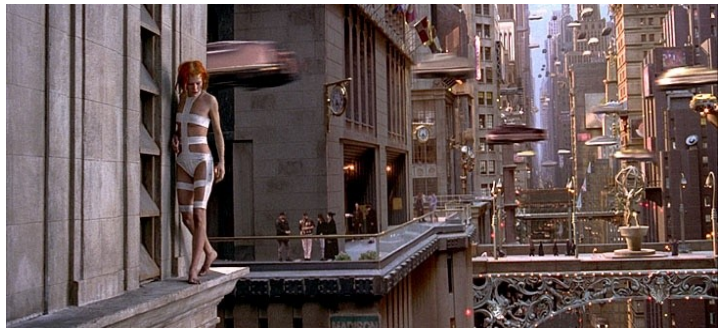
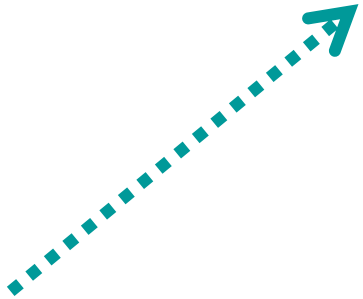
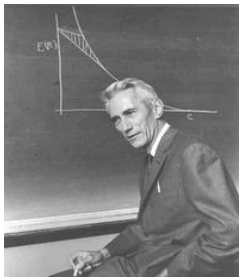
Du Cyber au Cyber-Physique

Gérard Le Lann
Gerard.Le_Lann@inria.fr





Reprinted with corrections from *The Bell System Technical Journal*,
Vol. 27, pp. 379–423, 623–656, July, October, 1948.



A Mathematical Theory of Communication

By C. E. SHANNON

BIRTH OF THE INTERNET

THE ARCHITECTURE OF THE INTERNET AND THE DESIGN OF
THE CORE INTERNETWORKING PROTOCOL TCP (WHICH LATER BECAME TCP/IP)
WERE CONCEIVED BY VINTON G. CERF AND ROBERT E. KAHN DURING 1973
WHILE CERF WAS AT STANFORD'S DIGITAL SYSTEMS LABORATORY AND
KAHN WAS AT ARPA (LATER DARPA). IN THE SUMMER OF 1976, CERF LEFT STANFORD
TO MANAGE THE PROGRAM WITH KAHN AT ARPA.

THEIR WORK BECAME KNOWN IN SEPTEMBER 1973 AT A NETWORKING CONFERENCE IN ENGLAND.
CERF AND KAHN'S SEMINAL PAPER WAS PUBLISHED IN MAY 1974.

CERF, YOGEN K. DALAL, AND CARL SUNSHINE
WROTE THE FIRST FULL TCP SPECIFICATION IN DECEMBER 1974.
WITH THE SUPPORT OF DARPA, EARLY IMPLEMENTATIONS OF TCP (AND IP LATER)
WERE TESTED BY BOLT BERANEK AND NEWMAN (BBN),
STANFORD, AND UNIVERSITY COLLEGE LONDON DURING 1975.

BBN BUILT THE FIRST INTERNET GATEWAY, NOW KNOWN AS A ROUTER, TO LINK NETWORKS TOGETHER.
IN SUBSEQUENT YEARS, RESEARCHERS AT MIT AND USC-ISI, AMONG MANY OTHERS,
PLAYED KEY ROLES IN THE DEVELOPMENT OF THE SET OF INTERNET PROTOCOLS.

KEY STANFORD RESEARCH ASSOCIATES AND FOREIGN VISITORS

VINTON CERF

DAG BELSNES
RONALD CRANE
YOGEN DALAL
JUDITH ESTRIN
RICHARD KARP
GERARD LE LANN

JAMES MATHIS
BOB METCALFE
DARRYL RUBIN
JOHN SHOCH
CARL SUNSHINE
KUNINOBU TANNO

DARPA

ROBERT KAHN

COLLABORATING GROUPS

BOLT BERANEK AND NEWMAN
WILLIAM PLUMMER · GINNY STRAZISAR · RAY TOMLINSON

MIT
NOEL CHIAPPA · DAVID CLARK · STEPHEN KENT · DAVID P. REED

NDRE
YNGVAR LUNDH · PAAL SPILLING

UNIVERSITY COLLEGE LONDON
FRANK DEIGNAN · MARTINE GALLAND · PETER HIGGINSON
ANDREW HINCHLEY · PETER KIRSTEIN · ADRIAN STOKES

USC-ISI
ROBERT BRADEN · DANNY COHEN · DANIEL LYNCH · JON POSTEL

ULTIMATELY, THOUSANDS IF NOT TENS TO HUNDREDS OF THOUSANDS
HAVE CONTRIBUTED THEIR EXPERTISE TO THE EVOLUTION OF THE INTERNET.

