Electromagnetic Considerations for Computer System Design

Ronald Pose & Carlo Kopp
Department of Computer Science
Monash University
Clayton, Victoria 3168,
Australia
rdp@cs.monash.edu.au

Introduction:

- Computer systems used in sensitive situations and contain valuable information
- Commercial sensitivity
  e.g. in a bank
- Industrial sensitivity
  e.g. control of factory
- Government or political sensistivity
- Military sensitivity

Risks

- Sensitive information leaking out of the computer system
  - This is well studied and understood
- Disruption of computer system operations through external influences
  - Relatively unstudied and not well understood

Information Leakage Risk

- Much effort has been expended on software
  - Secure Operating Systems
  - Authentication Systems
  - Encryption
  - Encrypted Networking
- Some work has been done on electromagnetic leakage
  - van Eck (Tempest)

Disruption of Normal Computer Operations

- Much Work Done in Increasing Security of Operating Systems and Critical Application Programs
  - encryption
  - authentication
  - replication and redundancy
  - self-checking and self-testing
- Little Work Done in Studying Threats to the Physical Operation of Computer Systems

Threats to Physical Operation of Computer Systems

- Physical Security
  – keep the machine physically secure
  – ensure its connections to other machines are secure
  – ensure its environment is benign
  e.g. air conditioning is adequate
- Electromagnetic Threats
  – consider computer system as a whole
  – networking, peripherals, power supply

System-Wide Approach is Essential

- Computers Operate as Systems
  - only as strong as the weakest link
  - highly dependent on networks
  - all components in system must be functional
  - power supply is an often overlooked weakness
- Must Deal with Threats Systemically
  - treat computer system as a whole
  - include its environment and its users

Electromagnetic Threats

- Eavesdropping
  - electromagnetic emissions can be intercepted and analysed to reveal sensitive information
  - emission through networking
  - emission through monitors
  - emission from the computer itself
- Disruption
  - electromagnetic fields
  - magnetic fields
  - power surges

Sources of Electromagnetic Threats

- Terrorist or Commercial Espionage
  - low emitted power weapons
  - low coverage
- Strategic and Military
  - high power weapons
  - could have fairly high coverage
  - designed to disable whole sites

Damage Effects

- Soft Kill - disrupts operations, downtime
  – cause the target to crash or reset
  – cause the target to lose data
  – cause the target to get into unrecoverable state requiring a reboot
- Hard Kill - permanent electrical or physical damage
  – loss of capacity to perform functions reliant on electronic infrastructure

The Electro Magnetic Pulse Effect:

- A nuclear weapon detonated at altitude ionises the upper atmosphere -> EMP
- EMP produces high voltage transients on cables, which damage electronic equipment
- Computers highly vulnerable due high content of high density MOS devices
- Effect similar to lightning strikes, but faster and more powerful

