More Dependable Systems in Computing
-Autonomous Decentralized Systems-

Hirokazu Ihara

International University of Health and Welfare

2600-1 Kitakanemaru Ootawara Tochigi 324-0011 Japan

Email; ihara@iuhw.ac.jp and h-ihara@msn.com

Abstract

The advent of the computer control systems (COMTRAC) for Japanese bullet railways (Shinkansen) is traced as the example of real time life critical system for these 25 years. Then the new system concept (ADC; Autonomous Decentralization concept) which has been proposed by the author's group is briefly reviewed with social demands. The concept is widely applied to the recent real time computer systems for solving dependable system development in Japan. Eligible examples of Autonomous Decentralized Systems for railway are showed. From the history learnt, future technical directions are indicated for dependable computing for the life critical systems.

1 Introduction

In March of 1972 Japanes COMTRAC (COMputer aided TRAffic Control) system went into operation controlling the Shinkansen high speed bullet train. This was one of the earliest applications of computer control to life critical, real-time public mass transportation and earned COMTRAC a place in Japanese social infrastructure. In December of 1971 the first computer system to control a subway, or Mass Rapid Transit(MRT) running on rubber tires began commercial operation in Sapporo city, just one month before the Olympic Winter Games began there. The author was responsible for developing these systems.

Next month, in February of 1998 the Olympic Winter Games return to Japan, this time to the Nagano highlands area. In the span of these twenty-five years, as a result of inevitable social pull and technology push factors, we have seen evolutionary changes to the structure of real-time computer systems.

The concepts which enabled COMTRAC grew out of the author's earlier design efforts to realize real-time dependable control systems. From work in the development of various railway traffic control systems, the author acquired a fundamental understanding of basic dependability issues. My colleagues and I were partially able to satisfy dependability requirements using a decentralized system organization along with suitable autonomous management and control functions. This paradigm change, to an autonomous decentralization concept, will be compared to representative conventional system structures and several other examples.

2 History of Railway Traffic Control Systems in Japan

The early 1960s' saw the rapid introduction of transistorized digital computers to industry. Automation and systems engineering became key words in the drive to advance the technology base. This lead to many projects aimed at the rapid introduction of the digital computer to real-time control of industrial processes, such as iron and steel making, electricity generation and distribution, chemical processing, manufacturing, and so on. While great strides were made, the computer\'92s reliability was not sufficient for the most critical applications, those having direct impact on public safety. In 1968, at Hitachi's System Development Engineering Group, the author took charge of a project having this type of critical application. The project goal was to implement the first digital computer traffic control system for the Shinkansen. The project was, certainly, on the cutting edge of real-time, critical, reliable control technology at the time.

During that decade, from 1968 through 1978, The author was responsible for developing COMTRAC and installing it as the basis of the Shinkansen control network. Fig. 1 shows the Shinkansen network now in operation throughout Japan. The first leg realized was the Tokaido line between Tokyo and Shin-Osaka in 1972. The second leg to become operational, the Sanyo line in 1975, extended from Sin-Osaka to Hakata on Kyushu Island. In 1983 the Tohoku line was inaugurated from Tokyo to Morioka in the northern part of the main island. This line branched off at Takasaki toward Niigata in 1985. Subsequently, Shinkansen lines in northern Japan branched at Fukushima to Yamagata in 1992, at Morioka to Akita last year, and at Takasaki to Nagano also last year. Nagano, as mentioned earlier, is the site of the Olympic Winter Games to be held in February. The first COMTRAC implementation, for the Tokai line in 1972 and shown in Fig. 2, had a dual system redundant structure enabling it to run synchronous but otherwise independent programs in two separate computers. Both computers calculated critical route control information. Specially tailored hardware compared this information and, in the event of any disagreement, this comparator would cut off both outputs and activate check programs in the two computers. The results of these check programs were compared to patterns that had been previously stored in the comparator's read only memory. By this means, the healthy computer system was identified, selected, and its output was transmitted as the correct route control command. System operation continued in this single-thread mode at a degraded safety level while operator action was taken to restore dual-thread capability as quickly as possible. Fig. 3 shows the next COMTRAC system to be implemented. It was structured symmetrically with three computers to improve the safety level in the event of a single failure. Two computers operated as before and, after a failure event, a third computer was automatically connected to the surviving computer to restore dual-thread operation. Availability of safety critical route control information was restored within 2.5 seconds by this means, within the 3 second outage requirement imposed by the train systems. We refer to this system structure as dual-duplex. It achieved better than four 9s, that is, 99.99% availability for 24 hour operation with no unsafe command output during its operational lifetime. In addition to this route control command generator, this second generation system included two additional mainframe computers(PP) in a duplex configuration for schedule planning. As mentioned earlier, this same system structure was applied to the Tohoku line in 1983. Software for the control of certain station operations system wide, as well as a station controller for Joetsu lines, was added to the system two years later in 1985. Of course, new functions were included to accommodate the changing socio-economic demands placed on railway transportation in Japan.