DEDICATED JULY 28, 2005

Verification and Evaluation of Communication Protocols

Gérard LE LANN and Hervé LE GOFF
Institut de Recherche en Informatique et Systèmes Aléatoires, Université de Rennes, Rennes, France

Transmission errors, failures and variable transit delays are important characteristics of computer communication networks. Hence, designing a reliable communication protocol for such an uncertain environment is a challenging task. A case study is reported which shows how helpful heuristic techniques can be in protocol verification and a theorem is given regarding synchronization of communicating entities.

Another facet of the communication protocol design issue is efficiency. Heuristic techniques have been used also to evaluate performances of various flow control mechanisms intended for internode protocols and transport protocols as well as performances as seen by users of computer networks. Finally data regarding tradeoff choices are given.

Keywords: packet-switching, simulation, flow control, communication protocols, interprocess synchronization, performance evaluation.

G. Le Lann received his Diplôme d'Ingénieur en Informatique from ENSEIHT, University of Toulouse and his Doctorat d'Etat in 1977, from the University of Rennes. Past activities include design and implementation of a real-time system for the French Navy and a seven computer star network at CERN (Switzerland). In 1972, G. Le Lann joined the Cyclades Project. Since 1974, he is leader of the Computer Network Group at IRISA, Rennes. Recent work includes formalization, design and performance evaluation of computer networks and distributed systems.

H. Le Goff received his Doctorat de Troisième Cycle in 1976 from the University of Rennes. In 1972 and 1973, H. Le Goff was with the Cyclades project at IRIA, participating in the software implementation of the first Cyclades transport stations. Since 1974, he is with the Computer Network Group at IRISA, Rennes. His main activities are related to the design and the performance evaluation and implementation of end-to-end protocols.

Computer Networks 2 (1978) 50–69

Introduction

First transport protocol specifications for the Cyclades computer network were issued in November 1972. It was felt necessary to invest some effort in assessing these specifications before embarking upon an implementation. The responsibility for this was given to the Computer Network Group of IRISA (Institut de Recherche en Informatique et Systèmes Aléatoires). Results of this work led to the definition of a new transport protocol, and are reported in part I.

For the last years, activities in protocol design have been blossoming, specially inside IFIP WG 6.1 (INWG). Part II includes detailed performance studies intended for current internode protocols, transport networks and users of transport networks.

This paper is a complete version of results partially published before [3–6], unpublished material and recent developments.

Part I. Heuristic techniques in verification of communication protocols

1. Introduction

In the Cyclades network [8], the transport protocol and the transport station (TS) are roughly equivalent to the host–host protocol and the NCP in the ARPA network. The initial design of the Cyclades transport protocol included three modes of operation: regular letters, letters on connections (liaisons) and letters on virtual channels (voies virtuelles).

Connections and VC's are opened and closed identically. Nevertheless, they provide for a different service. On VC's, sequential LT references are given by the TS. Error and flow control are performed automatically on a LT basis. A LT is not size-limited.

On connections, LT's are size-limited (255 octets) and are mutually independent. LT references are given by the user. LT's can be or not error-controlled. Flow control is dynamic and works as follows: a credit (CR) must be allocated to the sender for each LT to be sent. Requests must be made continuously

A Protocol for Packet Network Intercommunication

VINTON G. CERF AND ROBERT E. KAHN,
MEMBER, IEEE

fragmentation.

The destination TCP, upon reassembling segment A_1, will detect the ES flag and will verify the check sum it knows is contained in packet A_{12}. Upon receipt of packet A_{22}, assuming all other packets have arrived, the destination TCP detects that it has reassembled a complete message and can now advise the destination process of its receipt.

