4th Meeting of the U.S. Software System Safety Working Group
April 27th-29th 2004 @ MIT in Cambridge MA USA

Nancy's Shuttle
System Automation Overview

1 Introduction

Nancy's Shuttle is an entertaining, educational ride through the universe of safety. Guests board shuttle-themed vehicles from a Station Area themed as a space station, and depart for a low speed ride through various vistas designed to expose the rider to concepts of software and systems safety. The Show Area consists of three-dimensional sets recreating scenes of nuclear generators, airport control towers, bio-imaging systems, and other instances where software plays an integral role in system safety.

The attraction is capable of supporting a rider capacity of 1400 guests per hour, with the guest experience lasting approximately four minutes including unloading and loading operations. Each vehicle can accommodate up to seven guests, and will travel at a constant speed (approximately 3 feet per second) throughout the attraction.

Load Operators dressed as flight technicians will assist in the shuttle load/unload process. Guests will be escorted into queue lines, one for each of the three rows of seats in the vehicle. A gate will automatically open when a shuttle arrives in the load area. When guests are properly seated in the shuttle, the Load Operator will close the gate and initiate shuttle motion. Once the shuttle is launched, it proceeds without the need of operator intervention until it returns to the station and automatically stops for unloading. When guests have exited, the Load Operator will advance the shuttle to the load area for the next group of guests.

Under Load Operator control, shuttles can be added from a maintenance area or removed from the attraction by means of a pair of track switches located just downstream of the station where guests load and unload.

This document describes the role of automation in a new ride called "Nancy's Shuttle" to be constructed at the Safeware Theme Park. It contains information for engineering staff and other stakeholders needed to perform a preliminary evaluation of the feasibility, safety and maintainability of the subsystems involved in the automation of this ride.

2 Physical Overview

As shown in Figure 1, the ride site consists of three main areas: the Show Area, Station Area and Maintenance Area.

