Universidad de Costa Rica
Facultad de Ingeniería
Escuela de Ingeniería Eléctrica
IE-0523 Circuitos Digitales II
I ciclo 2024

Tarea #1 Descripción conductual de un controlador automatizado para la entrada de un estacionamiento

Oscar Porras Silesky C16042
Grupo 001

Profesor: Ing. Enrique Coen

13 de abril de 2023

Índice

1. Resumen.

Este proyecto presenta el diseño y la implementación de un controlador automatizado para la gestión de acceso a un estacionamiento, que se destaca por su capacidad de operar sin la necesidad de un reloj de sistema (clock). A través de un conjunto específico de sensores y actuadores, el sistema gestiona la entrada de vehículos de forma segura y eficiente, validando códigos de acceso binarios de 8 bits.

El éxito del proyecto se evidencia en la capacidad del controlador para manejar correctamente todas las situaciones previstas, desde la detección de la llegada de un vehículo hasta la activación de una alarma tras múltiples intentos de acceso incorrectos.

Las pruebas realizadas demuestran la fiabilidad del controlador en diversas circunstancias, incluyendo el manejo adecuado del cierre de compuerta tras el ingreso del vehículo y la activación de alarmas pertinentes sin la presencia de una señal de reloj.

Lo que distingue a este diseño es su operación asincrónica; en lugar de depender de un reloj para la secuenciación de eventos, el sistema utiliza la lógica conductual para responder directamente a las señales de los sensores.

2. Descripción Arquitectónica.

2.1. Diagrama de Bloques del controlador.

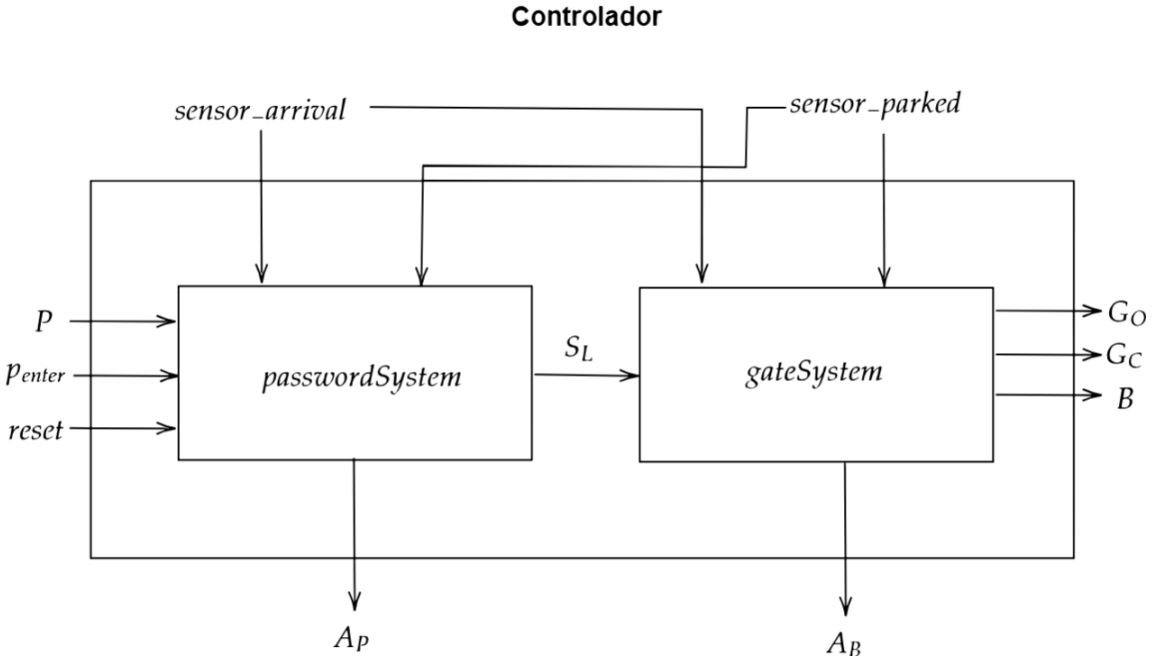

Figura 1: Archivos oculto y no oculto con comando ls y ls -a.

En la figura del controlador, se muestran las interacciones entre las señales del sistema y los módulos `passwordSystem` y `gateSystem`. Las señales y su propósito son los siguientes:

- `P`: Contraseña proporcionada por el usuario, representada como un valor binario de 8 bits.
- `p_enter`: Señal de confirmación de entrada de la contraseña. Cuando se activa, el sistema procede a verificar la contraseña ingresada.