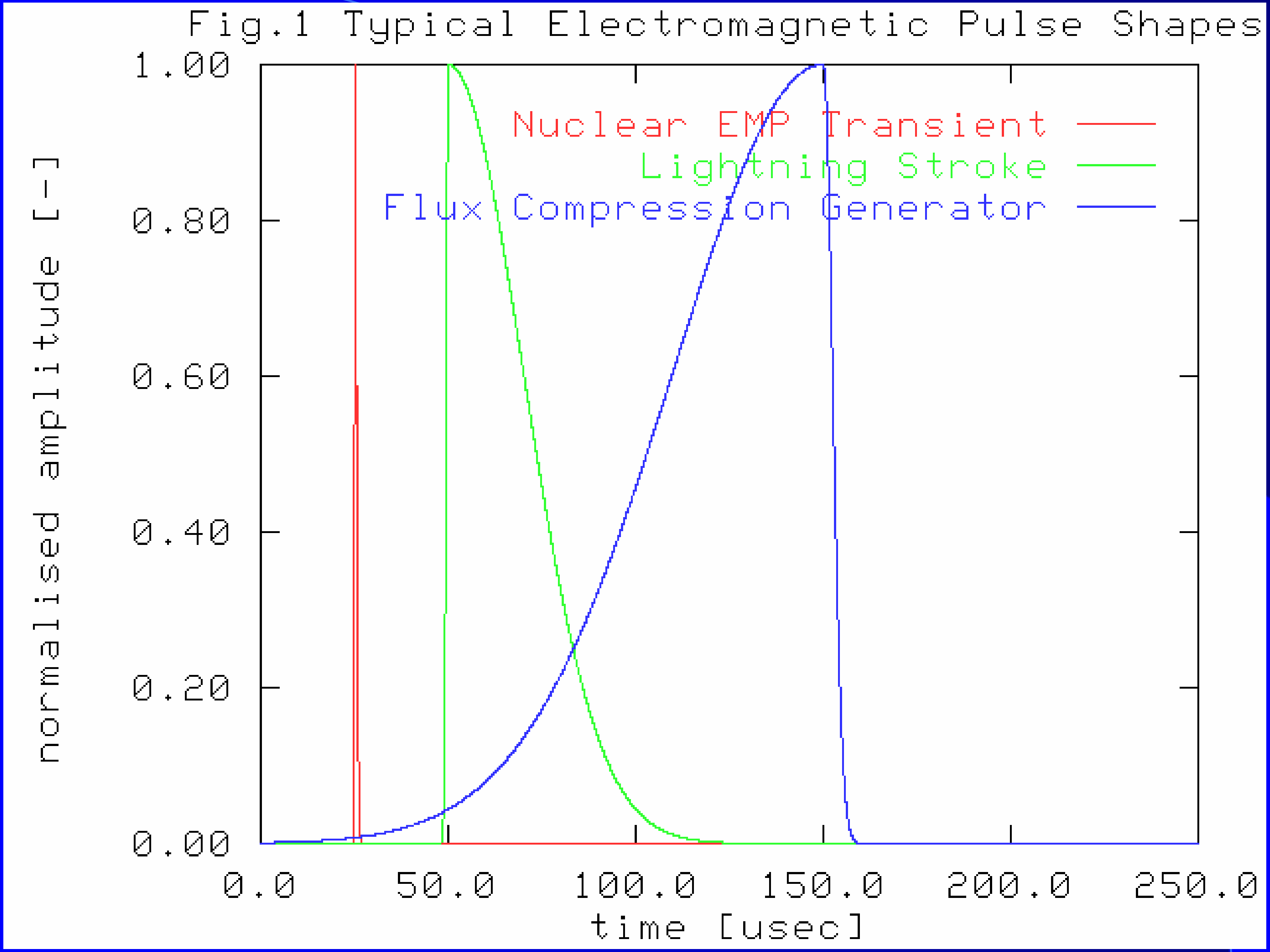
Fig.1 Typical Electromagnetic Pulse Shapes
Nuclear EMP Transient
Lightning Stroke
Flux Compression Generator
normalised amplitude [-]
1.00
0.80
0.60
0.40
0.20
0.00
0.0
50.0
100.0
150.0
200.0
250.0
time [usec]

E-bomb Technology Base:

- Power source - explosively pumped Flux Compression Generator (FCG)
- FCG pioneered by Los Alamos Labs during the 1950s
- FCG can produce tens of MegaJoules in tens to hundreds of microseconds
- Peak current of an FCG is 1000 X that of a typical lightning stroke

The Physics of the FCG:

- Fast explosive compresses a magnetic field
- Compression transfers mechanical energy into the magnetic field
- Peak currents of MegaAmperes demonstrated in many experiments

FCG start current is provided by an external source:

