FAULT TOLERANT COMPUTER CONTROL FOR A MAGLEV TRANSPORTATION SYSTEM*

Jaynarayan H. Lala, Gail A. Nagle
Advanced Computer Architectures Group
The Charles Stark Draper Laboratory
555 Technology Square, MS 73
Cambridge, MA 02139

George Anagnostopoulos, US Dept. of Transportation
Cambridge, MA 02142

SUMMARY

Magnetically levitated (Maglev) vehicles operating on dedicated guideways at speeds of 500 km/hr are an emerging transportation alternative to short-haul air and high-speed rail. They have the potential to offer a service significantly more dependable than air and with less operating cost than both air and high-speed rail. Maglev transportation derives these benefits by using magnetic forces to suspend a vehicle 8 to 200 mm above the guideway. Magnetic forces are also used for propulsion and guidance. The combination of high speed, short headways, stringent ride quality requirements, and a distributed offboard propulsion system necessitates high levels of automation for the Maglev control and operation. Very high levels of safety and availability will be required for the Maglev control system. This paper describes the mission scenario, functional requirements, and dependability and performance requirements of the Maglev command, control and communications system . A distributed hierarchical architecture consisting of vehicle on-board computers, wayside zone computers, a central computer facility, and communication links between these entities was synthesized to meet the functional and dependability requirements of the maglev. Two variations of the basic architecture are described: the Smart Vehicle Architecture (SVA) and the Zone Control Architecture (ZCA). Preliminary dependability modeling results are also presented.

I. INTRODUCTION

Magnetically levitated (Maglev) vehicles operating on dedicated guideways at speeds of 500 km/hr are an emerging transportation alternative to short-haul air and high-speed rail. They have the potential to offer a service significantly more dependable than air and with less operating cost than both air and high-speed rail. Maglev transportation derives these benefits by using magnetic forces to suspend a vehicle 8 to 200 mm above the guideway. Magnetic forces are also used for propulsion and guidance. A combination of factors such as high speed, short headways, stringent ride quality requirements, and a distributed offboard propulsion system make Maglev a unique mode of travel.

Maglev vehicles will travel at a much higher speed than conventional trains and at a significantly higher speed than conventional high speed rail. Although the higher speed increases transportation productivity, it implies more serious consequences if the control system fails to maintain safe train separation. Thus, the response time of the control system must be on a par with the response times of aircraft control systems. Furthermore, achieving a passenger load which makes the system economically viable, requires the shortest

* This work was sponsored by the Federal Railroad Administration under Contract DTFR-53-91-C-00043.

headways possible within the limits of safe train separation. This conflict between capacity and safety can be mitigated by the use of a fully automated and validated control system which offers significantly faster response times than one using human operators.

The Maglev control system will be comprised of sensors, actuators, communication links, and computers whose collective activities will be coordinated and directed by control and decision making software. Maglev control systems are required to make many decisions in real-time. The consequences of an incorrect or late decision could be catastrophic. Since human safety is at risk, the automated control systems must work correctly and in a timely manner under all expected operating conditions. Furthermore, since the failure of one part of the system can disrupt travel along an entire route, the control system for Maglev must not only be safe but also highly available.

Since hardware and software are expected to fail at some time during the life of the system, the system must be able to tolerate these faults while maintaining normal operations or, in the exceptional, worst case scenario, fail in a safe manner. That is, the system should continue to function correctly as a whole even when parts have failed. This is referred to as fault-tolerant operation. If this is not possible, the system must be able to systematically shut down in a safe manner, i.e., fail-safe operation.

Under the sponsorship of the US Department of Transportation, a design-for-validation methodology previously developed by Draper Laboratory [1] has been applied to the design of the control computer system for a hypothetical US Maglev Transportation System [2]. Following the key steps prescribed by the methodology, the mission scenario, functional requirements, and dependability requirements of the Maglev command, control and communications system were developed. Performance requirements were then quantified with variations allowing for both electro-dynamic (EDS) and electro-magnetic (EMS) suspensions.

A distributed hierarchical architecture consisting of vehicle on-board computers, wayside zone computers, a central computer facility, and communication links between these entities was synthesized to meet the functional and dependability requirements of the Maglev. Two variations of the basic architecture were developed: in the Smart Vehicle Architecture (SVA) the on-board computer has the primary responsibility for train control and the wayside zone computers provide backup and consistency checking; in Zone Control Architecture (ZCA) these roles are reversed.

A set of qualitative and quantitative evaluation criteria for the Maglev control computer system were developed. A fail-safe communication protocol for the SVA was proposed and used to model and analyze the dependability characteristics of this architecture.

II. MAGLEV MISSION SCENERIO

The first step in the design-for-validation methodology is to develop a concept of operations which defines the mission scenario, including the method of operation and the operational environment, and specifies the computer control functional requirements. The concept of operations presented here is intended to produce a control system which can meet the most rigorously demanding operational requirements of an advanced and fully developed Maglev transportation system. Figure 1 shows various phases of operation of a typical Maglev vehicle during a 24-hour period.

During a stationary pre-run inspection in the maintenance phase, the vehicle performs internal self-checks on all its vital systems. Another use of the maintenance phase is to perform routine periodic maintenance. At this time, the maintenance crew inspects the vehicle, reviews fault logs and conducts the

scheduled diagnostic tests called for by the vehicle life-cycle maintenance program. The interval between these maintenance periods can be adjusted to meet the availability requirement of the vehicle. When necessary, the crew replaces components (Line Replaceable Modules or Line Replaceable Units) identified as faulty. If the testing and normally scheduled maintenance procedures do not identify any major repairs, the crew advances the vehicle to the normal operation phase. Otherwise, the vehicle is taken off-line and moved to a bay or a central repair facility for more extensive depot maintenance.

During normal operation, built-in-test (BIT) maintenance operations are conducted in the background and any detected faults are logged in non-volatile mass memory. The average duration of travel is two hours and twenty minutes, including station stops and post-mission maintenance, for a total of twenty-two hours daily. There is an average of three off-line station stops per mission. Station stops last an average of three minutes, during which time passengers board and leave the train, and additional BIT maintenance is performed. The vehicle has sufficient redundancy in all of its systems to allow it to be dispatched with faults, should those faults occur during normal operation. Of course, there is some minimum complement of components which must be functioning to allow the system to maintain the required level of reliability for a given mission. This is called the minimum dispatch complement (MDC). If faults accumulate such that the MDC is not functioning, the vehicle is not allowed to continue operation as this would expose the passengers and crew to an unacceptable risk of injury. At this point the vehicle would operate in a degraded mode, so as to be able to arrive at the next station for repairs. Redundancy which exceeds the system requirements for safe operation increases the availability of the system by allowing dispatch in the presence of failed components. Furthermore, additional redundancy also enhances the maintainability of the system by deferring repairs until they are normally scheduled to take place in a maintenance facility.

The capacity of each vehicle is 120 passengers. The line speed between stations is 500 km/hour. Vehicles will be dispatched so as to allow a volume of 4,000 to 12,000 passengers per hour to travel along the route. At peak capacity, the headway for each vehicle is approximately 36 seconds or 4 kilometers at 400 km/hour.

Off-line stations offer significant advantages in terms of capacity and flexible schedules required by the inter-city transportation market in the US . An off-line station is essentially a section of guideway built parallel to the main line. A specialized section of the guideway, called the switch, allows a vehicle to be diverted to either the main line or the off-line sections. Navigation of the switch may be accomplished in two ways, referred to as active or passive switching. In so-called passive switching, the guideway simply forms a Y-shape and the vehicle negotiates a route down one fork or the other. In an active switch, a flexible section of guideway is moved from one position to the other, thereby altering the route the vehicle follows. In either case, switching poses a significant burden on the control system both for safety and performance.

