



DYNAMIC POSITIONING CONFERENCE
November 15-16, 2005

Control Systems I

The PC: Practical Control or Potential Chaos ?

Russell Hodge

C-MAR America (Houston)

Table of Contents

1	Introduction	2
1.1	Development of the PC: A History	2
1.1.1	The IBM Concept	3
1.1.2	The Fight for Market Dominance	3
1.2	PC History and Development: Conclusions	3
2	Technological Change	4
2.1	Moore's Law	4
2.2	Legislative Obsolescence	5
2.3	Technological Change: Conclusions	5
3	Viruses	6
3.1	Black Thursday -1988	6
3.2	Virus Forms	6
3.3	A Brief History of Virus Development	7
3.4	Viruses: Conclusions	7
4	Removable Media	8
4.1	Floppy Disks	8
4.2	The IOMEGA Family	8
4.3	CD and DVD	8
4.4	Flash Memory	8
4.5	The Peripatetic Problem	8
4.6	Removable Media: Conclusions	9
5	Ethernet	10
5.1	Ethernet Basics	10
5.2	Ethernet Errors	10
5.3	Erroneous Broadcast Frame Types	11
5.4	Familiarity	11
5.5	Ethernet: Conclusions	12
6	Distributed Networks	13
6.1	A typical Distributed DP System	13
6.2	Maintenance Mode	14
6.3	Operating Platforms and System Vulnerability	15
6.4	Distributed Systems: Conclusions	15
7	Summary	16
8	Sources	17

1 Introduction

The intent of this paper is to consider the ways in which the PC has affected the development of DP and related system architectures. It will examine some potential hazards which may arise from its use and how technological development may change our expectations for capital equipment in the future.

All modern DP systems employ a PC in some form or other. It may form the computing core of the system or only act as the Man Machine Interface (MMI), nonetheless it is present. Where the PC is the core of the control system potential inherent weaknesses could be critical to operation. In a system where the PC only acts as the human interface any PC fault would not be expected to effect DP position keeping. It shall be demonstrated that this may not necessarily be the case.

Aside from the immediate effects of PC failure there are other influences which could affect long term operability of a DP or a vessel management system. Some of these are technical in nature and have been the subject of speculation for some time. It shall be demonstrated that such speculation is already beginning to be confirmed. Other factors affecting long-term viability are less obvious; these too will be touched upon.

1.1 Development of the PC: A History

From the development of Colossus, the world's first truly digital programmable computer, at Bletchley Park in WWII to decode the German ENIGMA and LORENZ ciphers, through to the 1960's computers were large, delicate and expensive machines which could only be afforded by large corporations or government agencies. These machines were generally programmed to suit the individual needs of the buyers and hence, outside the high level programming languages such as FORTRAN, COBOL and PASCAL, no common operating system platform existed. Paper and magnetic tape were the predominant forms of programme storage, but the machines generally required some degree of manual programming in order to start the operator system loading process.

Following the introduction of the first operational amplifier in 1959 silicon etching technology increased at a rapid rate, gradually reducing the size required to house the basic unit. Honeywell introduced the first home microcomputer, the H316 Kitchen Computer, complete with maximum 32K memory and 1200 Baud serial port in 1969. It was advertised in the Neiman Marcus catalogue for \$10600. No one knows how many were actually sold.

During this period Frederico Fagin designed the first microprocessor, the Intel 4004, and developed the bootstrap loader which permitted a computer to start loading its operating system automatically from power on. These two developments opened the door to the low cost computer. The MITS Sclebi was introduced in 1974 and the Apple in 1976. Both these units were supplied in kit form and required assembly by the user.

In 1978 Dan Bricklin introduced Visicalc, the world's first automated spreadsheet. It may be argued that this programme alone sparked the PC revolution by bringing to the desktops of financial planners the ability to simply perform multiple predictive analyses which had hitherto required a considerable amount of repetitive work and large computing power. The introduction of the early versions of database and word processor programmes which, together with the spreadsheet, today comprise the standard office suite began to appear during this era.

The success of these programmes, particularly Visicalc, not only assured the eventual ubiquity of the PC as a desktop tool but also presented an obvious challenge to the large computer manufacturers. Unable to ignore the challenge IBM announced their entry in to the PC market in 1980.

