

Raimond Pigan, Mark Metter

Automating with PROFINET

Industrial Communication
based on Industrial Ethernet

SIEMENS

Second Edition

Pigan/Metter Automating with PROFINET



Automating with PROFINET

Industrial Communication
based on Industrial Ethernet

by Raimond Pigan
and Mark Metter

2nd revised and extended edition, 2008

Publicis Publishing

Bibliographic information published by the Deutsche Nationalbibliothek

The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available in the Internet at <http://dnb.d-nb.de>.

SIMATIC, S7-300, S7-400, ET 200S, STEP 7, Safety Integrated, SIMATIC NET, SCALANCE are registered trademarks of Siemens AG. If trademarks, commercial names, technical solutions or similar are not specifically mentioned, this does not mean that they are not protected. To improve readability, trademarks and the international designations PROFINET, PROFINET IO, PROFINET CBA, PROFIBUS DP, PROFIBUS DPV1, SCADA, SCALANCE, SINEMA are written in conventional notation (uppercase and lowercase letters).

The authors, translator and publisher have taken great care with all texts and illustrations in this book. Nevertheless, errors can never be completely avoided. The publisher, author and translator accept no liability, regardless of legal basis. Designations used in this book may be trademarks whose use by third parties for their own purposes could violate the rights of the owners.

www.publicis.de/books

ISBN 978-3-89578-294-7

2nd edition, 2008

Editor: Siemens Aktiengesellschaft, Berlin and Munich

Translation: Siemens A&D Translation Services, Erlangen

Publisher: Publicis Publishing, Erlangen

© 2008 by Publicis KommunikationsAgentur GmbH, GWA, Erlangen

This publication and all parts thereof are protected by copyright.

Any use of it outside the strict provisions of the copyright law without the consent of the publisher is forbidden and will incur penalties. This applies particularly to reproduction, translation, microfilming or other processing, and to storage or processing in electronic systems. It also applies to the use of individual illustrations or extracts from the text.

Printed in Germany

Foreword

The success story of Industrial Ethernet began in 1985 when Siemens presented the SINEC H1 based on IEEE 802.3. Especially because of its ability to exchange large quantities of data, Industrial Ethernet was predestined for use in production control systems. Three years later, special fieldbus systems such as Profibus started to establish themselves for communication at the field level. These permitted fast and reliable exchange of data between controllers and distributed I/O devices.

However, the increase in the volume of data to be transmitted resulting from increasingly intelligent field devices means that current fieldbus systems have reached their performance limits. With the first presentation of Profinet by PROFIBUS International in August 2000, Industrial Ethernet started to overcome this limitation. Profinet is making the way free for continuous communication from the field level up to the corporate management level.

Profinet as an open Industrial Ethernet standard now satisfies all requirements for industrial applications. It is a standard which combines industrial performance and the strict real-time communication requirements necessary for motion control applications with the advantages of modern office communication.

Profinet IO permits automation solutions to be implemented which were previously exclusively reserved for fieldbus applications. Profinet CBA divides complex automation applications into autonomous technological modules of manageable size. In both cases, existing fieldbuses can be integrated into future structures using proxies.

Profinet is the first communications standard which permits both standard and safety-related communication over Industrial Ethernet. With the PROFIsafe profile certified in accordance with IEC 61508, Profinet satisfies the highest safety requirements for the process and manufacturing industries in accordance with SIL 3 and EN 954-1 Category 4.

Profinet offers a complete solution ranging from industry-compatible cables and connectors up to switches with real-time capability. A security concept specially tailored to automation engineering covers access control, data encryption, authentication and logging, and takes into account the high network security requirements.

By means of Profinet, Industrial Ethernet has been “reinvented”, and its success story extended by a further chapter.

It is also our hope with the second edition of this book that readers will become rapidly and practically acquainted with the topic of Profinet. In addition to correc-

tions, the previous focal points “Distributed I/O” and “Distributed automation” have been updated, and the new topic “Safety” included.