The final parameters which can have a significant impact on the architecture of the Maglev control computer system are the ride quality and passenger comfort and the number and distance between wayside zone controllers and safe stopping areas.

The level of ride comfort for normal, non-emergency operations will meet the two hour reduced comfort limits stipulated by ISO-2631. For emergency situations, a deceleration range is allowed, depending on the severity of the situation. When conditions allow, a deceleration of not more than 0.25 g will be used. For extreme situations, for example, when necessary to decelerate to prevent or mitigate a sudden stop, decelerations of up to 0.5 g are allowed.

Between any two stations there are approximately forty wayside zone controllers. The distance between these wayside zones is 2 kilometers. The site of each wayside zone controller also serves as a safe stopping area between stations.

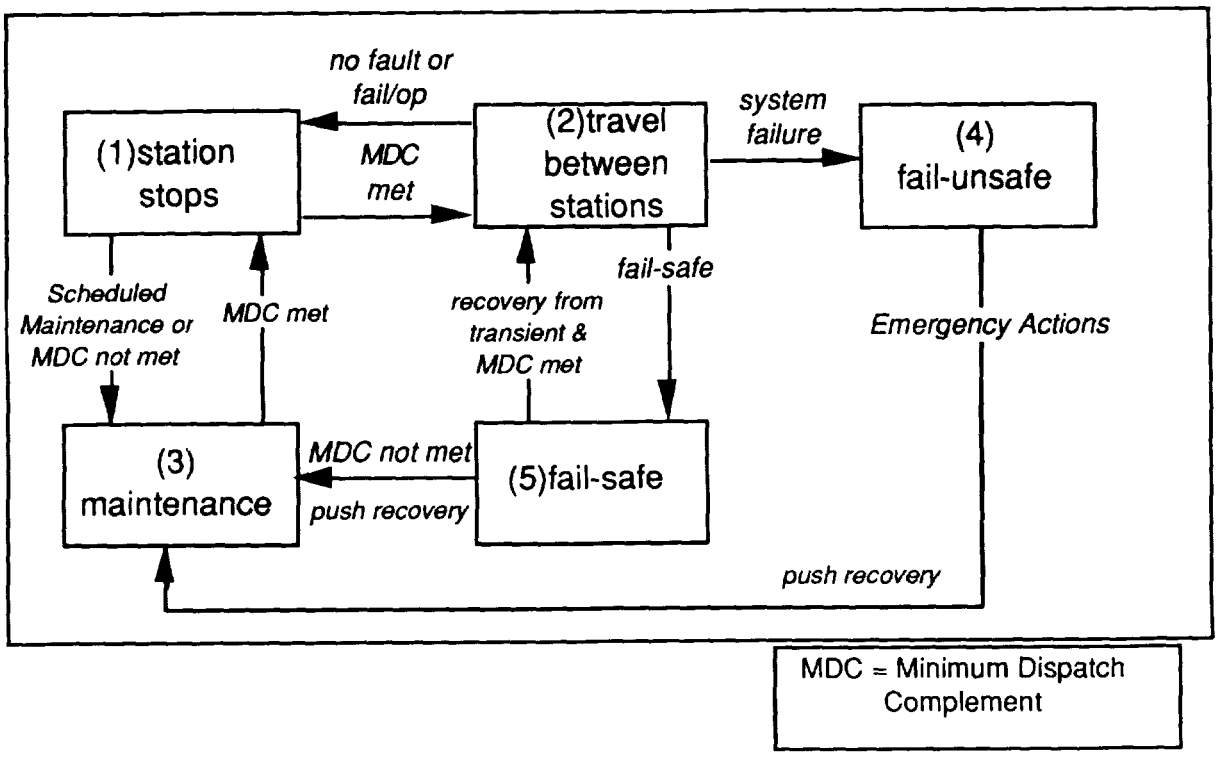

Figure 1. Maglev mission scenario vehicle state diagram.

III. MAGLEV FUNCTIONAL REQUIREMENTS

In order to determine the detailed computational requirements of the complete Maglev system, a set of functional requirements must be specified. Computational requirements include throughput, memory, processing lag, function iteration rate, order dependencies among functions, and I/O and inter-function communication rates. To fully specify the computer architecture for Maglev, constraints imposed on the control computer must also be provided, such as limitations on weight, power and volume.

Guided ground transportation control systems must perform three principal functions: control, protection, and supervision. In a fully automated system, these functions are performed by three main control system components: the onboard control computer, the wayside or zone control computer, and the central control computer. Each system component performs different aspects of each of the three principal functions. Historically, the vehicle control function has been performed by each individual train as it makes its way along the track. Wayside control has performed most of the functions pertaining to route integrity, such as operating the switching mechanisms and setting the maximum speed for a given section of track [4]. This division of tasks, which has been demonstrated to provide a reliable means of safe train separation, follows naturally from the fact the propulsion system which controls the velocity, acceleration, and braking of the vehicle is physically resident onboard the vehicle and the wayside has up-to-date knowledge of the track in its locale. However, the propulsion system for Maglev vehicles is *not* resident onboard the vehicle, but rather housed in stations distributed along the guideway. The design of the Maglev control system must reflect this important difference. The role of the central control computer is to perform the high level planning and coordination functions, such as setting up train arrival and departure schedules as well as scheduling maintenance operations. Central control also plays a role in coordinating the response of the system to an emergency situation. Some aspects of central control may actually be performed by computers located in stations.

Each of the three principal functions which must be performed by the Maglev control system, i.e. control, protection, and supervision, can be decomposed into several well-defined sub-functions. This purely functional analysis of the control system may be used as the basis for the design of a control architecture. By partitioning the sub-functions among the various control elements which make up the system, an optimal design for safety and reliability can be achieved. The functional decomposition of the Maglev control system is presented in Table 1. A quantitative analysis of the computational requirements of each function was performed and these results are summarized below.

Vehicle Control Functions

The vehicle state function is a sensing function which monitors the vehicle position, travel direction, speed, and acceleration. The velocity control function causes the speed and direction of travel of each vehicle to match the speed mandated by its travel profile (determined by the route planning and scheduling functions) in accordance with the existing conditions on the guideway. The velocity control must coordinate the activities of the individual propulsion power units in the guideway, which are nominally spaced at 2 km intervals along the guideway. Closer spacing of power units provides finer granularity of control for additional cost.

The levitation control for the EMS design consists of controlling the gap (about 8 mm) between the levitation magnets and the guideway at about 100 Hz. This is accomplished by controlling the current flow in the onboard electromagnets, which in turn determines the attractive magnetic force between the vehicle electromagnets and the guideway ferromagnets. For the EDS design, the gap does not require active control. However, the temperature of the superconducting onboard electromagnets needs to be carefully monitored and maintained at about 5° K. If the temperature rises above this value, quenching will occur leading to a loss of magnetic force.