- capacitor bank
- small FCG
- MHD device
- homopolar generator

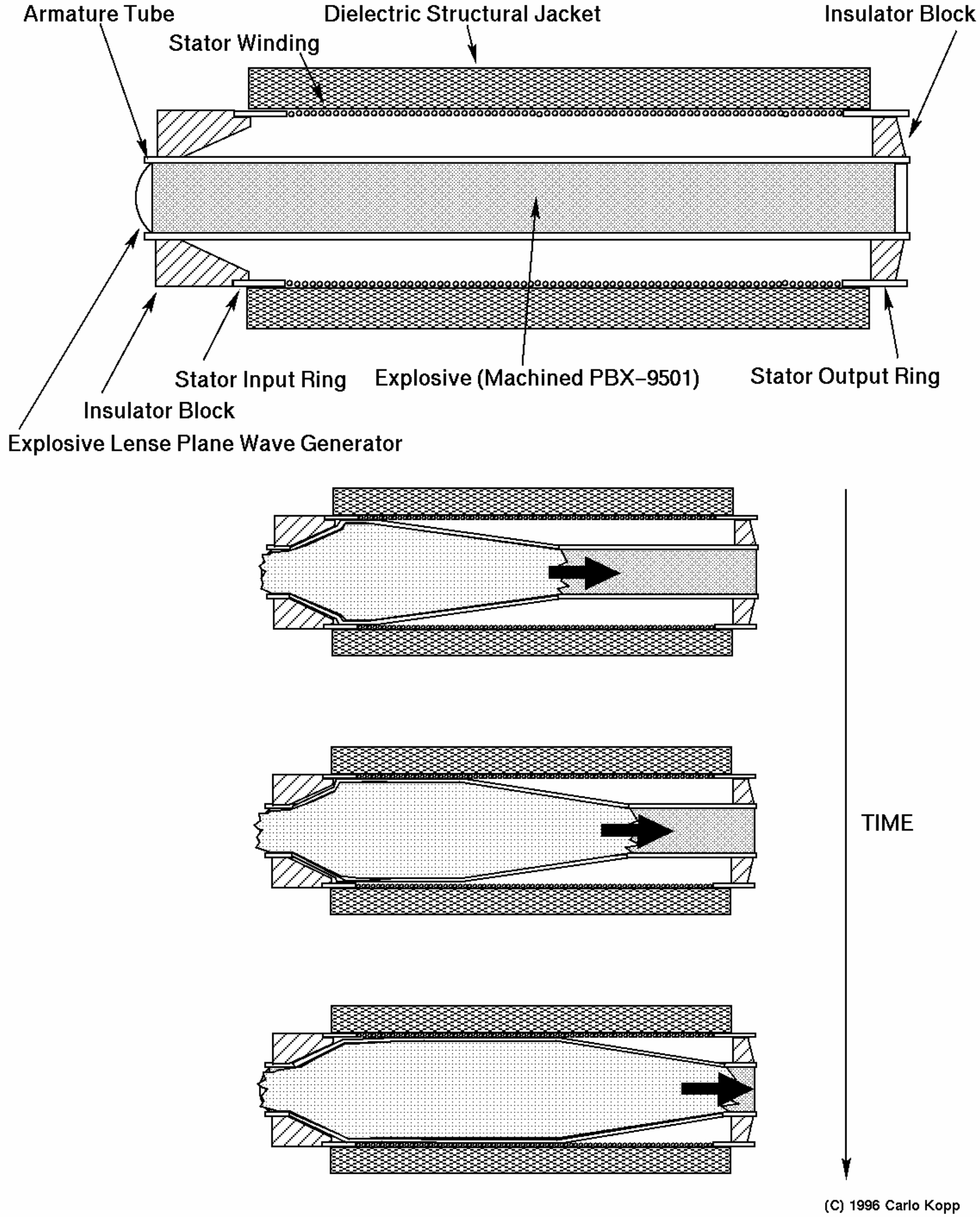

FIG.2 EXPLOSIVELY PUMPED COAXIAL FLUX COMPRESSION GENERATOR

FCG Internals:

- Armature - copper tube / fast explosive
- Stator - helical heavy wire coil
- Initiator - plane wave explosive lense
- Jacket - prevents disintegration due magnetic forces

FCG Operation:

- External power source pumps FCG winding with start current
- When start current peaks, explosive lense fired to initiate explosive burn
- Explosive pressure expands armature and creates moving short
- Moving armature compresses magnetic field