RETRANSMISSION AND DUPLICATE DETECTION

No transmission can be 100 percent reliable. We propose a timeout and positive acknowledgement mechanism which will allow TCP's to recover from packet losses from one HOST to another. A TCP transmits packets and waits for replies (acknowledgements) that are carried in the reverse packet stream. If no acknowledgement for a particular packet is received, the TCP will retransmit. It is our expectation that the HOST level retransmission mechanism, which is described in the following paragraphs, will not be called upon very often in practice. Evidence already exists[2] that individual networks can be effectively constructed without this feature. However, the inclusion of a HOST retransmission capability makes it possible to recover from occasional network problems and allows a wide range of HOST protocol strategies to be incorporated. We envision it will occasionally be invoked to allow HOST accommodation to infrequent

Any retransmission policy requires some means by which the receiver can detect duplicate arrivals. Even if an infinite number of distinct packet sequence numbers were available, the receiver would still have the problem of knowing how long to remember previously received packets in order to detect duplicates. Matters are complicated by the fact that only a finite number of distinct sequence numbers are in fact available, and if they are reused, the receiver must be able to distinguish between new transmissions and retransmissions.

A *window* strategy, similar to that used by the French CYCLADES system (voie virtuelle transmission mode [8]) and the ARPANET very distant HOST connection [18]), is proposed here (see Fig. 10).

Suppose that the sequence number field in the internetwork header permits sequence numbers to range from 0 to $n-1$. We assume that the sender will not transmit more than w bytes without receiving an acknowledgment. The w bytes serve as the window (see Fig. 11). Clearly, w must be less than n. The rules for sender and receiver are as follows.

Sender: Let L be the sequence number associated with the left window edge.

1) The sender transmits bytes from segments whose text lies between L and up to $L+w-1$.

2) On timeout (duration unspecified), the sender retransmits unacknowledged bytes.

3) On receipt of acknowledgment consisting of the receiver's current left window edge, the sender's

[2] The ARPANET is one such example.

Back to the future?

ARPANET / CYCLADES / INTERNET

Années 60

Aloha (Hawaï) planifié statique CSMA radio

Années 70

Ethernet ≈ Aloha sur câble planifié statique câblé

PRnet (Darpa): nomadic mobile SS radio

(+ GPS, GSM, WiFi, WiMax, CDMA radio, satellites, ...)