Table 1. Maglev Control System Functions

CONTROL	PROTECTION	SUPERVISION
Vehicle State	Safe Vehicle Separation	Route Planning
Velocity Control	Vehicle Position Control	Route Scheduling
Levitation Control	Route Integrity	Dispatching
Lateral Position Control	Emergency Stopping	Maintenance Scheduling
Propulsion Control	Emergency Speed Control	Operator Interface
Secondary Suspension Control	Emergency Position Control	Status Displays
Route Control	Emergency Response	Passenger Supervision
Vehicle Systems Monitoring	Failure Management	
Vehicle Systems Control		
Environmental Monitoring		

For lateral position control (EMS design) the gap between the lateral guidance electromagnets and the guideway must be actively controlled in the same manner as for the levitation magnets. For the EDS design, the temperature of the superconducting guidance magnets must be maintained in the same manner as that of the temperature control of the levitation magnets.

Propulsion is achieved by the use of a linear synchronous motor made up of conducting windings, installed along the length of the guideway, and variable frequency converters which, together with the necessary switch gear, are located at sites distributed along the guideway. Each power unit can control the motion of a vehicle along a section of guideway called a zone. The speed of the vehicle within a zone is controlled by varying the frequency of a traveling electromagnetic field produced in the stator windings of the guideway by the power electronics system.

The purpose of the secondary suspension system is to provide a satisfactory level of ride comfort to passengers in the vehicle. EDS systems which possess a fairly stiff primary suspension require an actively controlled secondary suspension to achieve a satisfactory level of ride quality. For EMS systems, active control may not be necessary but could be provided to enhance the overall smoothness of the ride and offset jerk due to sudden accelerations and lateral motions induced by turns and cross-winds. The secondary suspension can be provided by a combination of actively controlled aerodynamic surfaces and actively or passively controlled dampers.

The route control function guides the vehicle through one of two possible paths at switching points in the guideway as indicated in the route profile. If an active switch is employed, the switching mechanism must be engaged at precisely the right moment to allow adequate time to detect a possible mechanical failure and safely stop an approaching vehicle. Designs of passive switches vary greatly but all require control of either an electrical or mechanical subsystem with similar timing and verification requirements to those of an active switch.

Onboard systems such as lighting, temperature, air flow, secondary braking capability, charge level of onboard batteries, and door position control are monitored and adjusted periodically. Environmental conditions such as the electromagnetic field strength at various positions in the coach, lateral wind speed and direction and external temperature are measured periodically. Advance weather information is collected.

Vehicle Protection Functions

These functions provide a fail-safe mode of operation. They can override the actions of the vehicle control functions and take control of a vehicle which has exceeded some safety threshold.

The safe separation function is responsible for ensuring that a minimum spacing of 4 km or 2 zones is maintained between any two consecutive vehicles on the guideway. The route integrity function monitors the integrity of the guideway and the propulsion and levitation coils. The guideway must remain properly aligned and free from hazards such as ice, litter, animals, etc. The emergency stopping function is employed when the primary braking capability of the linear synchronous motor provided by the guideway has failed. Secondary braking is accomplished by a combination of aerodynamic braking from either the trailing flap or a parachute, eddy currents, and friction after the vehicle has contacted the guideway.

The emergency speed control function is employed when the propulsive force provided by the guideway has failed. Sufficient energy must be available from batteries and the linear generators (which operate only while the train is moving) to control levitation, braking, and other loads. The vehicle is only allowed to stop at areas deemed safe stopping areas. A safe stopping area provides a means of safe evacuation of passengers from the vehicle. The emergency position control function determines the exact stopping point for a vehicle in an emergency stopping situation. Information about safe stopping points is maintained for each zone along the guideway.

Vehicle Supervision Functions

Supervision functions include route planning, scheduling and dispatching vehicles on these routes, displays of vehicle status, position, and velocity, weather displays, etc. A detailed discussion of these functions can be found in [2].

Computational Performance Requirements

A quantitative analysis of each of the computer control functions was performed to determine the computer performance required to do all of the Maglev functions. Estimates were made of such parameters as the iteration rate, throughput, memory, sensor data, frequency of reading sensors and outputting actuators, etc. for each function. These estimates were aggregated to help size the computer and communication links. A detailed discussion of the performance requirements is outside the scope of this paper due to space limitations but can be found in [2]. However, in summary, we can state that 10 to 15 MIPS throughput, 20 to 25 Mbytes of on-line memory, about 5 to 10 Mbits/sec of I/O bandwidth, and a 100 Hz iteration rate for the highest frequency control tasks would be sufficient to not only perform the functions identified here but also allow for about 50% growth margin. These requirements are well within the state-of-the-art of current microprocessors. If performance requirements were the only driver, the design of the Maglev control computer system would be a fairly straightforward task. However, it is the dependability dimension as well as validation of the system which makes the design a challenging task. These requirements are discussed next.

IV. MAGLEV DEPENDABILITY REQUIREMENTS

Dependability is defined as the trustworthiness of a computer system such that reliance can justifiably be placed on the service it delivers [5]. Reliability, availability, and safety are some of the attributes used to quantify the dependability of a system.

The reliability requirement, stated as a probability of failure, for the system control software, and presumably for the hardware upon which it executes, for commercial Maglev transportation, as specified in the draft Maglev System Parameters [3], is 10^{-9}. This requirement is based on the commercial transport flight control requirements mandated by the US Federal Aviation Administration (FAA). Those requirements pertain to a 10-hr commercial passenger flight.

It should be noted that for aircraft, the terms reliability and safety are used interchangeably as far as the flight-critical controls are concerned. This is due to the fact that the failure of a flight-critical computer is always assumed to result in a catastrophic aircraft failure if there is no backup system. In other words, for flight control computers, there is no fail-safe state. Hence, the reliability of the system, i.e. the probability that it will operate correctly over a given time interval, is equal to the safety of the system, which is the probability that it will operate correctly *or* fail in a safe manner. This is not necessarily the case for Maglev. If the control computer on-board the vehicle were to fail, it may not always lead to a catastrophic vehicle failure. For example, the computer may fail-stop and the vehicle may coast to a stop on the guideway. Or, the computer may cause the vehicle to exceed the speed limit which may be detected by a wayside computer which, in turn, may not turn the power on to the next section of the guideway resulting in the safe stopping of the vehicle. Thus, there are several alternatives available to bring a Maglev vehicle to a safe stop in the absence of a functioning on-board computer which are not available to an aircraft in flight. For these reasons, the safety and the reliability requirements for Maglev must be distinguished. In particular, the reliability requirement stated above for a commercial transport aircraft becomes the safety requirement for Maglev vehicles, which then may be specified as follows:

"The maximum acceptable probability of failure of the (safety-critical) computers is 10^{-10} per vehicle per hour of operation."

This requirement applies to the total computer system, including the hardware and software of the onboard vehicle, wayside and central control facility computers. The reliability requirement for Maglev relates to the probability of successfully completing a trip and a reasonable value for not completing a trip due to computer system malfunction is 10^{-6} per vehicle per hour.

The overall reliability and safety requirements for Maglev may be illustrated as follows. If 1 billion trips, each of 1 hour duration, were undertaken by a fleet of Maglev vehicles, then all except 1000 trips should be completed successfully. Of the 1000 trips in which the vehicles did not arrive at their destination without incident, only 1 would result in a catastrophic accident. If we assume that Maglev trains have the same number of scheduled departures per day as airplanes in the US, i.e. 14,000 per day, and that each trip averages one hour, these 1 billion trips will take approximately 195 years. Over that period of time, in a system which met the stated reliability and safety requirement, there would only be five incomplete trips per year and a total of one catastrophic accident attributable to the failure of the control computer system.