The IBM PC was finally launched in 1981, it was based on the Intel 8086 microprocessor, contained 16k byte of memory, was equipped with one, or two, 160k byte 5-1/2 inch floppy drives and had an entry level price tag of \$1565.

1.1.1 The IBM Concept

The IBM PC contained two unique features, one was the design of the 8086 microprocessor itself and the other was the use of standard parts. The 8086 had a 16 bit addressing architecture and internal segment registers enabling it to 'page' address memory greater than 32k. Programming with this structure is extremely difficult and had it not been for the success of the IBM PC, based primarily on corporate brand recognition rather than technical design, the concept would have died an early death and quickly succeeded by units based on a directly addressed 32 bit memory architecture, such as the Motorola 68000 series microchip.

IBM also realised that fast-tracking the project was the key to obtaining market share and took the decision to use existing parts, a concept which was called 'open architecture', this decision which was eventually to prove fatal to them.

1.1.2 The Fight for Market Dominance

The IBM PC quickly began to grab market share from the other machines on the market. As its market share increased its competitors either died out, found a particular small market niche or copied the IBM structure. Copying the architecture eventually resulted in its becoming the de facto standard for PC development. In addition it helped to drive down market price and for competitors to encroach upon IBM's share of the market.

In the mid 1980's the first examples of the PC as a control device began to appear. The simplicity of the BASIC language, and later C derivatives, coupled with the RS232 serial communications port made it ideal for coupling to small, custom built, I/O modules. This utility eventually led to the use of the PC as a core device in distributed network systems.

The decision to use standard parts meant that other companies could construct and sell computers which operated on the same platform as the IBM PC, non IBM PCs were collectively known as clones.. The popularity of the PC and the clones meant that the price of the component parts began to fall. The competition in the marketplace eventually rose to such a level that in December of 2004 IBM announced the sale of their PC manufacturing division to the Chinese Lenovo Corporation, effectively ending their participation in the PC market.

1.2 PC History and Development: Conclusions

It can be seen from the mini-history that the PC has not developed into its present form not due to its technological superiority but from commercial pressures. Standard operating platforms make the development of software for a variety of applications commercially viable. In industrial applications the PC may be viewed as a cost effective solution to implementing control algorithms and networks. The question to be asked is what are the risks?

2 Technological Change

2.1 Moore's Law

In 1965 Gordon Moore wrote an article for the 35th anniversary edition of Electronics Magazine which has had enduring impact on the electronics industry. The observations made by Moore in the article have metamorphosed over time to be called Moore's law. Currently the 'law' is understood to state that the number of transistors which can be manufactured on a single die will double every eighteen months.

Empirical evidence suggests that while Moore's Law is not exact the data handling capability of microprocessors and associated cost is increasing on a curve approaching an exponential.