- `reset`: Señal utilizada para reiniciar el sistema y restablecer alarmas y contadores de intentos fallidos. Esta señal solo fue utilizada al principio y al final, para un inicio y finalización limpios.
- `sensor_arrival`: Sensor que detecta la llegada de un vehículo en la entrada del estacionamiento.
- `sensor_parked`: Sensor que detecta si un vehículo está estacionado y por lo tanto, si la compuerta debe permanecer cerrada.
- `S_L` (*Señal de Luz*): Señal de salida del módulo `passwordSystem` que indica si la contraseña proporcionada es correcta.
- `A_P` (*Alarma de Password*): Alarma que se activa cuando se ingresan tres contraseñas incorrectas consecutivas.
- `G_O`: Controla la apertura compuerta basándose en la validez de la contraseña y la señal del sensor de vehículo estacionado.
- `G_C`: Controla el cierre de la compuerta basándose en la validez de la contraseña y la señal del sensor de vehículo estacionado.
- `B`: Señal de bloqueo del sistema que se activa si se presenta una condición de error.
- `A_B` (*Alarma de Bloqueo*): Alarma que se activa cuando el sistema se encuentra en estado de bloqueo.

2.2. Diagrama de Bloques del funcionamiento de los archivos.

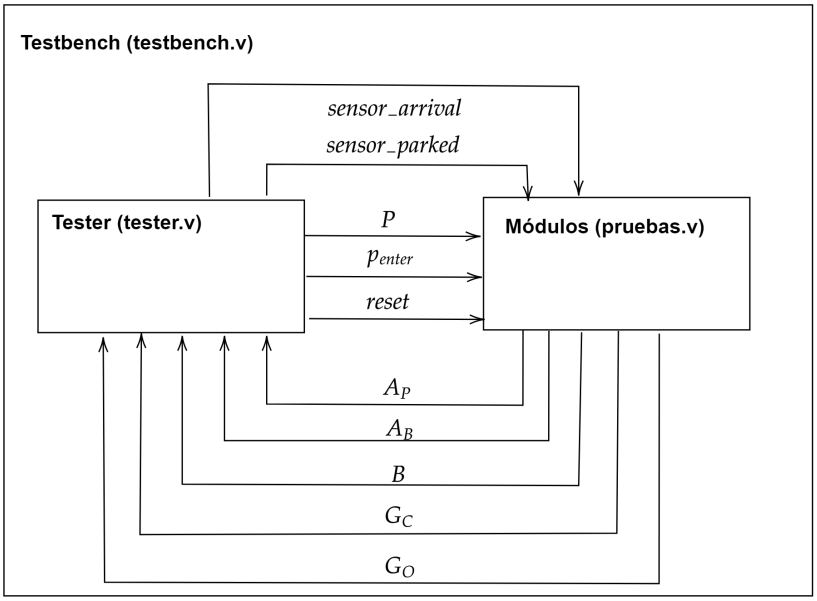

Figura 2: Diagrama de bloques de cómo los archivos se comunican.