The availability of the Maglev transportation system is going to play a very important part in the public's acceptance of this mode of transportation. For the domestic US commercial airlines, the availability of the airliners approaches or exceeds 99 per cent. Less than 1 per cent of the flights are delayed or cancelled due to mechanical, electrical, hydraulic or other aircraft system related failures. It is obvious that the Maglev transportation system will have to match or exceed this level of dependability in order to be accepted by the public. A reasonable availability requirement for Maglev may be specified as follows:

" The maximum acceptable probability of not being dispatch ready for a trip for each Maglev vehicle will be 10^{-2}."

This requirement applies to all the subsystems on-board each vehicle. The unavailability apportionment for the control computer subsystem is assumed to be one tenth of this, or 10^{-3} per vehicle per trip. That is, only one tenth of the unavailable vehicles will be stuck due to on-board control computer system failures.

V. MAGLEV CONTROL SYSTEM ARCHITECTURE

Section III presented the principal functions to be performed by the Maglev computer control system: control, protection, and supervision. These functions can now be mapped to specific computation sites within the overall control computer architecture.

The overall Maglev control architecture is distributed and hierarchical. Its principal subsystems are an onboard vehicle computer system for each vehicle, a wayside zone computer system for each zone, and a central facility computer system as shown in Figure 2. Two basic architectures, which represent extremes of a continuum, are presented here.

In the Zone Control Architecture (ZCA), the primary responsibility for vehicle control rests with the wayside zone control computers, with the onboard system providing backup and consistency checking. Vehicle protection is distributed among the three subsystems. In the Smart Vehicle Architecture (SVA), the onboard computer has the primary responsibility for vehicle control, with the wayside zone computers providing backup and consistency checking. The functions relating to vehicle protection are again

distributed among the three subsystems. The function-subsystem mapping for these architectures is shown in Table 2. In this table, **P** signifies the primary assignment, B signifies the backup assignment used for verification and consistency checking, and I represents local access to information in a database.

In both architectures, the vehicle protection subsystem operates independently from the vehicle control functions, and therefore provides a fail-safe mode of operation. In cases where the speed or position of a vehicle exceeds safety thresholds, these protection functions can override the actions of the control functions and assume control of the vehicle. The supervision function is performed by the central facility computer system, which also includes major computing subsystems located in stations. However, the supervisory data such as the travel or route profile for a given vehicle which is needed by the primary control computer to adequately perform its function is transferred to that computer on at least a daily basis and may be updated more frequently. This form of operation views all normal train travel as planned in advance and all passengers riding in reserved seats. However, either architecture could be adapted to a demand driven schedule which requires more real-time planning capability.

In general, those functions which can best be performed in one site over another are assigned to those sites. For example, the control of levitation, guidance, secondary suspension, and onboard systems like air conditioning and lighting all require the control of onboard actuators. Furthermore, the sensors needed to obtain feedback information for these systems are also onboard. Hence, the control of these functions should be performed by an onboard computer. Other criteria used to assign functions to particular computational sites include minimization of communication and data latency, minimization of adverse effects of failures of communication links and processors, and ability to validate the architecture. Functions which can be performed by an onboard computer with a minimum of communication overhead is that of emergency stopping, emergency speed control, and emergency position control. The emergency which these functions are intended to address is the failure of the guideway propulsion and primary braking capability. The power for these emergency operations comes from batteries carried onboard for that purpose. The vehicle must be able to reduce its speed, continue onto a safe stopping area and stop there so that passengers can disembark safely from the vehicle and the elevated guideway.

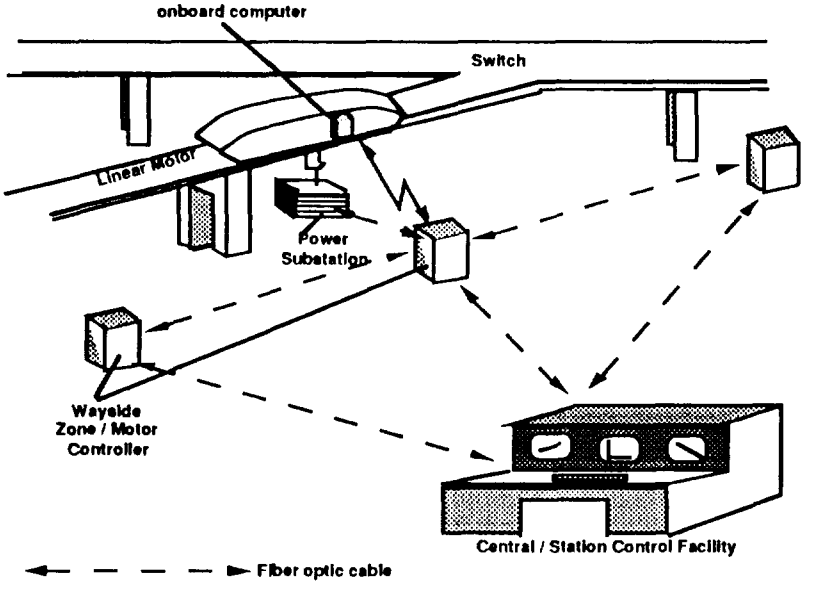

Figure 2. Maglev control computer architecture.

C-3.

Table 2. Function Assignment for the Zone Control Architecture and the Smart Vehicle Architecture

	ZONE CONTROL ARCHITECTURE			SMART VEHICLE ARCHITECTURE		
	Onboard	Wayside	Central	Onboard	Wayside	Central
CONTROL						
Vehicle Location	B	P		P	B	
Velocity Control	B	P		P	B	
Levitation Control	P			P		
Lateral Position Control	P			P		
Propulsion Control		P			P	
Secondary Suspension Control	P			P		
Route Control	B	P		P	B	
Vehicle Systems Monitoring	P			P		
Vehicle Systems Control	P			P		
Environmental Monitoring	B	P		P	B	
PROTECTION						
Safe Vehicle Separation	B	P		P	B	
Vehicle Position	B	P		P	B	
Route Integrity	B	P		P	B	
Emergency Stopping	P	B		P	B	
Emergency Speed Control	P	B		P	B	
Emergency Position Control	P	B		P	B	
Emergency Response			P			P
Failure Management			P			P
SUPERVISION						
Route Planning		I	P	I		P
Route Scheduling		I	P	I		P
Dispatching		I	P	I		P
Maintenance Scheduling			P			P
Operator Interface	P		P	P		P
Status Displays	P		P	P		P
Passenger Supervision	B		P	B		P

The rationale behind the ZCA is that, unlike conventional transportation systems in which the mechanism for vehicle propulsion is resident onboard, the Maglev system is powered from the guideway. The propulsion control must be co-located with the power converters, i.e. within the same zone control computers, since the required iteration rate is so high as to preclude any communication latency. Since the wayside zone controllers must communicate with each other to coordinate the speed of the vehicle as it passes from one zone to the next, they can also perform the function of safe vehicle separation and vehicle position which are related to vehicle speed. The communication between wayside systems can be carried out through very reliable media such as redundant fiber optic links. By locating sensors in the guideway,

the vehicle location and route integrity functions can also be performed by the wayside using sensors embedded in or alongside the guideway for these purposes. Route control, or the direction of the vehicle through a switch, can also be performed from a wayside computer, especially if the switching mechanism is that of a moveable section of guideway. The ZCA most closely resembles conventional railway control systems without the attendant communication overhead that characterizes systems controlling onboard propulsion from the wayside [4].