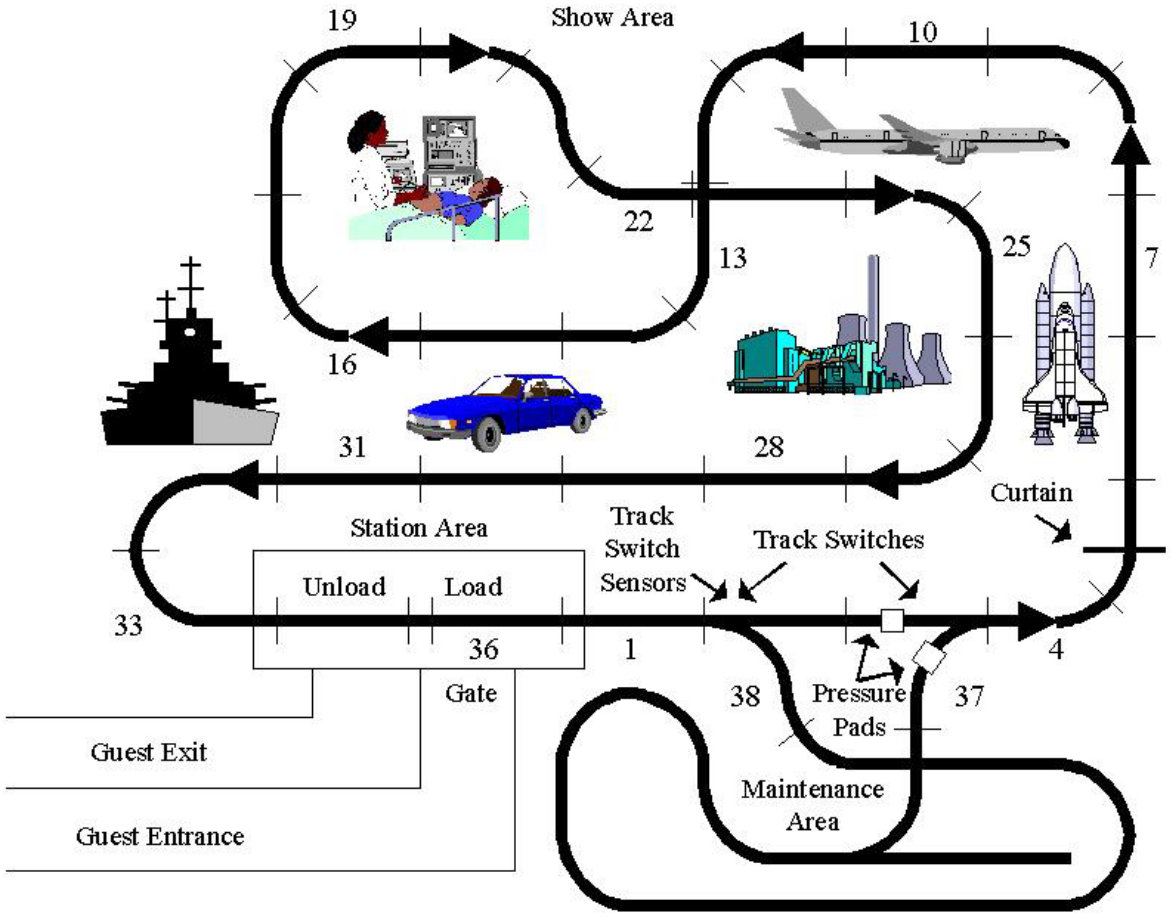

Figure 1 - Physical Layout

Vehicles may be added from the Maintenance Area, or removed from active use into the Maintenance Area by means of a pair of track switches located just downstream of the Station Area. Each track switch has two lockable positions, "main" and "maintenance in". During normal operation, both track switches will be in the "main" position. When the first track switch is set to the "maintenance in" position, the vehicle will be steered into the maintenance area. Setting the second track switch to the "maintenance in" position will steer a vehicle exiting the maintenance area back onto the main rail. The track switches are normally moved by the Load Operator using the Maintenance In selector switch on the Load Operator's Console. Either track switch may be moved independently by a maintenance operator using a mechanical crank. This allows vehicles to be moved by a self-powered towing vehicle into and out of the maintenance area when the segmented bus-bar is not energized.

While in the Show Area, each vehicle will pass through vistas on System Safety in the Space Exploration, Commercial Aviation, Medical Technology, Energy and Automotive Systems sectors. The length of the path in the Show Area is 594 feet.

At the entrance to the first vista, there is a computer-controlled sheet metal curtain that is raised to allow a vehicle to enter a darkened tunnel. This curtain blocks daylight from this first vista in the Show Area to allow for projection of a short video sequence. A hydraulic pump is used to raise the curtain. To prevent the curtain from dropping prematurely (e.g., as a result of a power failure), there is a computer-controlled braking mechanism that will prevent the curtain from dropping whenever the power supply for the hydraulic pump fails. This braking mechanism uses friction to immobilize the curtain. The fail-safe design of this braking mechanism ensures that the braking action will be applied even in the event of a total power failure, i.e., the braking action is applied when the braking mechanism is in the de-energized state.

The Station Area is divided into two zones: the Unloading Zone and the Loading Zone. It is possible to unload a vehicle while the previous unloaded vehicle is being loaded with guests. There is a gate at the entrance to the Station Area that prevents guests from entering the Loading Zone except during the vehicle loading process. There is a passive braking mechanism in both the Unloading Zone and Loading Zone that will cause a coasting vehicle to stop at a fixed position within each zone.

Each vehicle follows a path determined by a guide rail. There is a guide beneath each vehicle that latches onto the rail. There is a segmental bus-bar beside the guide rail that supplies electrical power to the vehicle through an electrical contact attached to the bottom of the vehicle. The vehicle rides on an elevated surface approximately 5 feet above ground level. (Because of seasonal flooding at the theme park, the track surface has been elevated to avoid electrical hazard that might otherwise occur if the energized bus-bar were immersed in water.) The width of each vehicle and the elevated surface is approximately 6 feet and 7 feet respectively.