High Power Microwave (HPM) Sources:

Higher lethality than low frequency FCG fields, many device types:

- Relativistic Klystrons
- Magnetrons
- Slow Wave Devices
- Reflex Triodes
- Virtual Cathode Oscillators (vircators)
- Spark Gap Devices

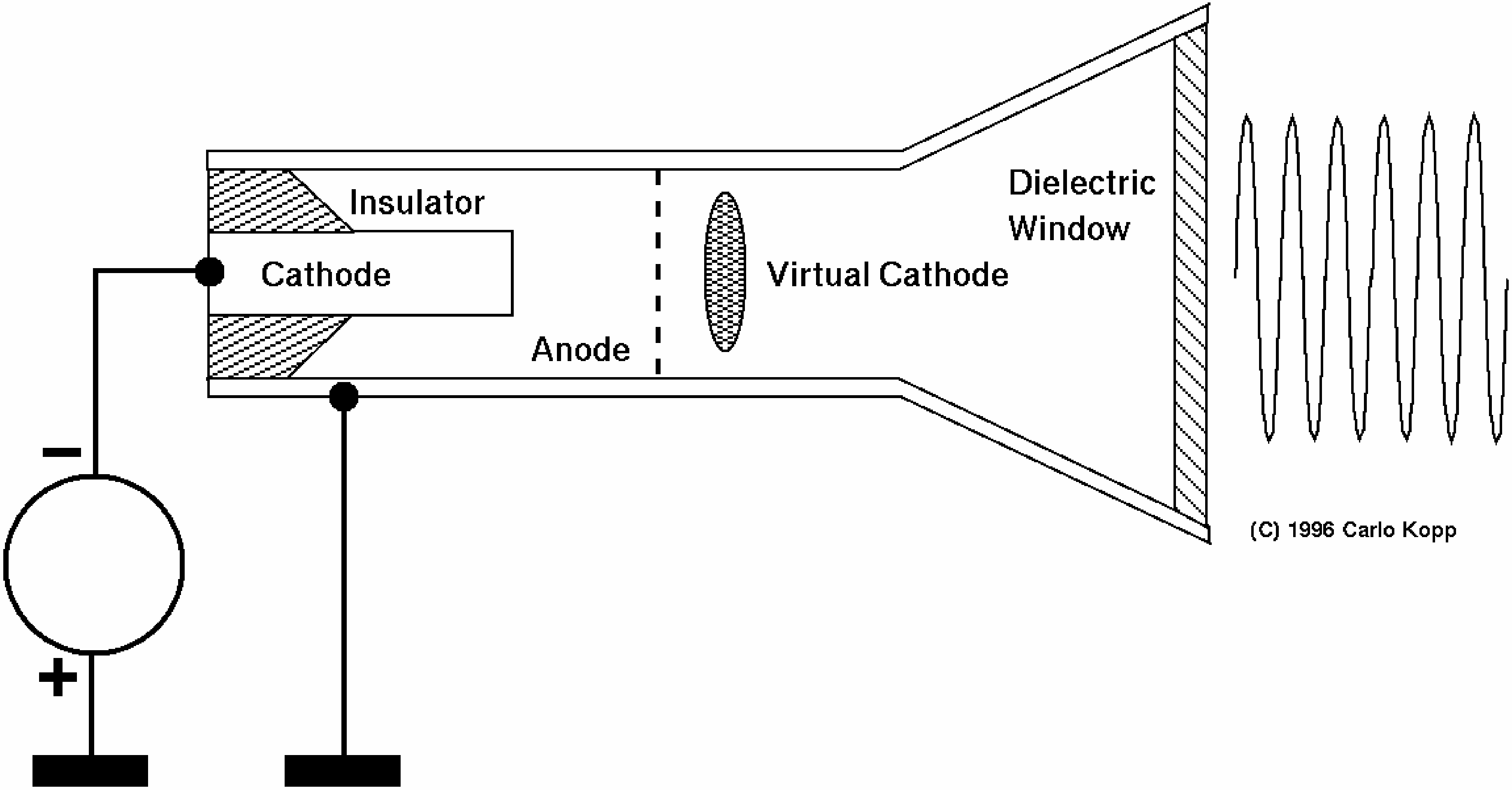

FIG.3 AXIAL VIRTUAL CATHODE OSCILLATOR

Vircator Physics:

- Relativistic electron beam punches through foil or mesh anode
- ”Virtual” cathode formed by space charge bubble behind anode
- Peak power of up to tens of GW for 100s of nanoseconds
- Anode typically melts in about 1 usec
- Cheap and simple to manufacture
- Wide bandwidth allows chirping of oscillation

Lethality Issues in E-bomb Warheads:

- Diversity of target set makes prediction of lethality difficult
- Different implementations of like equipment have differing hardness
- Coupling efficiency is critical to lethality

Coupling Modes:

Front Door Coupling through antennae.

- Destroys RF semiconductor devices in transmitters and receivers

Back Door Coupling through power/data cabling, telephone wiring

- Destroys exposed semiconductor devices
- Punches through isolation transformers.

Host Level Susceptibility

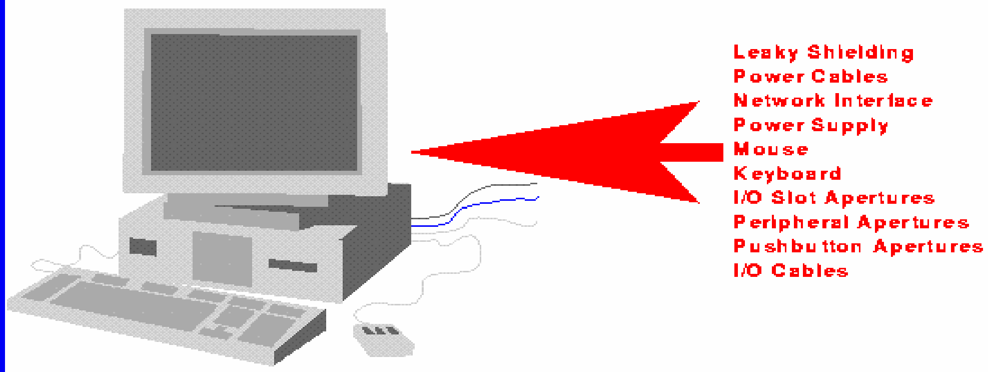

Fig.2 Host Level Susceptibility

System Level Susceptibility

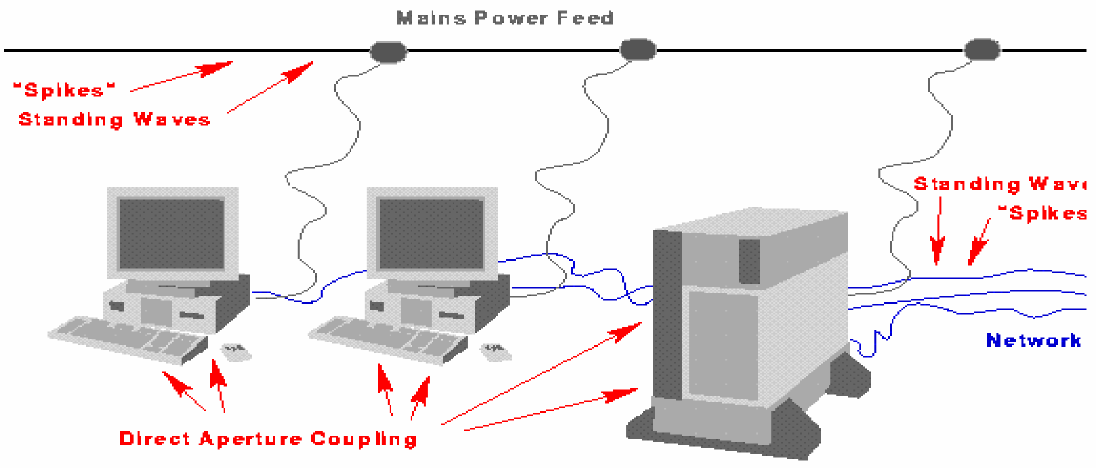

Fig 1 System Level Susceptibility

Semiconductor Vulnerability:

- Semiconductor components using CMOS, RF Bipolar, RF GaAs, NMOS DRAM processes are destroyed by exposure to volts to tens of volts of electrical voltage
- High speed - high density semiconductors are highly vulnerable due small junction sizes and low breakdown voltages

Damage Mechanisms:

- Low frequency pulses produced by FCG create high voltage spikes on fixed wiring infrastructure
- Microwave radiation from HPM devices creates high voltage standing waves on fixed wiring infrastructure
- Microwave radiation from HPM devices can couple directly through ventilation grilles, gaps between panels, poor interface shielding - producing a spatial standing wave inside the equipment cavity

Example Scenario:

- 10 GigaWatt 5 GHz HPM E-bomb initiated at several hundred metres altitude
- Footprint has diameter of 400 - 500 metres with field strengths of kiloVolts/metre

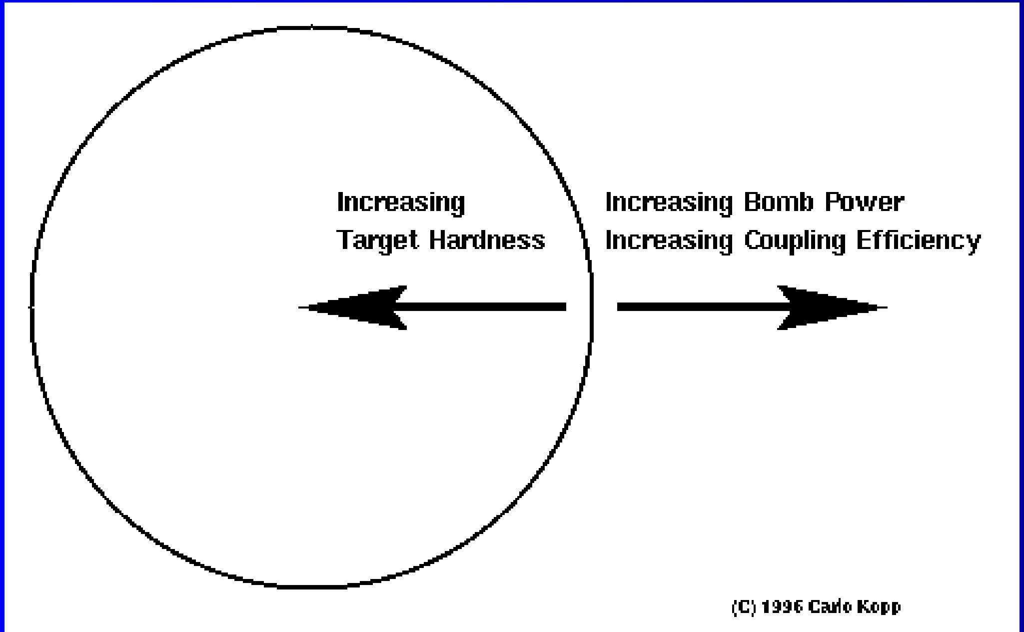

FIG.5.1 E–BOMB LETHAL RADIUS

HPM E-bomb Lethality:

Microwave bombs are potentially more lethal due better coupling and more focussed effects

- chirping allows weapon to couple into any in-band resonances
- circular polarisation of antenna allows coupling with any aperture orientation
- reducing detonation altitude increases field strength at the expense of footprint size

Defences Against E-bombs:

- Destroy the delivery vehicle or launch platform
- Electromagnetically harden important assets
- Hide important assets

Vulnerability Reduction (Hardening):

- convert computer rooms in to Faraday cages
- use optical fibres for data
- isolate power feeds with transient arrestors
- use non-electrical power feed schemes
- use electromagnetic “air lock”
- shielding must be comprehensive