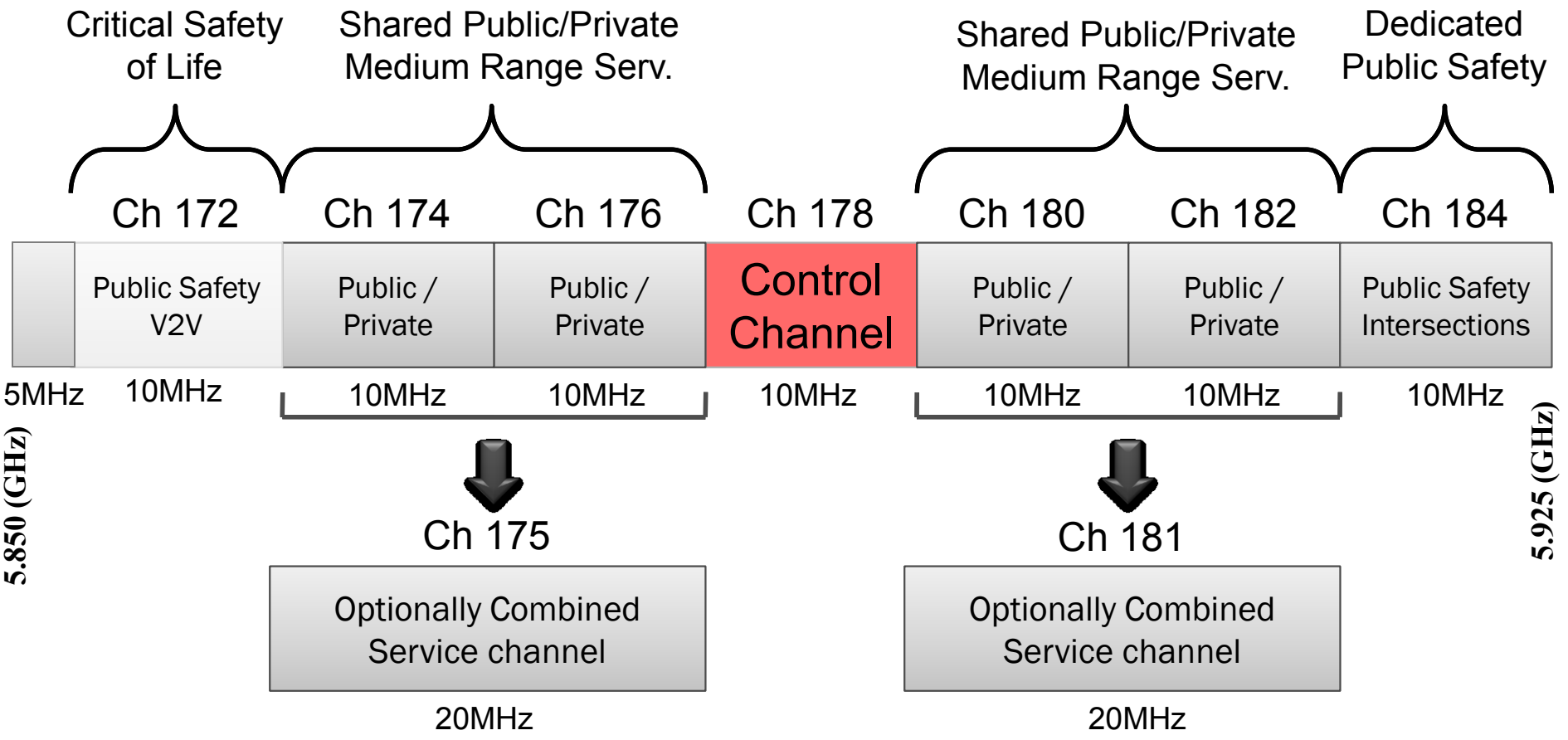
Années 00

WAVE ≈ Aloha mobile ad hoc mobile CSMA radio

[DSRC (IEEE 802.11p, 1609x)]

V2V omnidirectional communications

IEEE 802.11p channels
CSMA-CA

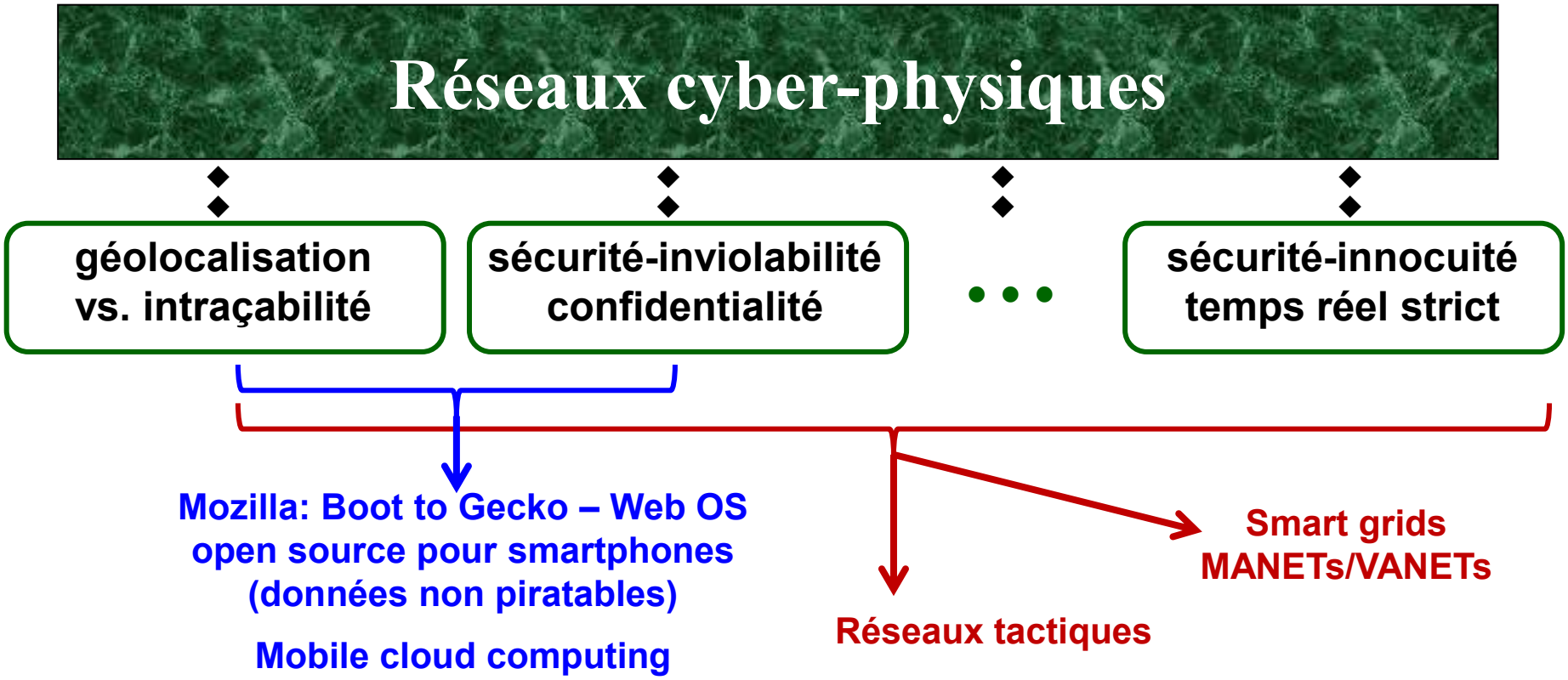


Looking into the future

LTE/4G/... /IoT/...
(hybridation)

Années 10^{++}

planifié/nomadic/ad hoc/opportuniste
statique/mobile/3D
câblé/infrarouge/radio cognitive/...