The COMTRAC systems controlling the Tokaido and Sanyo lines were updated with new hardware in 1988, as shown in Fig. 4. The front-end computer(FEP), which is a single-thread computer used to communicate with other computer systems, as well as a dual-thread message transfer computer(MAP) for passenger , were separately added to the main processors(RCP) in the COMTRAC configuration. In all, these computers were connected to 53 operator consoles by a double loop reliable network. The entire Shinkansen control network has undergone far too many changes to address here. The important point, though, is that it retains as its central organizational principle the COMTRAC organization first implemented in 1972 with its centralization, fundamental program structure, its time sharing processing. As the Shinkansen bullet train system expanded, the COMTRAC organizational principles formed the basis of a new paradigm for massively large real-time computer control systems.

3 Autonomous Decentralization Concept

3.1 Background

It is a generally accepted principle that in order for the system to accomplish its objectives efficiently, its components must be integrated in an efficient structure. As a system grows as large as COMTRAC did, it is learned that the following points must be given due:

(1) If the system stops operating, it not only affects the business management of the enterprise concerned, it can also have a serious effect on society.

(2) Provisions for accommodating open-ended system evolution should be included in the system design from the start. A large system cannot be constructed in a short time and it is generally necessary for any system to be expanded to accommodate changing demands and to incorporate new technologies. Furthermore, these modifications may need to be made while the system is functioning. Accordingly, systems that contain provisions for such phased, online expansion are desirable.

(3) Provisions for system maintenance during operation must be provided. Especially for online systems, maintenance procedures cannot be permitted to require suspension of critical system operations or to impact system-related services.

Fig. 5 illustrates the paradigm shift towards a more decentralized and flexible approach. The centralized system structure, which was characterized by time sharing processes and fixed protocols optimized for efficiency, proved unacceptably inflexible and difficult to expand. The distributed structure, on the other hand, focused on first creating and standardizing interfaces between structural units, then standardizing protocols governing communication across those interfaces.

While approaching the desired degree of flexibility, this approach proved unsatisfactory with regard to ever more severe critical system dependability requirements encountered during increasingly high-speed online, real-time operation. By the end of the 1970s', the author and colleagues had proposed a new concept, which we call Autonomous Decentralization, to improve performance in this regime. It was inspired by analogies to living organisms. Autonomous decentralized organizations are characterized by loose interaction modes between autonomous subsystems, these subsystems being dedicated to satisfying limited sets of local objectives and being capable of relatively unbounded growth in order to accommodate increasingly severe system conditions.