Each segment of the bus-bar supplies each vehicle with 120v single-phase power. The vehicle will achieve a constant speed of approximately 3 feet per second within 4 seconds of energizing the bus-bar. It will come to a complete rest within 3 seconds when the bus-bar is de-energized.

In the Show Area, the approximate length of each segment of the bus-bar is 18 feet. There are a total of 33 segment in the Show Area, numbered 1 through 33. There is one intersection in the Show Area at the boundary between Segments #12 and #13 and at the boundary between Segments #22 and #23, e.g., a vehicle entering the intersection from Segment #12 will exit the intersection into Segment #13. There are three segments in the Station Area and two segments in the Maintenance Area. Each vehicle is unloaded and loaded while at rest in Segments #34 and #36 respectively. Segment #35 is a short-length buffer zone between the Unloading and Loading zones. Segment #37 is energized when a vehicle is being moved from the Maintenance Area into the Show Area. Segment #38 is energized when a vehicle is being moved from the Show Area into the Maintenance Area. Except for Segments #37 and #38, vehicles are moved in the Maintenance Area by a self-powered utility vehicle. The vehicles are also light enough to be pushed or pulled by the maintenance Load Operators without machine assistance.

All of the ride controls are housed in a glass-sided booth located in the Station Area. Within this booth, the Load Operator has an unobstructed view of the entire Station Area and the initial portion of the Show Area (up to the curtain just before the first vista).

3 Operational Views

When the ride is operational, the Load Operator assists passengers during unloading and loading operations, as well as controls the dispatching of vehicles into the Show Area. The Load Operator is also responsible for moving vehicles into and out of the Maintenance Area. The Load Operator is also trained to respond to emergencies and other unusual situations.

There is a Main Power Reset Button mounted on one side wall of the booth and a Main Power On/Off Switch mounted the opposite side wall. The Load Operator's Load/Unload Console is mounted at waist level in front of the Load Operator (as the Load Operator stands in the booth facing the Loading Zone).

Pressing the Main Power Reset Button causes Main Power Relay #1 to be closed. The Main Power On/Off Switch is a mechanical switch that controls Main Power Relay #2; this relay is closed only when the switch is set to the "On" position. These two relays are connected in series. Hence, the main power supply is only connected to the ride when both relays are closed.

A view of the Load Operator's Console is shown below in Figure 2. The "Close Gates" button is not used. (It is included in the design because this particular console design was previously developed for another attraction where this button is required.)