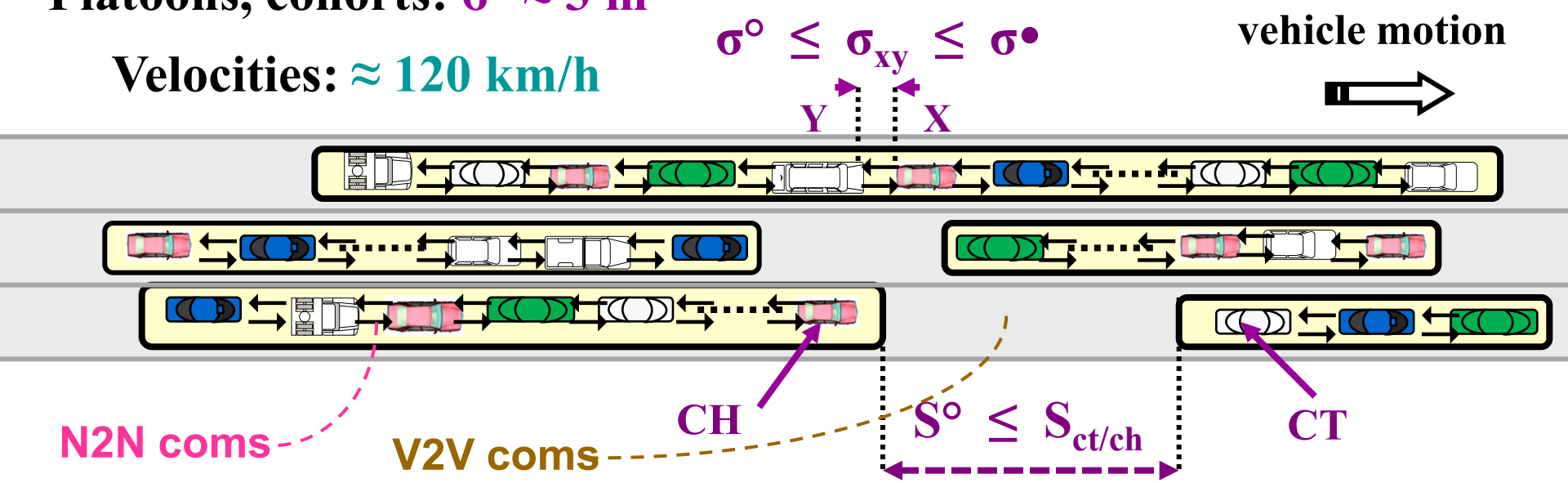


Examples of Cyber-Physical Networks/Systems

Air transportation: Safety figures have a **lower bound** in the order of **$1\text{-}10^{-9}$ per hour**

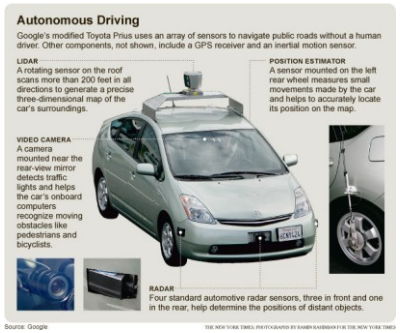
Platoons, cohorts: $\sigma^\circ \approx 3$ m