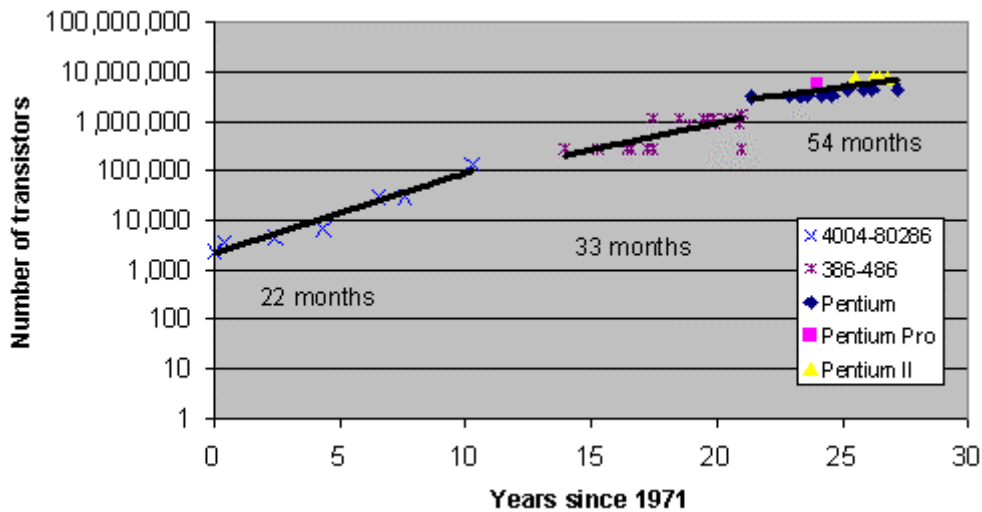


Figure 1 Growth of transistors on Intel Microprocessors – Grimm 1998

The obvious effect of this growth is a state of continuous obsolescence. Production runs of microprocessor based equipment, particularly those built on the Intel X86 engine, can be expected to last no more than two years. Industrial computer hardware may be expected to enjoy a longer life, but this is not necessarily the case with all equipment. In the shipping and offshore industries capital investment is expected result in a product with an operational life span of at least ten years without major equipment replacement. Commercial pressure almost invariably seeks the most cost efficient design solution and this has logically resulted in increasing use of PC based equipment in systems implementation.

The average construction time of a platform supply vessel from inception to entering operational service is fifteen months; a drilling vessel can be three years in the construction phase alone. Taking into account that a PC based control system cannot commence until the PC OEM has released the equipment to the market, that the unit has to be selected for DP system inclusion, and that any software changes required to make operation satisfactory on the new platform must be identified, implemented and tested before the upgraded DP system can be installed, it is not therefore beyond the bounds of possibility that the unit hardware is obsolete before the vessel enters operation.

This scenario applies not only to the Dynamic Positioning aspects of the vessel design, but also to any other electronic control system installed on the vessel.

2.2 Legislative Obsolescence

Electronic equipment contains a number of elements which have recently been recognised as toxic and having varying degrees of impact on the environment particularly at the time of disposal following the end of their useful life. This recognition has led to the introduction of legislation, notably in the EU, regulating the use of these elements, thus introducing a hitherto unseen development limiting the lifespan of electronic equipment; legislative obsolescence.

European Union Directive 2002/95/EC sets limitations on the amount of lead, mercury, cadmium, hexavalent chromium, polybrominated biphenyls (PBB) and polybromated diphenyl ethers (PBDE) which may be used in electronic equipment. The directive will be legally adopted by all EU member countries by July 2006. The adoption of the directive has already resulted in the withdrawal of at least one industrial PC used in a DP system,

2.3 Technological Change: Conclusions

Technological and legislative obsolescence can and have contributed to the premature demise of otherwise viable equipment. In an industry used to expecting functional operation and serviceability for periods of ten to fifteen years, budgetary arrangements will now have to take into account the possibility of complete system replacement in periods of a little as five years from commissioning. Accurate assessment of future serviceability requires increased communication of upgrade and spare part stock availability between vendor and operator. These conclusions do not only apply to PC systems but to almost any microprocessor based equipment.

3 Viruses

3.1 Black Thursday -1988

On November 3 1988 the Internet, barely out of its infancy, was attacked by a rogue programme of the type commonly referred to today as a worm.

The worm appears to have been released about six o'clock Pacific standard time in the MIT Artificial Intelligence laboratory. By eleven o'clock major computing centres were either under attack or off line. Sites infected included the Rand Corporation machine in Santa Monica, NASA Ames, Berkeley, University of Maryland Harvard, San Diego, Lawrence Livermore and Stanford. The fledgling Internet had collapsed and was to remain virtually unusable for two days.

The event occupied a few lines of newsprint and about ten seconds on the evening news. Should an attack of similar magnitude take place today business would come to a standstill. Wall St. could cease trading and national leaders would appeal for calm.

The worm was devised by a twenty three-year-old college student by the name of Robert T. Morris, after whom the worm was eventually named. It caused the crash of some 6000 machines at an estimated cost of 96 million dollars. For his crime Robert Morris was sentenced to 400 hours of community service, three years of probation and a fine of \$10,400.

There are two particularly interesting technological factors in the Black Thursday incident:

1. It raised attention to the possibility of large-scale Internet breakdown from malevolent sources
2. It was targeted at one specific communications protocol despite the many that were available at the time. The protocol was TCP/IP, the very same protocol upon which we rely today for electronic communication.

3.2 Virus Forms

Viruses come in two basic versions: worms and trojans. Worms are designed to make use of security holes in systems in order to propagate. Typically they will send and establish a small programme, often called a 'hook' into the target system. Then it will call the main programme to complete the infestation. Trojans, named for the Trojan Horse Of Hellenic myth, are usually disguised as genuine programmes, perhaps a game or an operating system upgrade.