I/O and Power Interface Hardening

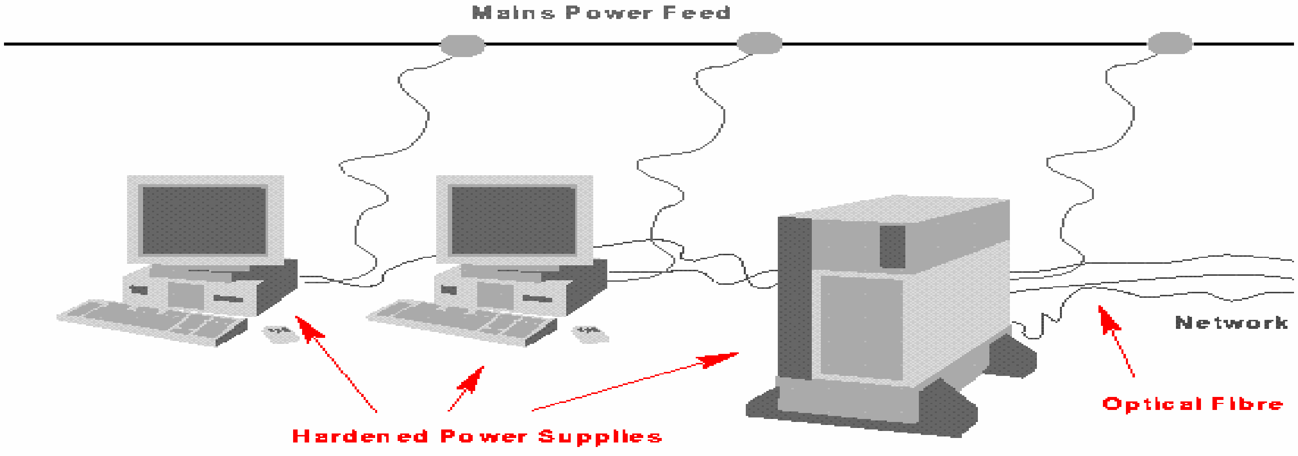

Fig 3.1 I/O and Power Interface Hardening

Comprehensive Host Hardening

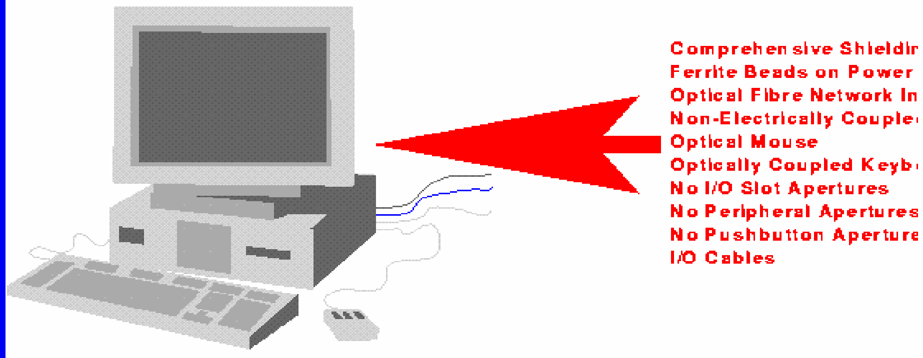

Fig 3.2 Comprehensive Host Hardening

Computer Room Hardening

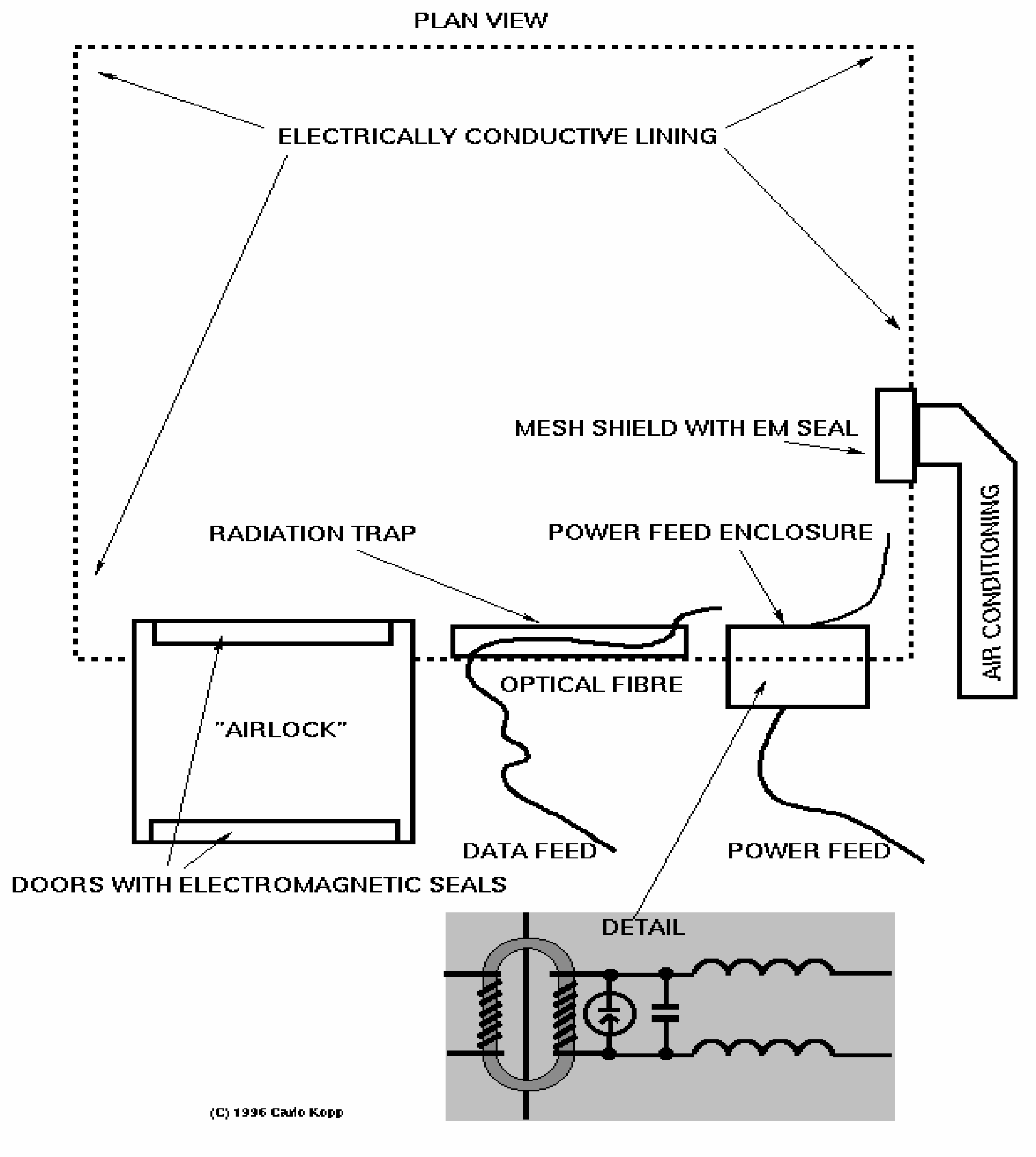

FIG.11 COMPUTER ROOM HARDENED AGAINST EM ATTACK

E-bomb Advantages

- Not lethal to humans
- Negligible collateral damage
- High tempo campaigns possible due the powerful “shock” effect of using a weapon of electomagnetic mass destruction
- No mass media coverage of bombing casualties (broadcast equipment destroyed) will reduce the threshold for the use of stronger measures

Punitive Missions

- The E-bomb is a useful punitive weapon as it can cause much economic and military damage with no loss of civilian life
- E-bombs could be profitably used against countries which sponsor terrorism and info-terrorism

Conclusions

- Hackers will soon realize that hardware is more susceptible at present than is software
- E-bombs are a non-lethal weapon
- The critical issues for the next decade are the hardening of fundamental infrastructure
- The cost of attack is very low
- Defensive measures need not be expensive if included in initial system design
- It is essential to consider electromagnetic attack as well as the usual hackers