3.2 Analogy Between Molecular Biology and Information Control

Please excuse me, but for you to understand the motivation for proceeding along this line of system development it will be necessary, at this point, to explain the view of cell growth that we held at the time. As we understood it, it had become known that fundamental mechanisms of biological processes, including morphogenesis and physical movement, could be viewed as being expressed by a sort of digital code embodied within the base sequence of deoxyribonucleic acid (DNA). Morphogenesis is the formation of the structure of an organism or part; differentiation and growth of tissues and organs during development .to be responsible for accomplishing the functions upon which cell behavior depends. The bodies of living organisms, of course, are formed by cell division with the DNA code surviving, to a great extent, and determining cellular functionality in succeeding generations. We understood that it was immuno-reaction mechanisms, which are reactions resulting from the recognition and binding of antigens by specific antibodies or by previously sensitized lymphocytes, again embodied in the DNA code within each cell, that determine how succeeding generations of cells are differentiated, identified, or inhibited. That is to say, we understood the production of antibodies to be ascribable to relevant DNA information. The author and colleagues understood this to be the fundamental mechanism, the mechanism centered on the information encoded in cellular DNA which ensures the growth of the individual organism and preserves the system. As described above, it seemed to us that molecular biologists had determined that the entire mechanism of morphogenesis and the preservation of organisms was due to information programmed into DNA. Many of the actions of DNA have not yet been clarified and some held the view that DNA was been programmed in advance, so to speak, to cope with unexpected changes in the environment. Two points were central to us in our efforts to develop our control technology: 1) First, that information was encoded in DNA, and 2) Second, that the individual organism could be viewed as a gene pool, a simpler conceptualization than we had been dealing with up to that time. Furthermore, we came to understand that information in living organisms is communicated throughout the body by the central nervous system as well as by various hormonal systems. With regard to the nervous system, we saw morphological and functional structure as organized units of neurons interconnected by intricate networks of synapses. In our view, information was transmitted via an analogue electrical network with the significance or meaning of data being proportional to electric pulse density. Thus, we saw neurons working as transmission controllers and synapses as transmission links. We viewed the hormonal system as a different type of communication system, one which could induce action in distant parts in response to information local to particular cells. We understood that hormones are produced by specific cells, are carried throughout the body by the blood stream, and are able to perform their functions by combining with specific receptors on target cells. It seemed to us that processes of regeneration through reproduction of genetic information in cells, resembles the operational cycles of computer programs. We compared the functionality of operating systems (OS) to biological phenomena and found parallels in the way information was treated, storage was controlled, various elements of information were deduced, input and output was handled, and the way in which features functioned to protect the system as a whole against external interference by removing or preventing intrusion.

It became apparent to us that the utility program, that particular part of the typical OS, could be compared to the instincts of living organisms. Programs, that is to say, application software developed to make microprocessors execute functions could be put into correspondence to the DNA programs in the cells of living organisms. Certain types of software modules are stored in unchanging Read-Only Memory (ROM) much as certain types of codes are stored as sequences in DNA. Random Access Memory (RAM), it seemed to us, corresponded to the more diffused and volatile storage locations within organisms wherein instinctive and non-genetic behavioral patterns are stored. Functions of survival and homeostasis in organisms corresponded, in our view, to the exception handling routines in processors, those routines responsible for reconfiguration, state control, and stability point seek functions, all necessary to correct system abnormalities. To us, program portability resembled the kind of preservation activity we saw in the behavior of genes in natural selection, that natural or artificial process that favors or induces survival and perpetuation of one kind of organism over others. This motivated us to require hardware to be flexible enough to support direct portability or replacement of software. We made it a fundamental principle to permit no hardware to impose more than an absolute minimum of well-characterized restrictions on software portability or replacement. This principle was absolute for us, because the OS program, as well as applications, were also replaced by degrees, as system specifications and requirements evolved. This evolution was similar, in our view, to the way organisms evolved in deference to dominant genes. To summarize our views concerning the correspondence between digital microprocessors and biological systems, the program, as embodied in DNA or code stored in semiconductor memory, is of vital importance. It is the hardware, which is to say, the organization of semiconductor or cell structure, that is temporary, like the gene pool, which supports the logical structure of the code.

3.3 Autonomous Decentralized System

The basic idea of the Autonomous Decentralization Concept (ADC) was induced from the analogy with biology. Living things are the integration of organs, which in turn are also the integration of cells.

We could consider that cells have uniformity of structure, equality of function and locality of information at the organ level. Each cell has the same programs embedded in their DNA chains. Each cell has its autonomy, which means cells can live and function by themselves, adapting to their environment. Organs or individuals are the integration of numerous cells, each with its autonomy and living in coordination with those around them. The system as a whole lives in a stable manner even though its metabolism is dynamic on a micro scale, growing, aging, and so on. Even though the system as a whole includes faulty subsystems, it is quite normal. In other words, the completely faultless system exists in but one of many permissible safe and fully functional states. This is our basic perception of system. Fig.6 shows the relation among centralized, distributed, and decentralized systems. The conventional, centralized system is shown here in the third quadrant and the distributed system is in the second and the fourth. All of the subsystems forming autonomous decentralized systems, placed in the first quadrant, upper right, have to satisfy autonomous controllability and autonomous coordinability as well as fault-tolerance and total system life cycle cost performance.

Autonomous controllability is defined as:

Even if any subsystem fails, the other subsystems can manage themselves.