Either variant described above may contain a 'logic bomb' which is a malicious programme designed to trigger from the system clock, the number of times a particular programme is run, or even a particular set of keystrokes.

Viruses may be designed to perform a variety of functions ranging from relatively benign to extremely destructive. In their most invasive forms viruses may destroy hard disk data, wipe BIOS programmes or call in spyware which may report the contents of the computer back to the originator or even permit remote access. There are variants responsible for spam generation or mass email transmissions to a dedicated target resulting in its effective collapse. This latter is known as a denial of service attack.

The following brief history shows that most virus generation concepts had evolved into maturity by the end of the 1990's. Most modern variants may be considered variations on these basic forms.

3.3 A Brief History of Virus Development

Although generally believed to be a fairly modern phenomena in computing history viruses have been in existence for longer than most people believe. In the 1960's and 70's there were programmes known as rabbits, which acted very much in the same way as worms do today. Elk Cloner, an early boot virus, existed for the Apple in 1981. As computers became popular the first Trojan Horses began appearing on computer bulletin boards. The first boot virus for the IBM PC, Brain, was developed in 1986 in Pakistan by the brothers Basit and Amjajad Farooq Alvi, who made the minor error of leaving their name and address in the body of the virus code. Despite a number of other outbreaks, and the discovery of self-replicating viruses, over the next two years in 1988 Peter Norton declared the existence of computer viruses to be chimeric. Robert Morris' worm struck down the Internet a few months later.

1992 saw the introduction of the first polymorphic virus generator. 1995 saw Microsoft accidentally release a virus in the beta version of Windows 95 and, Concept, the first macro virus for Word, Excel macro viruses were soon to follow. The following year saw a new generation of viruses targeted at Windows 95 and NT, these used a variety of methods including memory resident drivers and macros. 1997 saw the first Linux virus. Linux Bliss, and the first network worms, Homer, using FTP to propagate and Windows Internet Relay Chat worms.

1998 saw an explosion in new forms and witnessed the birth of the first polymorphics designed to attack Windows based systems, Win95-HPS and Marburg, BackOrifice which permitted the hacker remote management of the infected computer and closed with VBScript.Rabbit which could infect HTML files.

3.4 Viruses: Conclusions

Two immediate conclusions may be drawn from the history outlined above. Primarily that no operating system developed to date appears to be immune to viral infection. Secondly, from the fact that the majority of viruses have been directed at Microsoft products, in particular the MS DOS, Windows and Office product streams, a high profile system is more likely to have a virus targeted at it. Much of this latter may have to do with the psychology of the virus writers.

4 Removable Media

4.1 Floppy Disks

The first practically portable removable media was the eight-inch floppy disk developed by IBM in the 1960's. PC's shipped up to 1987 came with the improved 5-1/4 inch disk which was superseded by the more rigid 3.5 inch disk. The maximum capacity of the 3.5-inch device was 1.4Mbyte, a capacity small by current standards and is likely to be seen to disappear within the next few years yet it still maintains a degree of popularity for removable storage.

4.2 The IOMEGA Family

Iomega Corp have produced a series of successful and popular high speed access removable storage devices from the 10Mbyte Bernoulli box of the 1980s, the ZIP and Jaz drives of the mid '90s to the 35Mbyte REV drive. These devices can be configured to run through USB, ATAPI, and SCSI ports. However the increasing popularity of CD and DVD R/W disks and Flash Memory may well limit the use of the Iomega product range.

4.3 CD and DVD

Compact Disk technology first appeared in 1983 but it was not until 1988 that CD-R (Recordable) equipment became available and remained too expensive a technology to be commonly used in the PC environment for some years. Once the unit price for this technology dropped it rapidly began to dominate the market for portable mass storage media.

Further improvements in technology have resulted in the development of the DVD for re-writeable data storage. The standard CD storage capacity is 650Mbyte compared with the DVD's 4.7Mbyte.