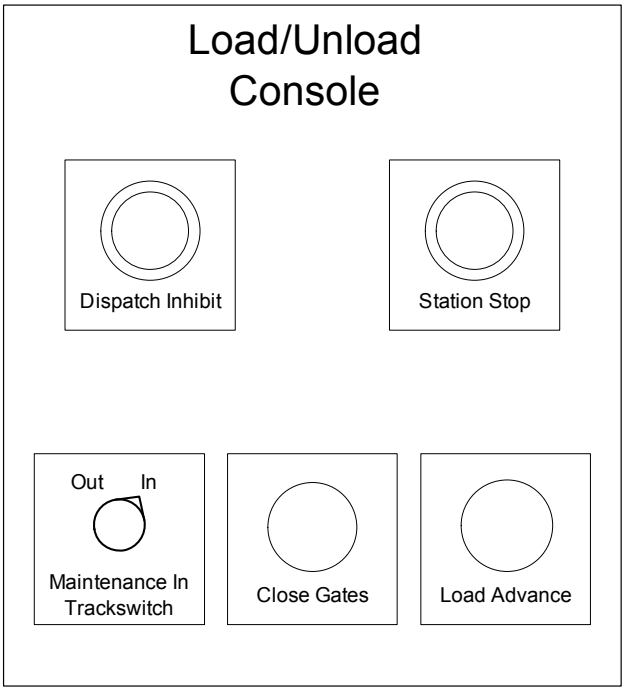

Figure 2 - Load/Unload Console

3.1 Normal Steady State Operation

When operating at maximum capacity, a vehicle may be unloaded in the Unloading Zone at the same time that the previously unloaded is being loaded with guests in the Loading Zone. After closing the gate, the Load Operator visually check that all guests in the Station Area are safely seated in the vehicle in the Loading Vehicle. The Load Operator then presses the "Load Advance" button on the Load Operator's Console. This action causes the vehicle in the Loading Zone to be dispatched to the Show Area and the vehicle in the Unloading Zone to be advanced into the Loading Zone. A vehicle is allowed to enter the Unloading Zone from the Show Area whenever the Unloading Zone is empty. The gate at the Station Area entrance will open automatically whenever a vehicle arrives in the Loading Zone. When operating at maximum capacity, a vehicle will be dispatched from the Station Area into the Show Area once every 18 seconds on average.

At any time, the Load Operator may inhibit the movement of the vehicle in the Loading Zone by pressing the Dispatch Inhibit button. Once pressed, vehicle movement in the Loading Zone will be inhibited until this push/pull button is pulled. While in this state, vehicles may still enter the Unloading Zone.

The ride may be operated below maximum capacity by shunting one or more vehicles to the Maintenance Area and dispatching vehicles less frequently in response to operational needs.

3.2 Removing and Adding Vehicles

A vehicle at rest in the Loading Zone may be removed from active use by means of the track switches. Prior to pressing the Load Advance button, the Load Operator must select the "In" position of the Maintenance In selector switch on the Load Operator's Console. After closing the gate and then pressing the Load Advance button, the vehicle will move into the Maintenance Area.

To add a vehicle from the Maintenance Area, the vehicle must be moved by the Maintenance Load Operator onto Segment #37. Prior to pressing the Load Advance button, the Load Operator must select the "In" position of the Maintenance In selector switch on the Load Operator's Console. After closing the gate and then pressing the Load Advance button, the vehicle will from the Maintenance Area into the Show Area.

3.3 System Startup

System startup is only performed only when the vehicles are unoccupied. The Load Operator must also ensure that no bus-bar segment is occupied by more than one vehicle. To initiate system startup, the Load Operator must first press the "power reset" button and then move the main power supply selector switch to the "on" position. After allowing a minimum of 30 seconds for the computer-based control system to complete initialization, the Load Operator should verify that the system is operating normally before loading guests into vehicles.

3.4 Emergency Stop

In the event of an emergency, the Load Operator may stop all vehicle movement within the Station Area by pressing the "Station Stop" button. Once pressed, all vehicle movement in the Station Area will be inhibited until this push/pull button is pulled.

In the event of an emergency in the Show Area or Maintenance Area, the Load Operator may use the main power supply selector switch to stop all vehicle movement throughout the attraction.

4 Automation View

Figure 3 is a context diagram that shows the inputs and outputs of the computer-based control system.