Autonomous coordinability is defined as:

Even if any subsystem fails, the other subsystems can coordinate their individual objectives among themselves.

In order to realize these properties in technology, a means of asynchronous broadcast communication with function encoding and data field scheme was invented. The subsystem generates information, immediately broadcasts it with an assigned code which signals the content of the information to all of the other subsystems. Any particular subsystem processes the broadcast information according to its needs. There is not a special communication control process between a designated sender and receiver. The receiver takes the initiative in this communication process. Thus, the database, which we refer to as a data field, consists virtually of distributed data in the subsystems. The subsystems can access their capturing data in their private data field immediately when they need them if other subsystems are out of order.

4 Innovation of Railway Traffic Control Systems

ADC was first applied to railway computer control systems. Every station and every train had nearly identical functions. This allowed the system to be comprised of a homogeneous set of subsystems. This is why we succeeded in applying ADC initially to railways. Fig.7 shows the general concept applied to railway control systems. In the system as shown here, the center does not execute any real-time function. Rather, the center dispatches train diagrams and rearranges train dispatch schedules. Local station controllers play almost all of the leading parts in real-time control. Fig. 8 shows an early examples of traffic control systems for subway introduced in the 1980s'. It shows that the subsystems at the various stations have an equal status and that the system has no command or supervisory upper level. Construction was done incrementally and the system was expanded on a yearly schedule without difficulty. Since then, almost all of the subway control systems in Japan have included this ADC structure.

New COMTRAC systems were also proposed along with ADC. This idea was applied to COMTRAC for the integrated Tohoku line and Joetsu line in 1995 as COSMOS. This new COSMOS (COmputerized Safety, Maintenance and Operation System), a version of COMTRAC, is shown in Fig. 9 as implemented in the Shinkansen bullet train line as implemented in the line to Nagano.

Conventional railways are another target application of computerized traffic control. Fig. 10 shows the main railway lines of the Tokyo urban district. As operations are very complicated, they are quite difficult to modernize. ADC provided the solutions, implemented as ATOS (Autonomous decentralized Transport Operation control System. There are 19 lines, over 300 stations, and more than 1200 km of rail. The number of trains controlled counts 6500 each day. Last March the Chuo line, which consists of 134 km of track and 51 stations and shown here by the thick solid line between Tokyo and Kofu, was initially brought into operation after great effort and much trial and error over more than five years. The lines shown dotted were introduced under centralized programmed route control some ten years ago using simple traffic processes. In contrast, another 18 lines using ADC, shown by lines, are now under fabrication and will be brought into operation year by year. The ATOS system structure has a three tier ADC hierarchy, at the station level, the line level, and at the coordination level. Each level consists of homogeneous subsystems. Nobody knows how many computers will participate in ATOS. Interlocking systems of train safety are changed from mechanical relay logic to computers operating under a 2 out of 3 majority scheme.

A committee organized by Japan East Railway Co., charged with defining the 21 century railway system, proposed basing new systems on ADC. Each train has its intelligent autonomy for safety and broadcasts its operating conditions in real time to neighboring trains by communication satellites and wireless communication means. The train position, vital information for running safely is calculated with Global Positioning System. Consequently the density of traffic will be efficiently increased with safe space between trains before and behind instead of the present fixed safety section control. Trains in the 21 century will run autonomously, controlled by their onboard computers with Artificial intelligence, in contrast to the fixed, centralized control centers that exist nowadays.

5 Conclusion

The advent of railway computer control systems in Japan was discussed. It is now widely recognized in Japan that Autonomous Decentralized Concept, which we proposed about 20 years ago, is a significant and suitable advance in real-time critical computer control structures. From a distance, being that the author is no expert in communication networks, it appears that the Internet and the various forms of Intranets are examples of our ADC concepts to communication systems.

Several other examples are emerging which seem to be using principles quite similar to ADC. One is for automobiles, Integrated Traffic Control systems now under development in many countries.

Air Traffic Control is evolving to place autonomy onboard the airplane, a capability described in the August 97 IEEE Spectrum magazine. Communication satellite systems are yet another example. Satellite constellations now under development will incorporate autonomous communication switching and orbit control principles, systems such as Iridium with 66 satellites and Globalstar with 48. The Mars Pathfinder interplanetary spacecraft successfully functioned on the surface of Mars this summer, due to a large extent to its use of autonomous principles. It is easy to imagine that several rovers might be sent for more complicated missions in the future. Rovers that work in cooperation will most likely be provided with autonomous controllability and autonomous coordinability because of the time delay in communications between the earth and other planets.