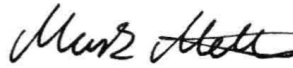
This new edition would not have been possible without our readers and their interest in this exciting topic, without Siemens and its friendly support in all technical matters. Thanks also to everyone who proof-read it in their free time and contributed to continuous improvement of the book with a wide range of constructive suggestions, and last but not least to our families for their understanding and patience during many late nights.

Sincere thanks to all!

Erlangen, August 2008

A stylized handwritten signature in black ink, appearing to read 'R. Pigan'.

Raimond Pigan

A handwritten signature in black ink, appearing to read 'Mark Metter'.

Mark Metter

Contents

1 From Contactor to Open Standard	13
1.1 The Simatic Success Story	13
1.1.1 Change in Structure Through Decentralization	15
1.2 The Road to Industrial Ethernet	15
1.2.1 Industrial Ethernet	17
1.3 Profinet	18
1.3.1 Profinet IO	19
1.3.2 Profinet CBA	20
1.3.3 Real-Time Communication	20
1.3.4 Fieldbus Integration	20
1.3.5 Security	21
1.3.6 Motion Control with Profinet	22
1.3.7 Safety on Profinet	22
2 Ethernet – Fundamentals and Protocols	23
2.1 Fundamental Structure of Ethernet	23
2.2 Standard Ethernet Frame	24
2.3 Ethernet or MAC Address	25
2.3.1 How to Find Out the MAC Address of an Ethernet Device?	25
2.4 Shared Ethernet	25
2.5 Switched Ethernet – Fast Ethernet	27
2.5.1 Switches as Intelligent Star Distributors	27
2.5.2 Full Duplex and Half Duplex Modes in the Switched Ethernet	28
2.6 Functions for Ethernet	29
2.6.1 Autonegotiation	29
2.6.2 Autosensing – Automatic Recognition of Data Rate	30
2.6.3 MDI/MDI-X Autocrossover	30
2.7 Gigabit Ethernet – an Introduction	30
2.8 10-Gigabit Ethernet	31
2.9 Power over Ethernet (PoE)	31
2.10 Protocols Based on Ethernet for Profinet	32
2.10.1 TCP/IP	32
2.10.2 UDP/IP	38
2.10.3 Further Protocols of the Network Layer	40
3 Real-time Communication	42
3.1 Requirements of Ethernet with Real-time Capability	43
3.2 Real-time@Profinet	44

- 3.3 Real-time Communication 47
 - 3.3.1 Send Clock Time and Bandwidth 48
 - 3.3.2 Phase 49
 - 3.3.3 Reduction Ratio and Send Cycle 49
 - 3.3.4 Frame Send Offset 50
 - 3.3.5 Real-time Connection Management 50
- 3.4 Isochronous Real-time Communication 51
 - 3.4.1 Isochronous Real-time Technology 52
 - 3.4.2 Configuration of IRT Applications 53
- 3.5 Time Synchronization 54
 - 3.5.1 Time Synchronization Sequence 55
- 3.6 Profinet Protocol Elements 59
- 3.7 Profinet ASIC 63
 - 3.7.1 Application 64
 - 3.7.2 Development of Profinet IO Devices 66
- 3.8 Protocol Analyzer for Profinet 67

- 4 Profinet IO – Distributed I/O 69**
 - 4.1 The Profinet IO Concept 69
 - 4.1.1 Profinet IO Device Classes 71
 - 4.1.2 Device Model of an IO Device 71
 - 4.1.3 Data Objects 74
 - 4.1.4 Context Management (CM) 75
 - 4.1.5 Application Relations (AR) 75
 - 4.1.6 Communication Relations (CR) 77
 - 4.1.7 Services and Protocols 79
 - 4.1.8 From Configuration to Up-and-Running System 87
 - 4.1.9 Proxy Functionality with Profinet IO 87
 - 4.1.10 Profibus Integration 89
 - 4.2 From Planning to Operation of a Plant 91
 - 4.2.1 Planning the Plant 92
 - 4.2.2 Configuration of Plants with Simatic Step 7 93
 - 4.2.3 Operation of Plant 119
 - 4.3 Diagnostics Functions for Profinet IO 121
 - 4.3.1 Identification and Maintenance Data (I&M Data) 122
 - 4.3.2 Diagnostics with Step 7 and NCM 123
 - 4.3.3 Diagnostics in the User Program of the IO Controller 132
 - 4.3.4 Network Diagnostics with SNMP 133
 - 4.3.5 Diagnostics on the Display Elements of Profinet IO Devices 134