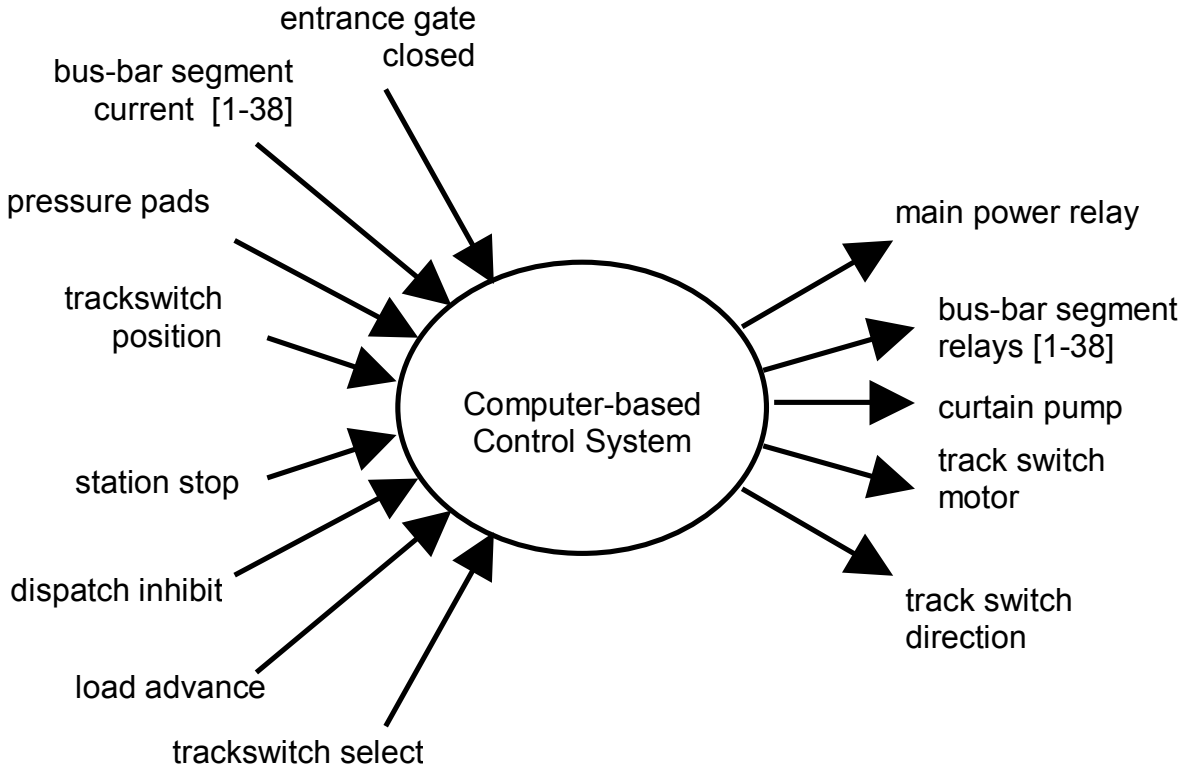

Figure 3 - Computer-based Control System Context

4.1 Control System Inputs

Each input to the control system is a single wire. The wire is energized to 24v to indicate that the input condition is true; otherwise, the wire is grounded to indicate that the condition

is false. By means of interface circuitry, each input condition is associated with a unique addressable memory location that may be sampled by the control software.

entrance gate closed – true when the gate at the entrance to the Station Area is closed and locked; otherwise false.

bus-bar segments current [1-38] – for each of the 38 bus-bar segments, true when current is being drawn by the bus-bar segment; otherwise false.

pressure pads – true when a force of at least 300 pounds is exerted on either of the two pressure pads; otherwise false. An unloaded vehicle weighs more than 400 pounds. The size and position of the pressure pads ensure that the full weight of the vehicle is applied to one of the two pressure pads before the vehicle reaches Segment #4.

track switch position – true when the first track switch (i.e., the track switch closest to the Station Area) is in one of its two position; otherwise false. Because of the mechanical linkage between the two switches, the position of the first track switch also indicates the position of the second track switch.

station stop – true when the Station Stop push/pull button is depressed; otherwise false.

dispatch inhibit – true when the Station Stop push/pull button is depressed; otherwise false.

load advance – true when the Load Advance button is depressed; otherwise false.

track switch select - true when the Maintenance In Switch selector switch is set to the "In" position; otherwise false.