The rationale behind the SVA is that an autonomous vehicle can most easily direct its own motion since it is in a position to obtain information about its own state and the state of its surroundings. It must be able to perform these functions for emergency purposes anyway. Hence, it may as well perform them for normal operations. It can easily communicate speed commands to wayside propulsion control systems using radio communication. Information about its speed, position, and acceleration are also easily obtained from a combination of a Global Positioning Satellite System and low cost Inertial Navigation Systems such as those based on micro-mechanical instruments, the technology for which will be available by the time the U.S. Maglev Transportation System reaches the prototype development stage. With information about its position and speed, it can perform the functions of safe vehicle separation and vehicle position control by communicating with vehicles both ahead of it and behind it on the guideway. By using onboard sensors, it can also perform route integrity checks both for alignment and obstacle detection. Furthermore, it can easily direct its movement through switches, i.e. perform route control operations, especially if the switches in use do not involve moveable sections of guideway but rather some vehicle-borne steering mechanism. The SVA most closely resembles the most advanced control systems being installed on conventional and high speed rail systems [4].

In order to determine the relative strengths and weaknesses of each architecture, a quantitative analysis must be performed. The dependability analysis of the onboard control computer for the SVA architecture is presented in the next section. The remaining analyses, namely the dependability analysis of the other components in the SVA and the ZCA and the performance analyses of both architectures, are planned for the next phase of this study. Additionally, life cycle cost also should be used as an evaluation criterion. Components contributing to life cycle cost include not only the initial acquisition cost of hardware and software but also the cost of validating and certifying the hardware and software for safety and the cost of maintaining the system over its life time.

VI. PRELIMINARY DESIGN SPECIFICATION OF THE SVA ONBOARD CONTROL COMPUTER

For the US Maglev Transportation System Onboard Control Computer (OCC), a baseline system using a Fault Tolerant Parallel Processor (FTPP) has been selected. The architecture of the Fault Tolerant Parallel Processor (FTPP) developed by Draper Laboratory was conceived to serve applications with requirements for ultra-high dependability and real-time performance. The FTPP architecture is described in references [6] and [7]. It is composed of many Processing Elements (PEs) and a few specially designed hardware components referred to as Network Elements (NEs). The multiple Processing Elements provide a parallel processing environment as well as components for hardware redundancy. The group of Network Elements acts as the intercomputer communications network and the redundancy management hardware. The FTPP architecture has been designed to accommodate up to 5 NEs and 40 PEs in a single cluster. PEs can be configured in triply or quadruply redundant virtual groups or virtual processors. Since a single state-of-the-art microprocessor provides adequate throughput for the present application, the FTPP is not used as a parallel processor here.

For the baseline OCC an FTPP with one triplex Virtual Processor (VP) and one simplex spare has been selected. The selection of this minimal system is based on the minimum redundancy level needed to mask hardware faults in real-time without suspending time-critical application tasks. If the baseline system falls short of the Maglev RMAS requirements presented in Section IV, additional processing elements

(PEs) and/or Network Elements (NEs) will be added as necessary. For the purpose of the present analysis, the processing elements will be Motorola 68040s which are directly compatible with the VMEbus-based network elements. This baseline system will be modeled for safety, reliability and availability in Section VII.

A brief review of the definitions of safety, reliability, availability, and related terms for the onboard computer is presented in Appendix I since they are particularly important to the following discussion and analysis.

OCC Functionality and Dependability Requirements

The functions performed by the onboard control computer were listed in Table 2. Although velocity and position of the vehicle are directly controlled by the wayside zone control computers (ZCCs), the vehicle itself monitors its precise position and velocity and determines its own speed profile based on existing conditions onboard, in its present zone, and in the system as a whole. The requested velocity is sent as a command via a radio communication link to the wayside zone control computer for the zone in which it is traveling. The iteration rates, throughput, memory, and I/O bandwidth requirements of the OCC ensemble of functions are well within the capabilities of the 68040-based processor board such as the MVME-167 with adequate margins allowed to perform operations for fault tolerance and redundancy management.

Since most of the functions performed by the onboard computer are safety-critical, the inability to perform these functions reliably constitutes an unsafe condition and requires that the vehicle be brought to a stop. However, the vehicle has no onboard mechanism which it can apply directly to stop itself in an emergency. Thus, it must communicate the command to stop to the wayside zone control computer (or the central control computer if the ZCC has failed), which can control the braking mechanism that can bring the vehicle to a stop. Every unsafe condition must be detected and cause a stop command to be issued. However, due to the redundant nature of the system, every fault does not create an unsafe condition. For example, as long as at least two channels of the OCC are operating correctly, safe operation of the onboard control computer is assured. Thus, if one of the three channels of a triplex OCC were to fail, the remaining two channels can continue to operate the vehicle safely.

A failure mode which poses a special problem for reliability (as distinct from safety) is the potential ability of a failed channel to generate an unnecessary stop command, a so-called false alarm. If safety were the only consideration, false alarms would not present a problem. However, false alarms drive down the reliability of the system by increasing the number of unsuccessful missions. In addition, false alarms also reduce the availability of the system as a whole. A disabled vehicle on the guideway renders the guideway unavailable to other traffic until it is removed. Such an event reduces the availability of the guideway.

What is needed is the guaranteed ability to stop safely when continued operation would be unsafe, as well as the ability to prevent false alarms from triggering unnecessary stops. The design discussed below operates in just that way.

OCC Architecture

Figure 3 shows a block representation of the FTPP-based onboard control computer. Three processing elements, designated T_A, T_B and T_C in the figure, form the fault tolerant virtual processor (VP) which conducts the onboard control functions. The fourth PE, designated S_1, acts as a spare. For simplicity, the four Network Elements (NEs) are not shown in the figure. Each Processing Element (PE) is connected to an I/O bus through a specialized interface called the monitor interlock. The redundant I/O

busses are identical. The sensors and actuators needed to perform all of the onboard control functions are attached to these busses, including the radio transmitter used to send velocity/stop commands to the wayside zone controller. Only one channel actually transmits a message to the zone controller. The VP decides which channel this will be.

The purpose of the monitor interlock is to prevent a channel or transmitter which has failed in an active manner from flooding the system with false messages, i.e. the monitor interlock transforms active faults into passive ones. It operates by turning off the power to the failed channel or to its I/O bus.