- 5 Profinet CBA – Distributed Automation 148**
 - 5.1 The Road to Distributed Automation 149
 - 5.1.1 Distributed Automation Systems with IEC 61499-1 150
 - 5.2 Profinet CBA 153
 - 5.2.1 Profinet CBA Concept 154

5.2.2 Profinet CBA Object Model	155
5.2.3 Integration of Fieldbuses	159
5.2.4 Profinet and Profibus Devices	159
5.2.5 Simatic S7 and Simatic Net Products for Profinet CBA	161
5.3 Profinet CBA Engineering	162
5.3.1 Generation of Profinet Components	163
5.3.2 Interconnection of Profinet Components with Profinet CBA Engineering Tool	164
5.4 Profinet Components	164
5.4.1 Technological Module	164
5.4.2 Profinet Components	164
5.4.3 Profinet Component Types	166
5.4.4 Device Configurations with Assignable Components	168
5.4.5 Profinet Component Description (PCD)	173
5.5 Creation of Profinet Components with Step 7	174
5.5.1 Creation of a Step 7 Basic Project	174
5.5.2 Loading of User Program Cycle by Communications Processes	174
5.5.3 Creation of the Profinet Interface	176
5.5.4 Creation of Profinet Components	182
5.6 Profinet CBA Communication	183
5.6.1 Interconnections	183
5.7 From Planning to Operation of a Plant	187
5.7.1 Planning of the Plant	187
5.7.2 Creation of Profinet Components with Step 7	188
5.7.3 Creation of Profinet Components with the Profinet Component Editor	194
5.7.4 Configuration of Plants with Simatic iMap	195
5.7.5 Commissioning and Testing the Plant	208
5.8 Profinet CBA Diagnostics	213
5.8.1 Offline Diagnostics with Simatic iMap	213
5.8.2 Online Diagnostics with Simatic iMap	217
5.8.3 Diagnostics using the Display Elements of Profinet CBA Devices	227
6 Profinet User Program Interfaces with Simatic S7	230
6.1 Fundamentals	230
6.1.1 Organization Blocks	231
6.1.2 Function Blocks	233
6.1.3 Functions	233
6.1.4 Data Blocks	233
6.1.5 System Functions and System Function Blocks	234
6.1.6 Records	237
6.1.7 Profinet IO Records	239
6.1.8 System State Lists (SSL)	244
6.2 Coding of Profinet IO Diagnostics Records and Configuration Records ...	247
6.2.1 BlockHeader	247
6.2.2 UserStructureIdentifier (USI)	248
6.2.3 ApplicationProcessIdentifier (API)	248