4.4 Flash Memory

The flash memory concept was first introduced in 1988 by Intel, being non-volatile it is frequently used to store the PC BIOS, although it is most familiar to PC users as a removable media device. Removable versions may use the PCMCIA slot or the now ubiquitous USB port and may use various formatting techniques such as Smart-Media, MMC, and Memory Stick, the latter gradually becoming synonymous with USB flash memories. The rapid decline in memory cost is driving this technology to become the preferred medium for portable storage or passing data from machine to machine in a non-networked environment.

4.5 The Peripatetic Problem

The size and ease of portability of re-writeable mass media such as the Floppy Disk, CD and Flash Memory combined with a degree of ubiquity in the PC world has both advantages and disadvantages. The advantages are immediately apparent, a common operating platform and a convenient means of storing back-up or archival material. These very advantages may also be seen as disadvantages. The 'brain' virus and the host of copycats which followed propagated through that very portability, there was no Internet for PC's in 1986.

A floppy disk or CD-R/W can become infected on a home PC. That infection can be transferred to a new host seven thousand miles away.

4.6 Removable Media: Conclusions

Portable media devices may be expected to continue to be used as means of storing or transporting data between PC's. Security of transportable media and the use of up to date anti-virus software is vital to prevent potential infection and failure of PC based machines.

5 Ethernet

5.1 Ethernet Basics

First conceived in the 1960s at the University of Hawaii as a packet radio network, Ethernet was implemented as a network cabling scheme at the Xerox Palo Alto Research Centre in 1972. Following a number of modifications and improvements, it became IEEE 802.3 standard in 1990.

Ethernet is a bus or star bus based technology which makes use of a protocol known as Carrier Sense Multiple Access with Collision Detection (CSMA/CD) to control bus traffic. Equipment connected to the bus can be a combination of listeners and talkers, it is common for all equipment to have the capacity for reception and transmission of data on the bus.

In essence CSMA/CD operates by each device listening to bus activity. Should a device require to transmit data on the bus it will attempt to do so when it detects the absence of data traffic. In the event that another device attempts to transmit simultaneously an error will be generated and the device will wait a random period of time before attempting to retransmit. To some degree the network requires collisions to occur in order to regulate the network, however excessive collisions can slow down or cause the network to cease functioning entirely.



Although a number of alternate industrial data transmission systems exist, for example Profibus, FIP, CAN Bus, DeviceNet, Echelon LON, and a variety of error detection systems are available based upon protocols such as BCH, Manchester and Reed-Solomon, the Ethernet protocol is fast becoming the control communication medium of choice. This is not because it is superior to the other methods available but, since it has proved triumphant in the battle for supremacy in the PC communications, it has the benefit of mass production and consequent commercial edge. It can be seen from the description of its operation that it can be neither hierarchical nor prioritising in nature. This can be a disadvantage in a critical real time operating scenario.

5.2 Ethernet Errors

A network storm takes place when any device on a network broadcasts data frames indiscriminately without reference to the CSMA/CD operating parameters.

There are three basic methods by which Ethernet transmissions can be disturbed:

- A) Physical damage to the transmission medium
- B) Failure in an active component, 'talker', on the network
- C) Excessive activity on the network.

Physical damage can be easily resolved by the adoption of redundant networks. This solution has been adopted by the industry. Any active device attached to a network, Network Interface Card (NIC), switch or router can fail such that it continuously broadcasts blank data packets. Excessive activity can be the result of too much data traffic or of a phenomenon known commonly as a `network storm`.

5.3 Erroneous Broadcast Frame Types

Although not intended to be comprehensive, the following short list outlines the basic types of false data packets, which can result in reduction of network speed and potential total failure:

1. Chernobyl Packet, results in network meltdown.
2. Christmas Tree Packet, a packet with all options enabled.
3. Kamikaze Packet, similar to the Chernobyl
4. Sourcerer's Apprentice, receipt of a message causes multiple messages to be sent.

The potential of network disturbance by blind packet transmission has been recognised for some time and a number of techniques have been developed to mitigate them. However it should be noted that the development of such techniques is a responsive reaction to the integral weakness of the protocol itself. The addition of processes designed to identify, isolate or prevent system error migration may be considered as `Band-Aid` solutions, which increase the complexity, and therefore the potential of failure, of the system under consideration.

Such solutions are not foolproof. During the preparation of this paper a furore arose over the presentation at the Black Hat convention of a paper dealing with major security flaws in routing software. It has been considered by some that these flaws could permit virus writers to generate new network killing applications. This controversy has had a major influence in the preparation of some sections of this paper and is considered to be of particular relevant to the secure operation of DP and vessel management systems.

