal or a VPI Agent are used, security can be device-oriented, instead of network-oriented. This helps to simplify network architecture, which tends to be complicated for a network with many mobile or nomadic devices.

4) Logging: A VPI Portal may log all transactions, as in most cases, it doesn't suffer from resource restrictions. Transaction logging leverages not only access control, but is a major part in system control and security.

VI. SYSTEM EXAMPLE

A system example with a distributed set of participating companies maximum is shown in Fig. 2.

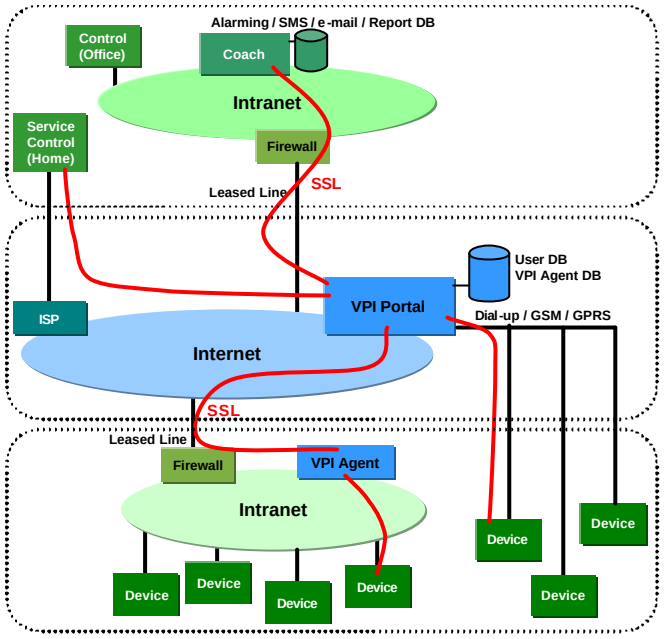

Fig.2 Architecture of a VPI system

1) Service Company: A Service Company runs systems for a customer. For this, the appropriate information is put in a database. The specialists in the service company may access the VPI Portal via their intranet. This intranet is secured with a firewall. However, as VPI Clients generate standard HTTP traffic, firewall filters don't apply.

It is well possible to use encryption on the way from VPI Client to VPI Portal, however, this might endanger portability.

Additionally, the service workers can access the VPI Portal from everywhere via the public internet. This makes remote administration faster, less cost-intense and more flexible.

2) Internet Service Provider: It is of major importance that the VPI Portal may be run at a Service Provider, which allows cost reduction, flexibility and availability. However, most ISPs have lots of restriction concerning additional services. As all functions are available with standard HTTP GET- and POST-methods, integration with any ISP is possible.

3) Customer: The customer may run his devices in his own intranet. Crossing the customer's firewall is as easy as with the service company, as traffic characteristics is limited to standard HTTP.

It is well possible to use encryption on the way from VPI Client to VPI Agent or VPI Device, however, this might endanger portability.

In case there are distributed VPI Devices in the field, they may be accessed via dedicated connectivity. The optional VPI Agent is not used in this case.

VII. VPI – COMPLIANCE TESTS

Compliance tests for VPI systems are currently under development at [7] and will be offered within this year as soon as the standard is available. The compliance tests will include conceptual verification as well as real-life tests.

VIII. VPI – MEMBERSHIP

Since its foundation in August 2002, VPI has gained rapid acceptance and unites 17 companies of different fields (Status July 2003). Those are:

1) Semiconductor Manufacturer / Distribution:
- Dätwyler Electronics AG
- Memec AG, Division Impact

2) System Suppliers:
- SSV Software Systems GmbH
- Selectron Systems AG
- Aartec AG
- SAIA-Burgess Controls AG
- Syslogic Datentechnik AG
- Tixi.Com GmbH

3) Service Provider:
- emazy
- Mitsubishi International GmbH
- unimontis AG

4) Enginering and Consulting:
- iniNet AG
- Steinbeis-Transfer-Centre Embedded Design and Networking, Loerrach

5) Software:
- Ascom Systec AG
- Rolitec AG

6) Mechanical Engineering:
- TRUMPF Laser GmbH + Co. KG
- TRUMPF Laser Marking Systems AG

Other companies are invited to join VPI initiative, to continue its way to bring a unified and secure web control with embedded devices into life. This target can be achieved only with a broad community of international companies.

IX. REFERENCES

[1] http://www.vpi-initiative.com

[2] Stevens, R., *TCP/IP Illustrated*, Vol. 1: Boston 1994, Vol. 2: Boston 1995.

[3] Sikora, A., *Technische Grundlagen der Rechner-kommunikation*, Munich 2003.

[4] Fielding, R., et.al., *Hypertext Transfer Protocol -- HTTP/1.1*, RFC2616, available at, e.g.: http://www.ietf.org/rfc

[5] Rescorla, E., *SSL and TLS - Designing and Building Secure Systems*, Boston 2001.

[6] Walter, K.-D., *Messen, Steuern und Regeln per Internet*, Munich 2002.

[7] Steinbeis-Transfer-Centre Embedded Design and Networking, Loerrach; http://www.ba-loerrach.de/stzedn