6.2.4 SlotNumber	248
6.2.5 SubslotNumber	248
6.2.6 ChannelNumber	249
6.2.7 ChannelProperties	249
6.2.8 ChannelErrorType	250
6.2.9 ExtChannelErrorType	251
6.2.10 ExtChannelErrorAddInfo	253
6.2.11 ModuleIdentNumber	253
6.2.12 SubmoduleIdentNumber	253
6.2.13 ModuleState	254
6.2.14 SubmoduleState	254
6.3 Profinet IO User Program Interfaces	255
6.3.1 Organization Blocks with Profinet IO	255
6.3.2 Standard Functions for Communication with Profinet IO	262
6.3.3 System Functions and System Function Blocks with Profinet IO	275
6.3.4 Special Functions for Profinet IO	287
6.4 Profinet CBA User Program Interfaces	294
6.4.1 Organization Blocks with Profinet CBA	295
6.4.2 System Functions with Profinet CBA	297
6.4.3 Special Function Blocks and Functions with Profinet CBA	300
7 Profinet Devices and Networking	305
7.1 Passive Network Components	306
7.2 Transmission Media in Line-based Electrical Networks	306
7.2.1 Electrical Signal Transmission with Profinet using 100Base-TX	307
7.2.2 1000Base-TX	308
7.2.3 Technical Implementation – FastConnect	309
7.2.4 Bus Cables for Fast Assembly – IE FC Cables	310
7.2.5 IE FC RJ45 Plugs	311
7.2.6 Hybrid Connector	312
7.2.7 M12 Connector	313
7.2.8 IE FC Outlets	314
7.2.9 FastConnect Stripping Tool	315
7.2.10 IE TP Cords	315
7.2.11 System Configurations in Electrical Networks with Outlets	316
7.3 Optical Signal Transmission	317
7.3.1 100Base-FX	319
7.3.2 1000Base-SX and 1000Base-LX	320
7.3.3 Fiber-optic Cables – Designed for Industry	321
7.3.4 FO Plug Connections and Permanent Connections	322
7.4 Radio Networks with Profinet	323
7.4.1 Radio Technology	324
7.4.2 WLAN Topologies	325
7.5 Security with WLAN	327
7.5.1 Wired Equivalent Privacy (WEP)	327
7.5.2 WEPplus	328

7.5.3 Extensible Authentication Protocol (EAP)	328
7.5.4 Wi-Fi Protected Access (WPA)	328
7.5.5 IEEE 802.11i (WPA2)	329
7.6 Scalance W	329
7.6.1 The Components of Scalance W	331
7.6.2 Scalance W788-1PRO	332
7.6.3 Scalance W788-2PRO	335
7.6.4 Scalance W744-1PRO	336
7.6.5 iPCF with Scalance W	337
7.6.6 CP 7515	338
7.6.7 IWLAN/PB Link PN IO	339
7.6.8 Accessories for WLAN Devices	341
7.6.9 Configuration and Parameterization of Scalance W	344
7.6.10 Sinema E (Simatic Network Manager Engineering)	344
7.7 Active Network Components	346
7.7.1 NICs – Network Interface Cards for Programming Devices and PCs ...	347
7.7.2 CP – Communications Processors for PLCs in the S7 World	350
7.7.3 Further Profinet Products	356
7.7.4 Fundamental Information on Hubs and Switches	363
7.7.5 Switches for Industrial Use: Scalance X	365
7.7.6 Routers	380
7.8 Topologies for Profinet Networks	382
7.8.1 Star	382
7.8.2 Tree	383
7.8.3 Line	384
7.8.4 Ring	385
7.9 Installation Guidelines for Optimization of Profinet	387
7.9.1 Electromagnetic Compatibility	387
7.9.2 Installation Guidelines for Electrical and Optical Data Cables	388
7.10 Configuration of Scalance X Devices	390
7.10.1 Scalance X005	390
7.10.2 Scalance X100	391
7.10.3 Scalance X100 Media Converters	391
7.10.4 Scalance X200	392
7.10.5 Scalance X200 IRT	393
7.10.6 Scalance X400	394
7.10.7 General Rules for Design of Profinet Networks	395
7.10.8 Summary of Fundamental Standards and Directives Applicable to Profinet Networking	396
8 Profinet Security	398
8.1 Scalance S	399
8.2 Protection Functions of the Security Modules	402
8.2.1 The Firewall Functionality	402
8.2.2 Packet Filters	403
8.2.3 Stateful Packet Inspection	405