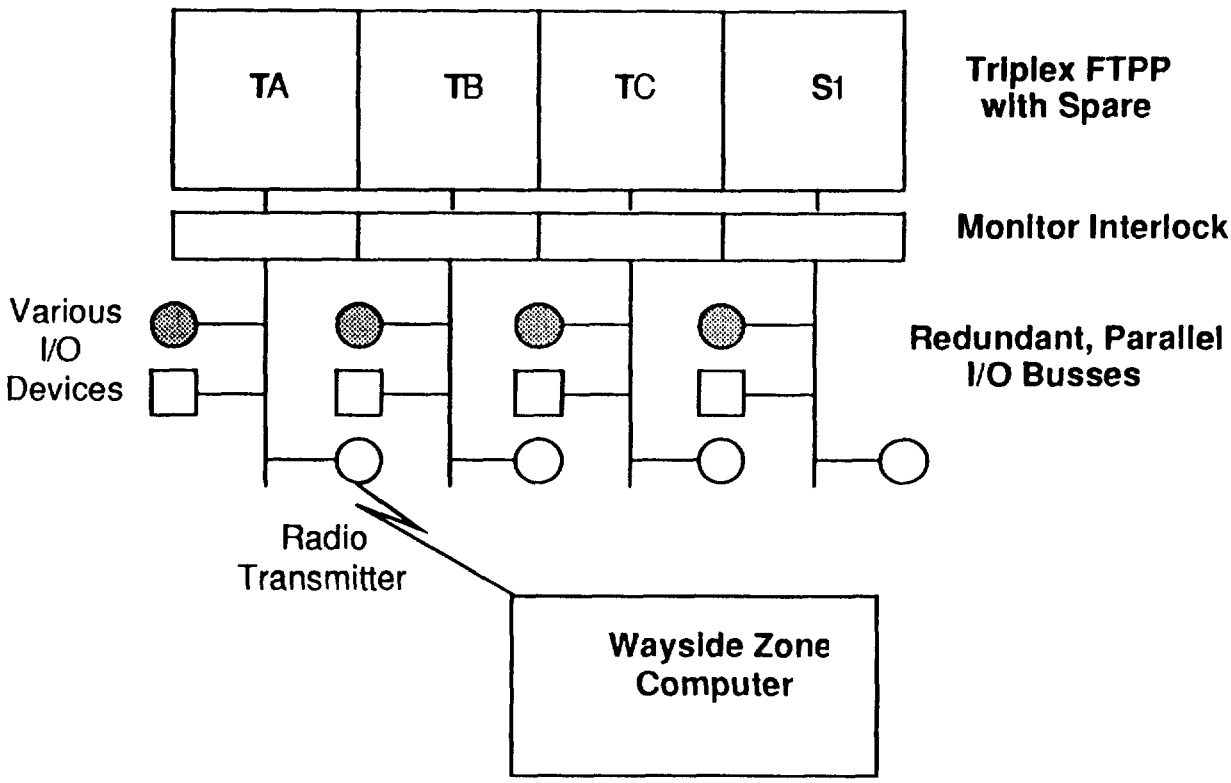

Figure 3. Block diagram of FTPP-based OCC architecture.

Spare PEs or NEs can be used in the OCC to increase availability. Activating a spare is a form of automated repair called reconfiguration. Although the time required to effect this type of automatic maintenance is only on the order of one second, it is still a relatively long period of time to suspend the vehicle control application which typically must execute every 10 milliseconds. Hence, for this analysis, it is assumed that reconfigurations of this type only occur when a vehicle is stopped at either a station or on the guideway following an emergency stop. If modelling shows the reliability of the triplex system is inadequate, the baseline system will be upgraded to a quadruplex FTPP (4 PEs) with 5 NEs and one spare PE.

OCC-Zone Controller Communication Protocol

The communication protocol followed by the onboard and wayside zone computers is designed to prevent false alarms while guaranteeing that every real alarm condition in the OCC results in the transmission of a stop command. It operates as follows. Periodically, the vehicle transmits a *well-formed*

message (WFM) to the wayside zone controller. The specification of a well-formed message is presented below. The maximum allowable time period between a vehicle's transmission of two consecutive well-formed messages is denoted τ_1 in Figure 4. If the zone controller receives a well-formed message from the vehicle, it replies with an acknowledgement within a bounded period of time. The maximum allowable time between a zone controller's reception of a WFM and the OCC's reception of the acknowledgement is denoted by τ_0 in the figure. Since the time between the transmission of a message by the OCC and its reception by the ZCC is very small relative to the values of τ_1 and τ_0, these events can be considered as occurring simultaneously.

These time-out periods are important because the absence of either an expected message or an acknowledgement by either side within the time-out period results in a corrective action. When the corrective actions do not produce the required response, a potentially unsafe condition exists and results in an emergency stop. Thus, if the ZCC does not receive a WFM within a small multiple of τ_1, it assumes that the OCC is in an unsafe condition and so performs an emergency stop. Similarly, if the OCC does not receive an acknowledgement from the ZCC within τ_0 after transmitting a WFM, it assumes that the outgoing message has been corrupted and performs some recuperative action such as switching to another transmitter and retransmitting the message.

The format of a well-formed message transmitted from an OCC to a ZCC is shown in Figure 5. The message consists of a data field and an authentication field. The data field carries the velocity command and other information which the zone controller uses to propel the vehicle at the indicated speed as well as some information specific to the fail-safe communication protocol. The authentication field consists of N 64-bit subfields whose value is uniquely determined as a function of the current message and the channel of the FTPP which generated the value. Each subfield is called the signature of its channel. Each channel of the FTPP is able to generate a unique, unforgeable signature for use by the wayside zone controller in authenticating a message, and, for a given message, no channel can generate the signature of another channel. Prior to transmitting the WFM to the ZCC, each non-faulty channel of the OCC signs the outgoing message and delivers it to the designated transmitter over the OCC's interchannel communication links. Since N is the redundancy level of the onboard VP, $3 \leq N \leq 5$. Thus for the baseline system $N = 3$. Details regarding the subfields in a WFM and their use in the protocol can be found in [2].

OCC-Zone Controller Communication Protocol Operation

One further aspect of the protocol involves the number of onboard radio transmitters and receivers which participate in message passing. While each I/O bus contains a radio transmitter, at any given time only one onboard transmitter is used to send a message. Hence, the wayside zone controller only needs to process a single message. To provide the designated transmitter channel with the capability to append the appropriate authentication fields to the message to be transmitted to the ZCC, each channel independently calculates its signature and provides it to the designated transmitter over the OCC's inter-channel communication links. However, the radio receivers in all onboard channels listen for the acknowledgement. If an acknowledgement is not received by a majority of the channels' receivers within a specified timeout period after transmission of a WFM, the message is retransmitted from another transmitter. Other fail-safe mechanisms are in place to deal with failures of the ZCC. These include the ability of neighboring ZCCs to act as backups for each other as well as the ability of the central control computer to bring any vehicle to a stop anywhere along the guideway. The details of these mechanisms are beyond the scope of this analysis but must be specified before the fail-safe design of the system can be considered complete. Similarly, if the zone controller does not receive a WFM from the onboard system within a specified timeout period (such as some multiple of τ_1 seconds), it initiates an emergency stop procedure.

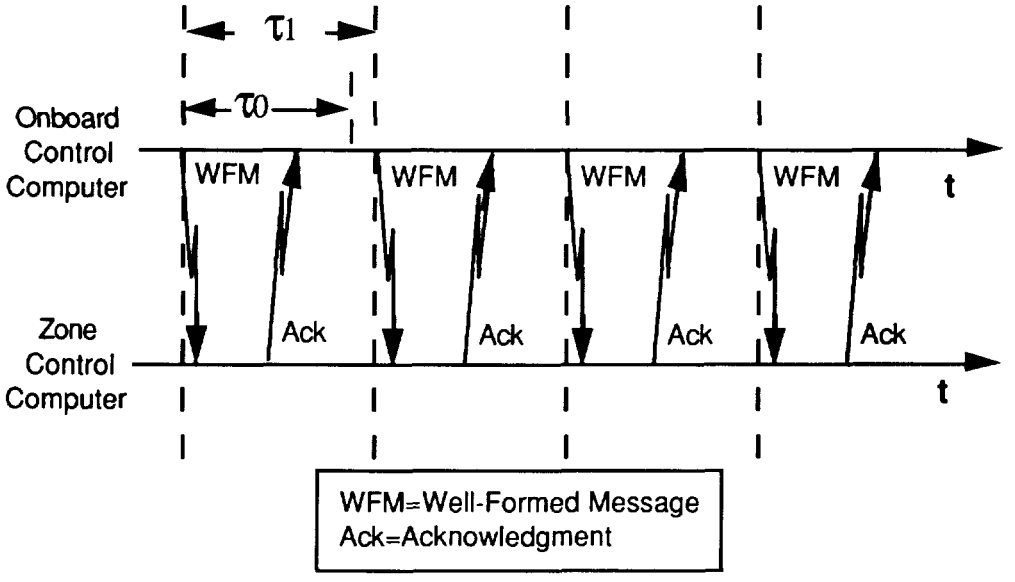

Figure 4. Timing relationships for fail-safe communication protocol.