When systems will consist of large numbers of autonomous subsystems which are discussed here, onboard computer systems are much more important from dependable point of view. Mobility of computer needs light weight, small volume and low power dissipation as well as high performance. In addition, system level dependability is a must. So, investigation of chip level redundancy is one of the important research and development target for more dependable computing.

System validation prior to building a system by gathering COTS(commercially available off the shelf) products and maintenance after its inauguration became more important. Security against malicious attacks and invaders to the life critical systems which spread spatially may be one of the most vital items of system dependability. Security should be guaranteed in as low subsystem level as possible, for example, chip level.

Legacy of systems is also a threat to system construction. Technical knowledge, information or industrial structures are rapidly changing and varnishing according to ever-progressing of computing technologies. And replacement of a total system is almost impossible in some limited duration.

Author convinces that solutions on the above problems will be found in biological activities. Though the author has traced the advent of computer system control structures for critical applications by showing railway traffic control systems in this paper, Autonomous Distributed Systems have been applied to many other computer control applications by Hitachi over these past 15 years. I am greatly proud that a large research group, consisting of 141 professors and researchers from various technology, sociology, and scientific backgrounds, in universities as well as in research institutes have been supported by the Japanese Ministry of Education, five year research project on autonomous decentralization systems from 1990 through 1994. Their keen and deep research results are highly valuable for further investigation of system structures.

Acknowledge

My great gratitude goes to Prof. Sy-Yen Kuo of National Taiwan University and Prof. Yoshihiro Tohma of Tokyo Denki University for giving me the opportunity of the key note speech at 1997 Pacific Rim International Symposium on Fault Tolerant Systems, Dec.1997 as well as Prof. Yinong Chen of University of Witwatersrand for his encouragement of making the paper. The paper owes very much to Mr. Daniel Martin, one of my colleagues at Hitachi Ltd. for his improving the sentence in the paper and Mr. Masahide Ushiyama of International University of Health and Welfare for his editorial support .

Reference

(1)H.Ihara et al.; "Fault Tolerant Computer System with Three Symmetric Computers" IEEE Proceedings,Vol.66,No.10,pp.1160-1177(1978)

(2)K.Mori, H.Ihara et al.; "Autonomous Controllability of Decentralized System aiming at Fault Tolerance" Proceedings of 8th IFAC World Congress, pp.1833-1839(1981)

(3)K.Mori, H.Ihara et al."Autonomous Decentralized Loop Network " IEEE Compcon Spring'82,pp.192-195(1982)

(4)H.Ihara, K.Mori; "Highly Reliable Loop Computer Network System based on Autonomous Decentralization Concept" IEEE FTCS-12,pp.187-194(1982)

(5)Miamoto, H.Ihara et al.;"FMPA; Fault Tolerant Multi-Microprocessor System based on Autonomous Decentralization Concept" IEEE FTCS-13,pp.4-9(1983)

(6)H.Ihara,K.Mori;"Autonomous Decentralized Computer Control Systems",IEEE Computer,pp57-66(1984)

(7)K.Mori, H.Ihara et al.;"Autonomous Decentralized Computer System and Software Structure", Computer System Science & Engineering, pp.16-22(1985)

(8)H.Ihara; "Revolution of Reliable Computing in Hitachi and Autonomous Decentralized System", Vol.1 Dependable computing and Fault Tolerant Systems-The Evolution of Fault-Tolerant computing , Verlag, pp.77-100(1987)

(9)N.Kanekawa, H,Ihara et al.;"Dependable Onboard Computer Systems with A New Method" IEEE FTCS-19,pp.13-19(1989)

(10)H.Kato, H.Ihara et al. ;"Long life Dependable Computers, On board Application", Vol.4 Dependable Computing and Fault Tolerant Systems-Dependable Computing for Critical Applications, pp.153-173(1991)

(11)M.Ito ed.;"Jiritubunsan"(Report on Autonomous decentralization),Poject report in Japanese(1994)

(12)This paper is written based on the key note speech given by H.Ihara at IEEE Pacific Rim International Fault tolerant Systems'97 in Taipei, Taiwan (Dec. 1997)