8.2.4 Application Level Gateways	405
8.3 Network Address Translation (NAT, NAPT)	406
8.4 Virtual Private Network (VPN)	408
8.5 IPsec Protocol	409
8.5.1 Security Modes of IPsec	409
8.5.2 Key Management with Internet Key Exchange (IKE)	410
8.5.3 Limits of IPsec	411
8.6 Simatic Net Scalance S612 and S613	412
8.7 Simatic Net SOFTNET Security Client	413
8.8 Example Configurations	415
8.8.1 Operation of Scalance S as Firewall	415
8.8.2 VPN Tunnel with Scalance S	420
9 Safety Technology and Profinet	426
9.1 Introduction to Safety Technology	426
9.1.1 Objective of Standards	427
9.1.2 Risk Assessment	429
9.2 Integrated Safety Technology	431
9.3 Technological Concept of PROFIsafe	432
9.3.1 Technical Advantages of PROFIsafe	433
9.3.2 PROFIsafe in the 7-layer Communications Model	434
9.3.3 Discovery of Possible Communication Errors to Achieve Functional Safety	435
9.4 Simatic Products with PROFIsafe Capability	436
9.5 PROFIsafe and Profinet with IWLAN	436
9.6 System Overview of Profinet with PROFIsafe	438
9.7 Profisafe in Practice	439
9.7.1 Programming of Safety Programs	439
9.7.2 Protection of the Safety-related Application	440
9.7.3 Integration of Sensors	441
9.7.4 Verification Support	443
Glossary	445
References	448
Index	454

1 From Contactor to Open Standard

The predecessors of current programmable logic controllers (PLC) were connection-oriented controls with the bit data customary contactor controls. Up to that point in time, controls were characterized by circuit technology. Control tasks were solved by hardware connections between simple logic circuits. The hardware had high space requirements, but the flexibility was greatly limited: every modification usually required arduous conversion work.

In 1968, a group of engineers at General Motors designed the first PLC, and the first functional programmable controllers appeared at the beginning of the seventies. The first devices were designed similar to power equipment, and could be connected using the same cables and tools as for contactor controls. The most significant benefit was that modifications could be carried out independent of the hardware. Microprogrammed PLCs with multiprogram capability came on the market at the beginning of the 1980s, and permitted control tasks to be implemented in the form of software routines.

1.1 The Simatic Success Story

In 1958, Siemens AG introduced the Simatic G, a first modular but not yet programmable concept based on germanium semiconductors with resistor-transistor logic (RTL) (see Fig. 1.1). The Simatic N and H systems with silicone semiconductors and diode-transistor logic (DTL) initially followed in 1964. In the next step, the Simatic C1 and C2 with integrated circuits with high-noise-immunity and surge-proof logic (HLL) were launched on the market starting in 1971, as well as the Simatic C3 with transistor-transistor logic (TTL). One feature was common to these continuously improved systems: none of them was freely-programmable.

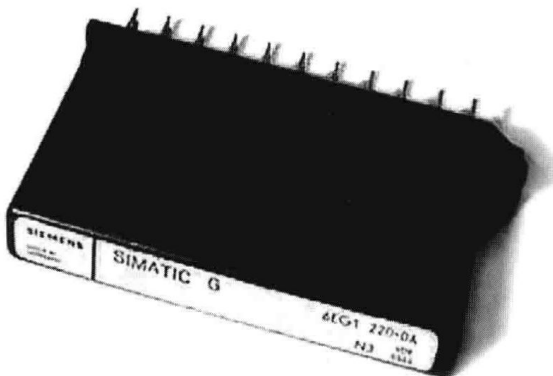


Fig. 1.1
Simatic G module

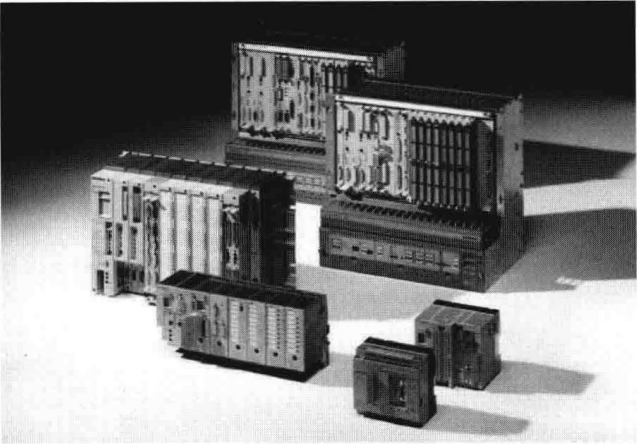


Fig. 1.2 Simatic S5

The freely-programmable Simatic S3 controller was developed in 1973. This PLC is the great-grandfather of modern PLCs. With the Simatic S5 system in 1979, Siemens achieved the complete breakthrough in the mass market to become the global leader (Fig. 1.2).