5.4 Familiarity

The commercial drive for economic competitiveness has led to the standardisation of interfacing Ethernet based network systems in industrial and commercial use. The RJ45 connector and Ethernet hub are becoming so common as to be almost considered as household items. Connector cables can be bought pre-fabricated in office supply stores and supermarkets for a few dollars. A complete network kit, including cabling, hub or switch can be bought for less than fifty dollars.

The basic Ethernet addresses used in local area networks are so well known that many can recite them by heart or they can be found on the Internet with simple search criteria. These are the same addresses commonly used in DP and vessel management systems. In order to improve connectivity the latest operating systems are equipped with simple to use set-up procedures enabling individuals with limited computer experience to install a local area network within a matter of hours. The simplicity of connectivity, the ease of set-up and day to day encounters with PCs have led to a high degree of familiarity and confidence in their use and operation by users with limited computer knowledge. That confidence and familiarity has removed from the computer an essential quality ingrained into the operators and programmers of the pre-PC generation: fear.

5.5 Ethernet: Conclusions

The Ethernet Protocol is not primarily designed for real time process control applications. It has become widely used in these applications primarily due to commercial considerations. Failure modes, either physical in nature or software generated can lead to network failure. Familiarity and ease of communication set-up has resulted in excessive confidence in the use and lapses of security in network installations

6 Distributed Networks

6.1 A typical Distributed DP System

Figure 2 below is representative of a basic distributed DP network. It comprises redundant Operator Stations, redundant DP controllers, redundant network distribution and remote process control stations. The process stations may perform a variety of functions including thruster control, power monitoring and sensor interfacing. Conceptually the system is the same as any remote process control system with the exception of the DP controllers.