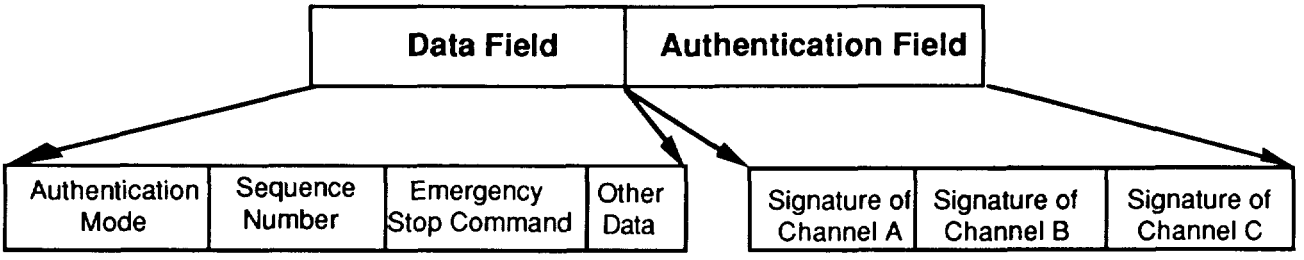

Figure 5. Format of a well-formed message for the fail-safe communication protocol.

To see how this works consider the following scenarios. Suppose that the onboard computer considers that channels A, B and C are working, and that the transmitter connected to channel C is designated to transmit radio messages to the ZCC. Thus, the message contains an authentication mode of ABC. Now suppose that C fails and transmits a stop command. The wayside zone controller would detect this as a false alarm since at most one authentication field (C's) would be valid. (Recall that C cannot forge the signatures of other channels.) This message will not be acknowledged by the ZCC within the timeout τ_0, causing the onboard computer to retransmit a message from another channel, channel B for example, which is not failed and which therefore does not contain a false emergency stop command. Note that this message contains valid digital signatures from channels A and B, thus meeting the requirements for a WFM emanating from a triplex OCC. Thus, the failure of one channel does not trigger an emergency stop. As long as two channels continue to operate, messages are authenticated with the valid signatures of the two working channels.

Furthermore, the OCC's local fault diagnosis function can now update the authentication mode in the first WFM which is sent after the failure is detected to indicate that the OCC is now operating in a duplex mode. Thus the authentication mode field now contains the value AB. Next suppose that channel B, the designated transmitter in this scenario, fails. Either B attempts to transmit messages that are not well-formed or ceases transmission altogether. In either event the ZCC will shut down the vehicle after expiration of the timeout. Alternatively, A can detect B's failure and send an emergency stop message.

Since this message has only one authentic signature, that of channel A, the vehicle is brought to a stop by the ZCC as required by the communication protocol. If, for some reason, A's message does not get through, the ZCC will not get a WFM, the timeout period will expire, and the vehicle will also be brought to a safe stop. Finally, if B fails such that it sends a "false-alarm" emergency stop message which has only one valid authentication signature and hence is not a WFM, the vehicle is again safely brought to a stop by the ZCC. Stopping at this point is a correct action since, by definition, B has failed leaving only a working simplex, namely channel A, in the system.

VII. SVA ONBOARD CONTROL COMPUTER DEPENDABILITY ANALYSIS

The primary objective of the dependability analysis is to produce a first order estimate of the safety, reliability, and availability of the baseline SVA Onboard Control Computer. Additionally, it is desirable to specify a system which is cost-effective by not allocating more redundancy than needed to meet the RMAS requirements, i.e. to determine the Minimum Dispatch Complement (MDC) and to determine the spare components needed to meet the availability requirement with a reasonable maintenance schedule.

The mission state diagram for the Maglev vehicle, shown in Figure 1, was used to construct a detailed Markov model for reliability and safety. Of special interest are the fail-safe and fail-unsafe states. There are only two events which can drive the system to a fail-unsafe state: coincident hardware faults and common mode failures. The probability of the former is addressed below. The probability of the latter cannot be stated with certainty; however, it can be reduced by various avoidance, removal and tolerances techniques. A system failure which results in a fail-safe state does not necessarily require push-recovery to rescue the vehicle. If the failure occurs as a result of a transient fault, which is by far the dominant failure mode, the system may be restarted and the mission completed, albeit not on schedule. It has been noted that the public can accept outage times of short duration (a few minutes), but outages longer than an hour have a very negative impact. Hence this ability to recover from transient faults is very important to public acceptance of Maglev.

The details of the Markov models, the underlying assumptions about component failure rates, fault detection and recovery rates, etc. as well as the dependability evaluations of all the configurations analyzed are beyond the scope of this paper. These details can be found in reference [2]. Only a summary of the results of the dependability modeling effort is presented here.

Reliability and Safety

The reliability and safety of the baseline triplex OCC as well as a quadruplex version, for a single mission, were evaluated with and without transient fault recovery. The advantage of not recovering from transient faults is that exposure to coincident faults during the transient recovery period is avoided. The disadvantage is that unreliability due to exhaustion of redundancy is not minimized. In the second policy, the OCC attempts recovery from transient faults, which reduces the unreliability due to exhaustion of redundancy but increases the exposure to coincident faults during the recovery period.

Two kinds of safe shutdowns are possible under a no-transient-recovery redundancy management policy: "soft" shutdown and "hard" shutdown. If a fault is transient, the vehicle is stopped, the OCC re-initializes itself and resumes operation as a fault tolerant controller, and the vehicle is restarted. This is a soft shutdown. Thus this state does not contribute to vehicle unreliability, although it will contribute to a late arrival at the destination station. In the hard shutdown states, the OCC has shut down due to permanent faults and cannot re-initialize itself and resume operation as a fault tolerant controller, so this state does contribute to vehicle unreliability. External activity such as a tow or physical replacement of an OCC component is required before the vehicle can be cleared from the guideway. Finally, in the "unsafe failure" category, the OCC is unable to safely control or shut down the vehicle.

The Markov models were evaluated for mission times ranging from 1 to 5 hours using the values for the failure and reconfiguration rates shown in Table 3. The results, for a mission time of 2.5 hours, are presented in Table 4.

Table 3. Failure and Reconfiguration Rates

Rate	Value
Permanent Failure Rate, λ_p	1×10^{-4} per hour (10,000 hours MTBF)
Transient Failure Rate, λ_t	1×10^{-3} per hour (1,000 hours MTBF)
Reconfiguration Rate From Permanent Faults, μ_p	5.5×10^{6} per hour (20 msec)
Reconfiguration Rate From Transient Faults, μ_t	2.8×10^{4} per hour (1 sec)

Table 4. Reliability and Safety of Triplex & Quadruplex OCC

Configuration	Probability of Soft Shutdown	Probability of Hard Shutdown	Probability of Unsafe Failure
No Transient Recovery			
Triplex	1.2×10^{-5}	2.5×10^{-6}	2.6×10^{-12}
Quadruplex	4.2×10^{-8}	9.9×10^{-10}	5.3×10^{-12}
With Transient Recovery			
Triplex	0	1.3×10^{-6}	4.7×10^{-10}
Quadruplex	0	3.5×10^{-10}	9.4×10^{-10}

When the triplex OCC is operated without transient fault recovery, the dominant failure mode is soft shutdown. Since soft shutdowns are caused by transient fault accumulation, the OCC can re-initialize from the transient faults after shutting down the vehicle, and subsequently restart and safely control the vehicle. Hard shutdowns are less likely than soft shutdowns, and are caused by permanent fault accumulation. Finally, the probability of unsafe failure is much less likely than either of the two safe shutdown modes. In this case, unsafe failure is primarily caused by a second fault occurring while the OCC is in the process of diagnosing and reconfiguring from a previous fault.