The Simatic S5 could be programmed using various special languages. Those initially used were the statement list (STL), function block diagram (FBD) and ladder diagram (LAD) in the Step5 software package.

The Simatic S7 range was introduced in 1995. Simatic S7 is the basis for Totally Integrated Automation (TIA). TIA is a uniform solution platform from Siemens for all industrial sectors, and consists of a complete range of matched products and solutions for solving automation tasks.

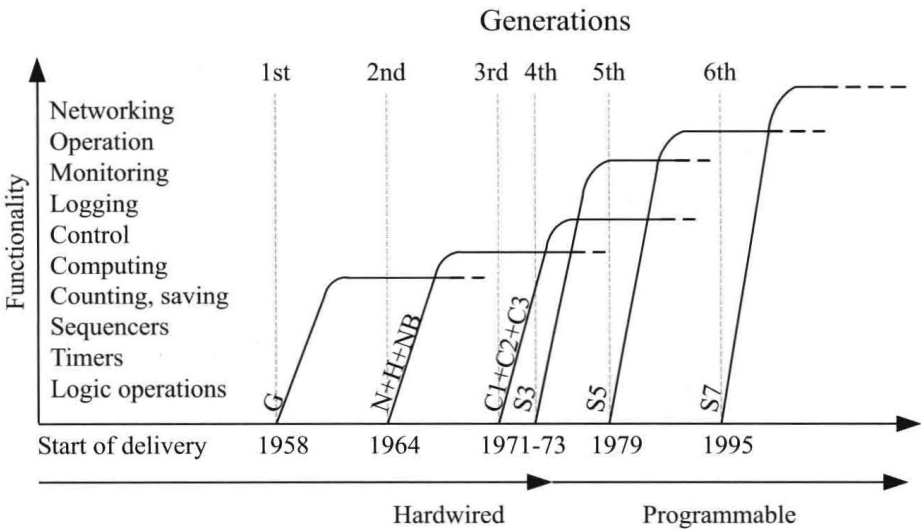


Fig. 1.3 Summary of dates and functions of the Simatic generations

In the course of further development of the Simatic S7, the range was extended by a series of controllers with graded performances and configurations with the associated signal converters for various input and output voltages as well as output currents. In the meantime, the range extends from small PLCs for simple binary operations up to large devices for complex tasks which previously could only be handled by process computers (see Fig. 1.3).

One of the most important factors in the development was the simple handling of the system. A rugged design without fans has been made possible which permits direct connection of external cables using screw or plug systems.

Not only the controllers developed further, the programming environment did as well. In addition to the generation of programs, the programming devices allowed their correction and documentation, plant commissioning and troubleshooting. To permit the supervision and documentation of functional sequences it soon became possible to connect standard I/O devices such as printers and display terminals to the PLCs. The first Windows-based graphical user interfaces for programming became available from 1985. Programming with comment lines and the structured design of PLC programs then became possible.

1.1.1 Change in Structure Through Decentralization

The next innovation jump in the PLC's history was triggered by a change in structure toward the decentralization of inputs and outputs. Decisive for this was the desire to reduce cabling costs. The I/Os moved closer to the place of action, and were connected to the central controller by means of thin two-wire or four-wire cables (fieldbuses). Mini programmable controllers now handled simple tasks directly on site, the central PLCs were offloaded. Control commands were passed on from the central controllers to the distributed switching devices over fieldbus networks. The first I/O devices in IP 65/67 degree of protection meant that additional terminal boxes could also be omitted.