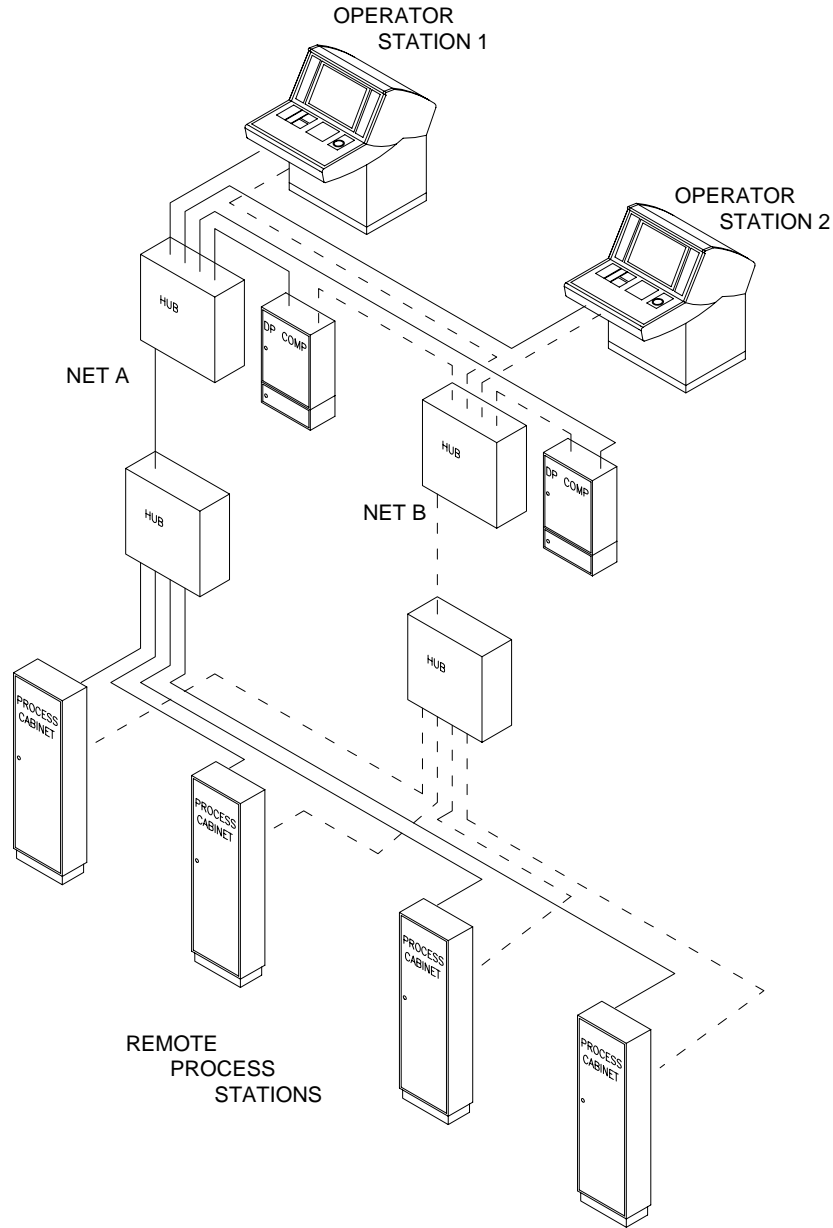


Figure 2 Typical Distributed DP Network

So long as the system has no means of connection to any other network then it is isolated from external influences and, theoretically, is safe from viral infection. However, this isolation is only assured so long as any portable media, Floppy Disk, CD etc has been fully verified to be virus free prior to installation in the network. Generally speaking most vendors go to some lengths to ensure portable media is free from infection. The system itself however, almost universally, does not come provided with anti-virus protection to prevent the installation of accidentally contaminated media.

6.2 Maintenance Mode

Maintenance of system software is often performed by the installation of an additional computer, in rare instances a permanently installed PC, though more usually a laptop device. Figure 3 below illustrates this principle.

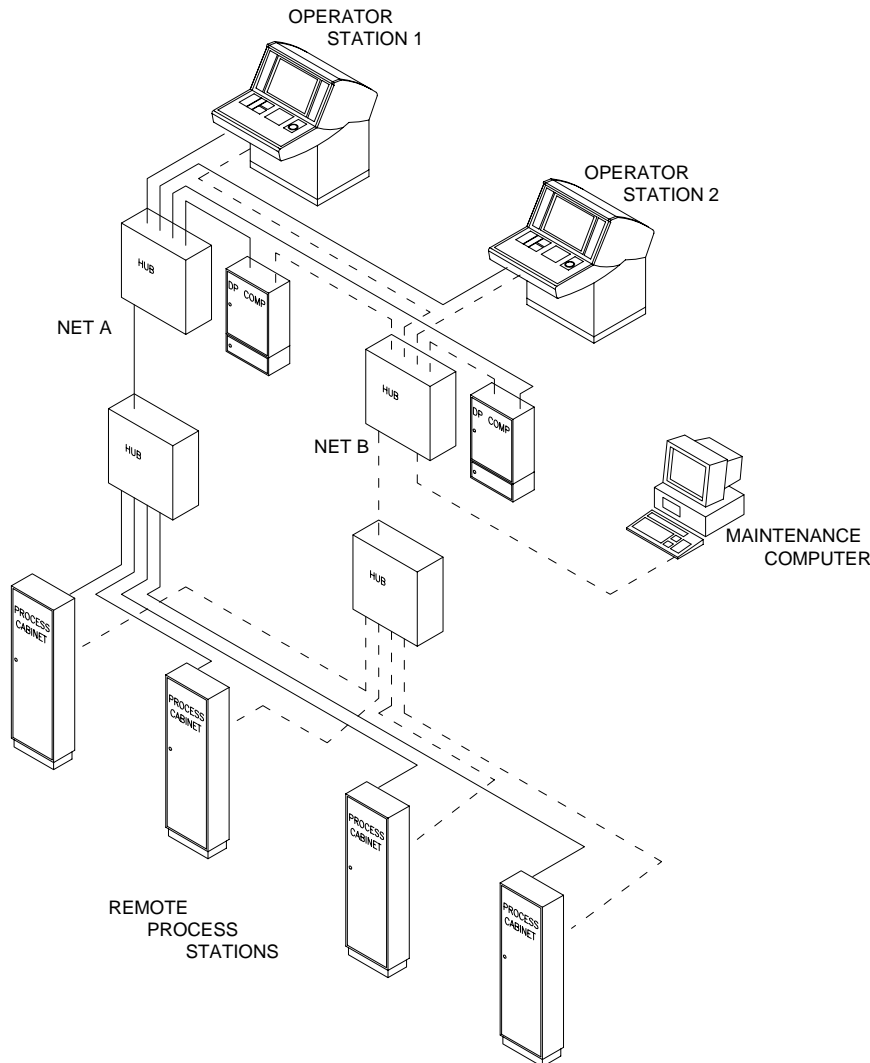


Figure 3 Distributed Network with Maintenance Computer

As with the initial example, it can be seen that so long as the network and the maintenance computer are isolated and verified virus free the network is free from viral contamination.