When the triplex OCC is operated with transient fault recovery, the soft shutdown failure mode is nonexistent. The probability of unsafe failure is higher by several orders of magnitude due to increased exposure to a second coincident fault during the transient recovery period.

The probability of unsafe shutdown for a quadruplex OCC is slightly higher than that of the triplex OCC because the quad's added hardware increases the overall failure rate and, consequently, the probability of coincident faults. However, the probability of both hard and soft shutdowns is significantly reduced due to the increased redundancy of the quadruplex.

As the above analysis shows, both the triplex and quadruplex OCC configurations exceed the safety requirement of 10^{-9} per hour. However, because the transient-recovery redundancy management options for both configurations result in unsafe failure probabilities which are uncomfortably close to the OCC's safety requirement, the no-transient-recovery option is preferable for safety reasons.

The triplex OCC without transient recovery marginally meets the OCC's reliability specification (i.e., probability of hard or soft shutdown) of 10^{-6} per hour, while the additional redundancy of a quadruplex OCC enables it to exceed this requirement with a wide margin. Because the triplex OCC only marginally meets the reliability requirement, this analysis leads to the selection of a quadruplex OCC operated without transient fault recovery as the baseline OCC configuration.

Availability

The OCC availability depends on the number of Fault Containment Regions (FCRs) in the OCC, the MDC, and the scheduled maintenance interval. The previous analysis indicates that the MDC must consist of four FCRs in order to meet the reliability and safety requirements. Availability of two OCC configurations was modeled: one with only the MDC, i.e., 4 FCRs, and another with a spare FCR, i.e., a total of 5FCRs. The scheduled maintenance interval is a free variable which can be determined based on the OCC's maximum allowable unavailability. The availability modeling results are presented in Table 5 for a maintenance interval of 200 hours (approximately 8 days).

Table 5. Availability Analysis of OCC

Configuration		MDC	Unavailability after 200 hours
5 FCRs	4		3.7×10^{-3}
4 FCRs	4		7.5×10^{-2}

The availability analysis indicates that 1 spare FCR yields an unavailability after 200 wall-clock hours of 3.7×10^{-3}, which slightly exceeds the OCC maximum unavailability requirement of 10^{-3}.

Further detailed analysis is necessary to perform some tradeoffs. For example, the maintenance interval can be decreased while maintaining a nominal configuration of 5 FCRs. The life-cycle costs of more frequent periodic maintenance must be compared to the savings accrued due to lower FCR hardware procurement costs. Or an additional FCR can be added to increase the nominal configuration to six FCRs. This would allow the maintenance interval to be stretched to 400 hours. The acquisition cost of the additional FCR hardware must be compared to the savings accrued by deferring periodic maintenance in a life cycle cost analysis to determine the cost-effectiveness of this strategy. Also, the failure rate of the OCC components can be decreased in a number of ways, such as reducing their complexity (while still meeting the required OCC functionality), exploiting advanced packaging (which may increase the OCC's cost), utilizing higher-quality components (which may also increase the OCC's cost), or housing the components in a more benign environment in order to reduce their failure rates.

IX. SUMMARY AND CONCLUSIONS

Magnetically levitated vehicles operating on dedicated guideways at speeds of up to 500 KM/HR are now being designed in the US, Europe and Japan. The operation and control of these vehicles will be totally automated. This paper has defined the functions that must be performed by the automated control computer system. Safety, reliability, and availability requirements for the control computer system were also defined. A distributed hierarchical architecture consisting of vehicle on-board computers, wayside zone computers, and a central computer facility was defined to meet the functional and dependability requirements of Maglev. Two variations of the basic architecture, the Zone Control Architecture and the Smart Vehicle Architecture, and their qualitative attributes were also discussed. An architecture for the control computer onboard the Maglev vehicle (OCC) for the SVA was presented along with a communication protocol which provides a fail-safe mode of operation without reducing mission reliability

or overall system availability. Detailed Markov reliability and availability models of the OCC in the SVA were constructed and used to analyze the safety, reliability, and availability of the OCC. Based on this analysis, a baseline configuration of the OCC was selected which meets its dependability and performance requirements in a cost effective and maintainable manner.

Future work includes modeling of other major components of the SVA such as the Zone Control Computers, the Central Computer, communication links and a similar detailed analysis of the ZCA, followed by a comparative life cycle cost analysis of the two alternative architectures.

ACKNOWLEDGEMENT

This work was performed under contract DTFR 53-91-C-00043 with the Federal Railroad Administration of the US Department of Transportation by the Draper Laboratory. Their support is gratefully acknowledged here.

REFERENCES

[1] Lala, J.H., et al., Advanced Information Processing System for Advanced Launch System: Avionics Architecture Synthesis, NASA Contractor Report-187554, C. S. Draper Laboratory, Inc., Cambridge, MA, September 1991.

[2] Lala, J. H., Nagle, G. A., and R. E. Harper, "Verification Methodology for Fault-Tolerant Fail-Safe Computers Applied to Maglev Control Computer Systems," Final Report DOT/FRA/NMI-92/26, Contract DTFR 53-91-C-00043, US DOT, C. S. Draper Laboratory, May 1993.

[3] Final Report, National Maglev Initiative, Government-Industry Workshop, Argonne National Laboratory, Argonne, Illinois, November 1, 1990.

[4] Peterson, C., "Monorail Control System Safety," Journal of Electrical and Electronics Engineering, vol. 10, pp. 28-35, Sydney, Australia, March 1990.

[5] Dependability: Basic Concepts and Terminology, J. C. Laprie, Ed., vol. 5 of Dependable Computing and Fault-Tolerant Systems, Vienna, New York: Springer-Verlag, 1992, pp. 11-16.

[6] Harper, R., Lala, J., Deyst, J., "Fault Tolerant Parallel Processor Overview," 18th International Symposium on Fault Tolerant Computing, June 1988, pp. 252-257.

[7] Harper, R., Lala, J., "Fault Tolerant Parallel Processor," J. Guidance, Control, and Dynamics, V. 14, N. 3, May-June 1991, pp. 554-563.

APPENDIX I: DEFINITIONS

Mission: A *mission* is defined as a trip from one station to another, including departures and arrivals at stations.

Safety: A mission completes *safely* when one of two conditions is met: either (1) the mission completes successfully, i.e. the vehicle arrives at its destination without incident, or (2) the mission is not completed successfully but no one onboard is injured, i.e. when the vehicle stops safely at some intermediate point along the guideway.

Fail-Safe: The ability to bring the vehicle to a safe stop under all possible failure conditions is denoted as the *fail-safe* feature of the system.

Reliability: The probability that a trip completes successfully is defined as the *reliability* of the system. The reliability requirement is not as stringent as the safety requirement because of the existence of the fail-safe mode of operation.

Availability: The *availability* of the system is defined as the probability that a given vehicle is ready to depart for a mission on time, i.e., it has the minimum dispatch complement (MDC) operational.