It became quickly evident that further field devices such as drives or valves are required for a distributed automation solution in addition to the distributed input and output devices. At the beginning of the 1990s, a start was made toward standardization of many fieldbuses with the target of defining a future-oriented standard open to all manufacturers. Nowadays, all important bus systems can be connected over different communication interfaces, where Industrial Ethernet, Profibus and AS-Interface are the most important representatives in Europe.

1.2 The Road to Industrial Ethernet

Robert Metcalf presented his idea of the "Ethernet" (Fig. 1.4) at the National Computer Conference in 1976. The term "Ethernet" should be a reminder of the old idea of the "light ether" which surrounds the earth and which, according to ancient tradition, was the propagation medium for electromagnetic energy. Similar to the "light ether", the coaxial cable should be the passive medium for passing on the message from a transmitter to all connected participants.

In 1980, a group of companies with DEC, Intel and Xerox published the so-called DIX standard. This replaced the bis dato experimental state of the Ethernet by an open, fully-specified 10-Mb/s system. Standardization was carried out in 1985 by the Institute of Electrical and Electronics Engineers (IEEE) under the number 802.3 as a networking standard for local area networks (LANs). The way was then opened up for establishment as an industrial standard.

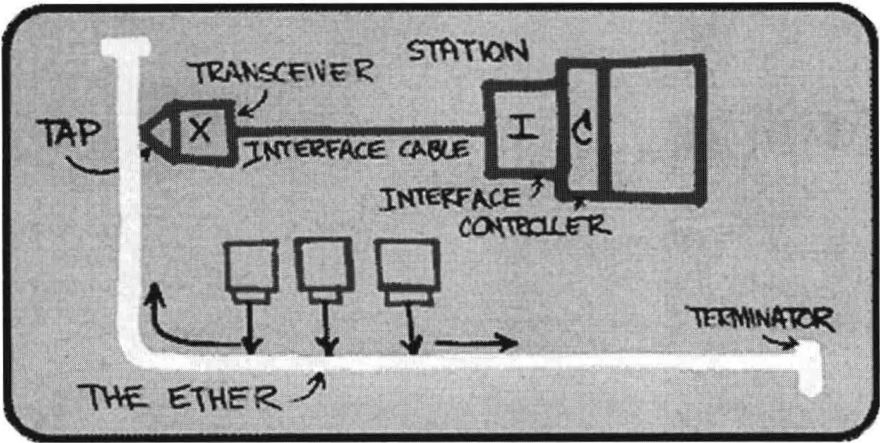


Fig. 1.4 Presentation of the Ethernet at the National Computer Conference

The so-called “Ethernet” is basically a data network technology based on data frames. Ethernet allows all participants present in a LAN to exchange data with every other device connected in the same network in the form of so-called frames or packets. Nowadays, Ethernet technology links devices over long distances all over the globe. The Internet is based completely on this technology. Ethernet describes the type of signaling, and defines the packet formats and protocols. Various components of it also specify standards for media such as cables and connectors. From the viewpoint of the OSI model, Ethernet specifies both the physical layer (OSI Layer 1) and the data link layer (OSI Layer 2). Ethernet is standardized to the greatest possible extent in the IEEE standard 802.3. In the nineties, it advanced to the most widely used LAN technology, and has now displaced all other LAN standards such as Token Ring, FDDI and ARCNET. Ethernet can provide the basis for network protocols such as TCP/IP, AppleTalk or DECnet.

A number of extensions to the Ethernet standard were introduced in the course of time, especially with respect to cabling and speed. The original Ethernet 10BASE5, also known in the meantime as “Thicknet” is of no significance any more. The Thicknet was followed by 10BASE2 “Thinnet”, also named Thinwire or Cheapernet. 10BASE2 used significantly thinner and therefore cheaper coaxial cables, and became extremely popular. It can still be encountered in home or older office networks. The triumph of the twisted-pair standard started in 1990. With 10BASE-T and the associated data transmission rate of 10 Mb/s, Ethernet achieved the final industrial breakthrough.