6.3 Operating Platforms and System Vulnerability

Although the general topography of distributed systems is not subject to extensive variation, the same does not apply when considering hardware or software implementation of the control equipment. For example the main DP computer may be DOS or Windows based in one arrangement where another may utilise an alternate real time operating system, such as VX Works.

Where a non-DOS or Windows based operating system is employed, the DP computers may be expected continue to function following a virus attack but any DOS or Windows based unit would be infected with the risk of potential failure. Such a set of circumstances might result in the DP system continuing to function normally but the operator station controllers becoming inactive with loss of display and operator function. However, if the infection were designed to generate blind packet transmission the entire network would be at risk.

Where any system, either DP or integrated management, is fully based on a DOS or Windows platform the risk is that all equipment connected to the network would fail with the consequent loss of all remote control functions. The consequences of such a failure would be severe.

Recent trends are for the remote maintenance of vessel management and dynamic positioning systems through Internet portals. The advisability of ensuring adequate security in this event should be treated with considerable seriousness.

6.4 Distributed Systems: Conclusions

When operated in isolation, distributed systems employing PC based market prominent software in any part of the network are unlikely to be at risk to the results of exposure to potential virus contamination. In such cases, however, measures should be taken to ensure that all portable media or maintenance equipment which is likely to be connected to any part of the control system are free from viral infection. Where a control system employing PC based market prominent software is likely to be connected to an Internet portal for any reason, operators and vendors should ensure that all means available are taken to secure all equipment involved in the operation from the risk of viral infection.

7 Summary

The PC has become the MMI, and in some cases the core computer, of all modern Dynamic Positioning Systems. It has achieved this status not through technical superiority but due to its ubiquity in the commercial marketplace.

Of the various influences which the PC will have on dynamic positioning and process control the most prominent will be that of technological advance. The speed of technological advance will increase the rate of both software and hardware redundancy. The use of PC equipment will result in increased maintenance costs through the necessity to maintain higher levels of spare parts on board vessels to supply the need for line unit replacement where continuity of operation at sea is of prime importance. Strategic planners must now take into account the possibility that essential equipment obsolescence may result in high level upgrade, if not total system replacement, at a considerably higher frequency than would have been considered as little as ten years ago.

The effect of legislative action remains unpredictable since this is largely driven by political moment. However, unforeseen legislation may render equipment obsolete in a short timeframe.

Commercial pressure is leading towards the adoption of standards which potentially expose dynamic positioning and vessel management systems to the same risks as domestic equipment. The use of these standards and operating platforms has led users to a degree of familiarity and confidence without raising the awareness of risk. The probability of viral infection, while generally accepted as being low carries with it the greatest threat to the safe operation of DP and VMS systems. This vulnerability and the probability of catastrophic failure may be mitigated by the implementation of industry specific, low market profile, operating platforms, the use of 'locked' or non-standard portable media and communication protocols.

8 Sources

The following list details the main sources used in the compilation of this paper. Numerous other web, based sources were also consulted which are not credited

A Tour of the Worm	D. Seely, University of Utah
Black Hat Day 1: A Cover Up ?	Washington Post 27 July 2005
Cyberpunk	Hafner and Markoff, 1991
Network Storm Knocks out NY Stock Exchange	Computer Weekly June 3 2005
Software – Then, Now and the Future	D. Godfrey
The Hacker's Handbook	Hugo Cornwall, 1985
The Lives and Death of Moore's Law	Ilka Tuomi
The Logic of Failure	Dietrich Dorner, 1997
The Ubiquitous Reed-Solomon Codes	B. Cipra, SIAM News 1993
Threat Assessment of Malicious Code and Human Threats	Bassham and Polk, National Institute of Standards and Technology, 1994