Velocities: ≈ 120 km/h



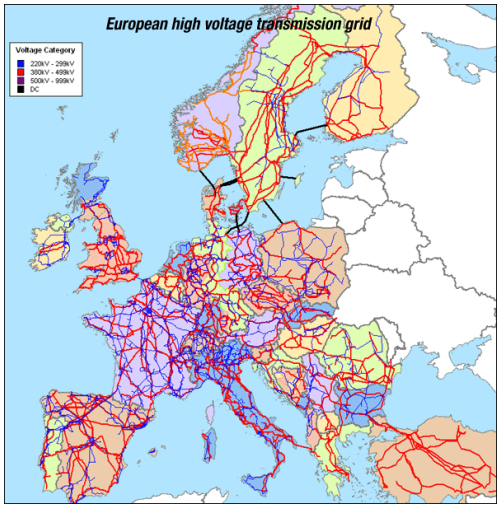
Volvo

Google

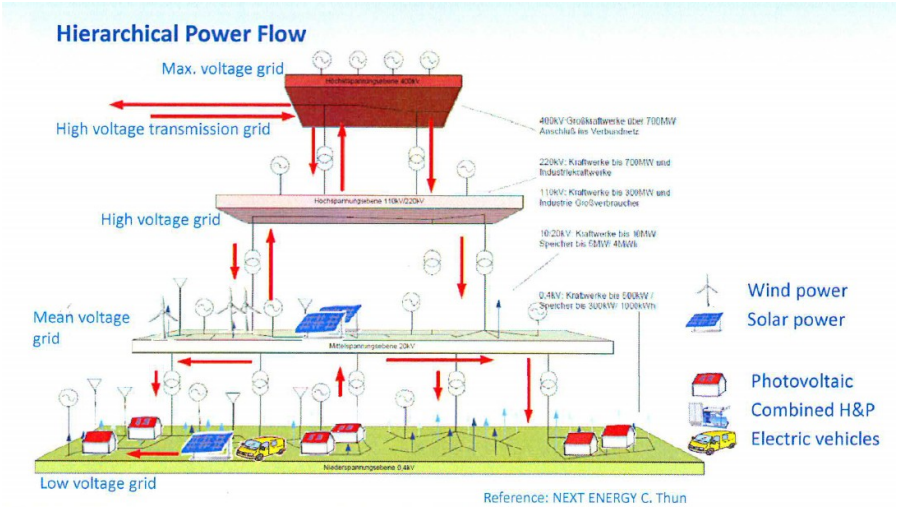


Intelligent Vehicular Networks

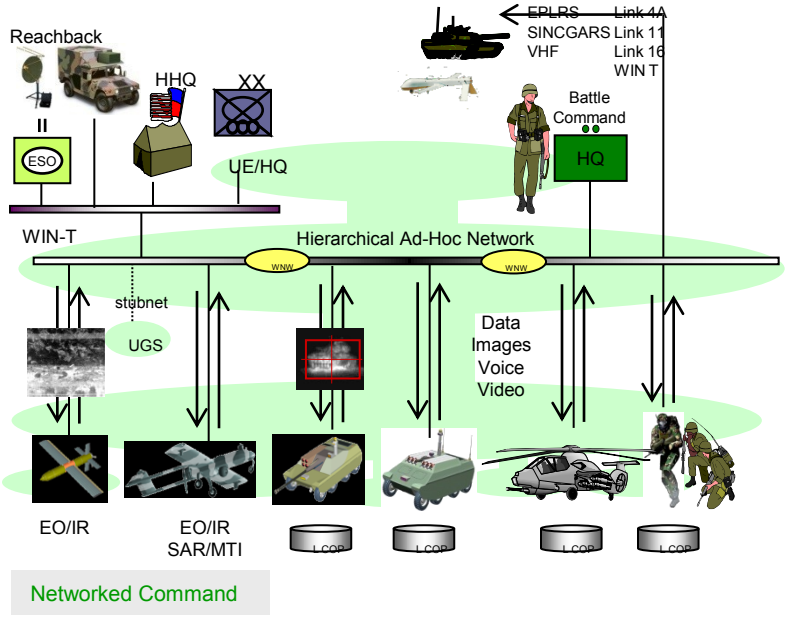
Examples of Cyber-Physical Networks/Systems



Smart Grids



Tactical Networks



Ultra-high safety

Ultra-high reliability

Ultra-high availability

Ultra-tight timeliness

Many open problems with safety-critical communications in mobile wireless cyber-physical networks

Notably:

Can we reasonably expect green lights from safety authorities when asserting:

① « We can develop safety arguments despite lack of guaranteed message deliveries within « acceptable » delays »? …

② « We can develop safety arguments despite lack of guaranteed bounds (worst-case) for radio channel access delays »? …

CSMA-CA is a non solution! Fixed TDMA is a non solution!

∃ un protocole MAC sans collision, qui offre des taux d'utilisation canal très élevés en présence de nombreux mobiles en interférence mutuelle (≈ 75% pour ≈ 870 "contenders")
(to be patented or published)