4.2 Control System Outputs

Each output of the control system is a single wire. The wire is energized to 24v to indicate that the output condition is true; otherwise, the wire is grounded to indicate that the condition is false. By means of interface circuitry, each output condition is mapped to a unique addressable memory location that may be set to true or false by the control software.

main power relay – when energized, opens Main Power Relay #1, causing all power to be shut off from the ride. (This will also shut off the computer-based control system.)

hydraulic pump – when energized, hydraulic pump is engaged, causing the curtain at the entrance of the first vista to be raised. Otherwise, the curtain will slowly return to the lowered position by the force of gravity as the hydraulic fluid is allowed to escape through a value into a reservoir.

bus-bar segment relays [1-38] – for each of the 38 bus-bar segments, when energized, causes a relay to be closed which, in turn, causes the bus-bar segment to be energized.

gate opener – when energized, unlocks the gate allowing it to automatically swing open. (The gate is connected to a spring which is stretched when the Load Operator closes the gate.)

track switch motor – when energized, close a relay which, in turn, engages a motor that moves the track switch assembly. The track switches are connected to a single motor that moves both track switches simultaneously between the two possible positions. The two track switches are identical and the mechanical linkage between the motor and the two track switches guarantees that the two switches will move exactly the same distance while the motor is enabled.

track switch direction – when energized, causes the track switch to move towards the "maintenance in" position.

track switch locking pins – when energized, engages locking pins that lock each track switch at its current position. The track is free to move when this output is not energized.

4.3 Functional Behavior

As a vehicle leaves the Show Area, it enters the Unloading Zone. Through the effect of de-energizing the bus-bar for Segment #34 (which engages a mechanical brake on the vehicle motor), the vehicle will stop at the Unloading Position. When the Load Operator presses the Load Advance pushbutton on the Load Operator's Console, the bus-bar in the Unloading Zone will be re-energized and the vehicle forward will move forward into the Loading Zone. Pressing the Load Advance button will also re-energized the bus-bar segment in the Loading Zone causing the vehicle in the Loading Zone to be dispatched into the Show Area. Movement of a vehicle in the Loading Zone may be inhibited by the Load Operator by pressing the Dispatch Inhibit push/pull button. After being pressed, this button must be physically pulled to discontinue the inhibit condition.

The gate at the entrance to the Station Area opens automatically as soon as a vehicle enters the Loading Zone. The gate must be closed by the Load Operator after the next group of guests have entered the Loading Zone. There is a sensor that detects when the gate is closed. After the guests have been loaded into the vehicle, the vehicle will only start moving when the Load Operator presses the Load Advance pushbutton if the gate is determined by the computer to be in the closed position.

The hydraulic pump used to raise the curtain at the entrance to the first vista is turned on when either pressure pad senses a sudden load increase. The pumped is turned off when the same pad senses a sudden load decrease.

To maintain separation between vehicles, the control system will ensure the bus-bar immediately upstream of an energized bus-bar is always de-energized. Otherwise in the Station Area, the control system will energize the bus-bar of the current segment and next downstream segment for each vehicle. The control system must also prevent collisions in the intersection within the Show Area.

When the Load Operator changes the position of the Maintenance In selector switch on the Load Operator's Console, the track switch locking pins will be released, the appropriate track switch direction will be signaled and the track switch motor will be engaged. The motor movement must stop as soon as the track switch reaches the desired position to prevent damage to the track switch or damage to the motor. To complete the operation, the track switch locking pins will be locked.

The computer-based control system is a dual-processor configuration where one processor serves as the primary node and the other processor is the standby node. The standby node monitors the actions of the primary node and will automatically assume control of the system if it detects an indication that the primary node has failed.

5 Design Goals

The main goals for the design of this system are:

1. Guest and Operator Safety – the system should fail safe.

2. High Reliability and Availability – the system should rarely fail.

3. Low Development and Repair Cost – use "off the shelf" components whenever possible.

6 A Note to the Reader

This document was developed for use in a workshop on safety analysis. There are known deficiencies in both this document and the system described by this document.