2.3. Diagrama de estados.

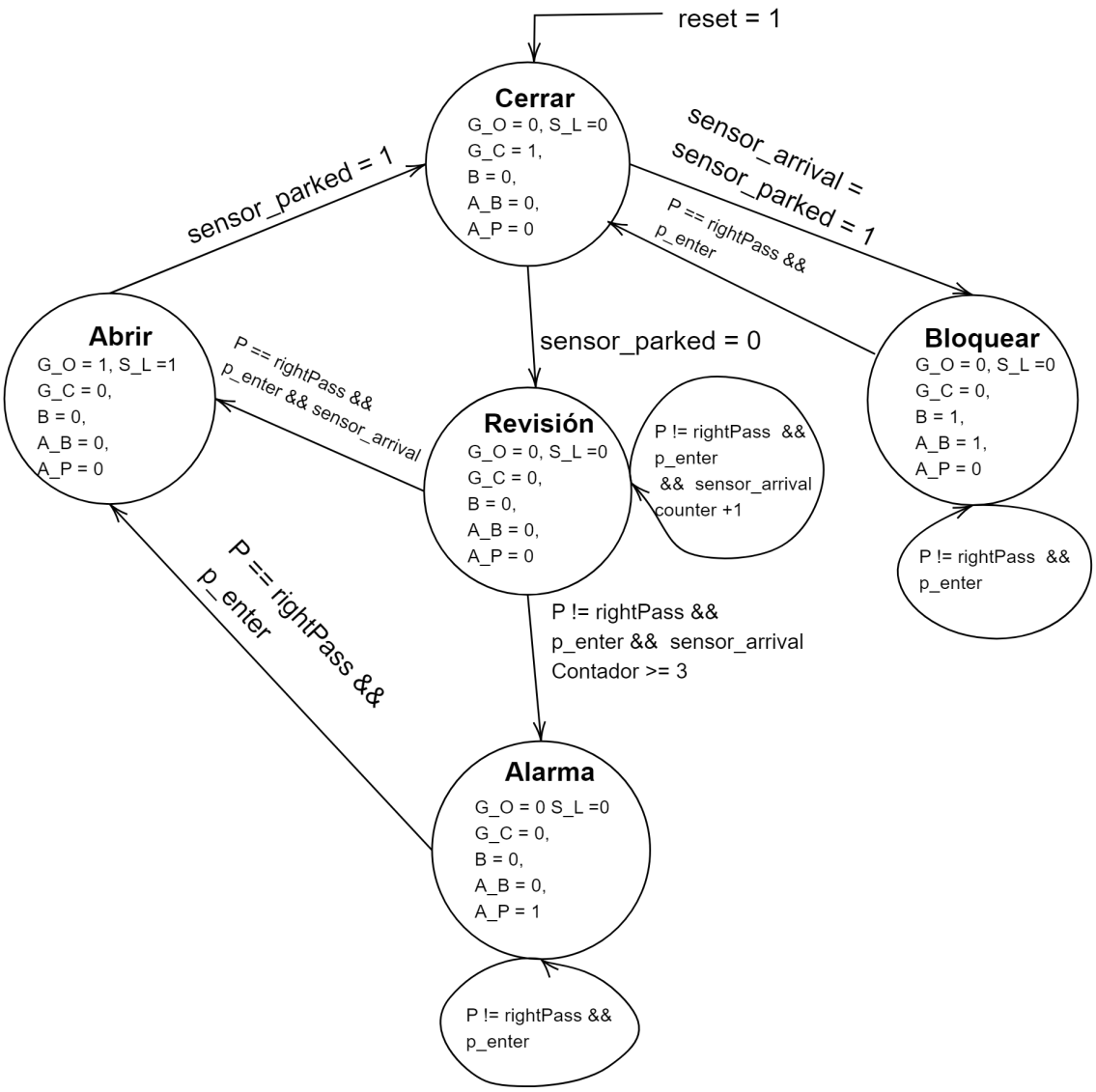

Figura 3: Diagrama de estados del sistema entero.

3. Plan de Pruebas.

El plan de pruebas se diseñó para validar el funcionamiento del controlador de acceso a estacionamiento automatizado. Se enumeran a continuación las pruebas realizadas, describiendo cada una con su propósito específico, los pasos ejecutados, y los resultados esperados. Se destaca que no se utilizó un *clock* para sincronizar las pruebas, aprovechando la respuesta inmediata que permite la lógica conductual del diseño frente a las señales de los sensores.

1. **Prueba #1: Funcionamiento normal básico.**

   - *Descripción:* Verificación de la funcionalidad básica del sistema con un vehículo que llega y proporciona una clave correcta.

- *Pasos:*
  i. Envío de pulso de reset.
  ii. Simulación de la llegada de un vehículo.
  iii. Ingreso de la clave correcta.
  iv. Actuación de la puerta para permitir el acceso al vehículo.
  v. Verificación del cierre de la puerta una vez estacionado el vehículo.
- *Resultado esperado:* El sistema abre y luego cierra la compuerta sin errores.

2. **Prueba #2: Ingreso de pin incorrecto menos de 3 veces.**

   - *Descripción:* Respuesta del sistema a intentos de acceso con clave incorrecta seguidos por el ingreso correcto de la misma.
   - *Pasos:*
     i. Reset del sistema.
     ii. Simulación de llegada de otro vehículo.
     iii. Dos intentos de acceso con claves incorrectas.
     iv. Ingreso de la clave correcta.
   - *Resultado esperado:* La compuerta permanece cerrada durante intentos incorrectos y se abre con el ingreso correcto.

3. **Prueba #3: Ingreso de pin incorrecto 3 o más veces.**

   - *Descripción:* Prueba de la activación de la alarma tras tres ingresos incorrectos consecutivos.
   - *Pasos:*
     i. Envío de pulso de reset.
     ii. Simulación de llegada de un nuevo vehículo.
     iii. Tres intentos consecutivos con claves incorrectas.
     iv. Ingreso de clave correcta para resetear la alarma.
   - *Resultado esperado:* Alarma activada tras tres intentos incorrectos y desactivada con el ingreso correcto.

4. **Prueba #4: Alarma de bloqueo.**

   - *Descripción:* Esta prueba evalúa la lógica de bloqueo del sistema cuando se detecta simultáneamente la llegada de un vehículo y un vehículo estacionado, una condición que no debería ocurrir bajo operación normal y que, por lo tanto, debe activar una alarma de bloqueo.
   - *Pasos:*
     i. Se envía un pulso de reset para inicializar el sistema.
     ii. Se simula la llegada de un vehículo mientras ningún vehículo está estacionado.
     iii. Se activan ambos sensores para simular una situación de bloqueo.
     iv. Se introduce una contraseña incorrecta manteniendo el estado de bloqueo.

v. Luego se ingresa la contraseña correcta para verificar que el sistema se desbloquee correctamente.

vi. Se desactiva el sensor de llegada y se espera para simular que el vehículo ya no está llegando.

vii. Finalmente, se simula la salida del vehículo estacionado para restablecer el sistema y prepararlo para la siguiente entrada.

viii. Se simula la prueba número 1 y debe funcionar con normalidad.

- *Resultado esperado:* El sistema debe reconocer una condición anormal y activar la alarma de bloqueo. Después de ingresar la contraseña correcta, el sistema debe desbloquearse, lo cual se verifica al permitir la entrada del siguiente vehículo sin activar la alarma de bloqueo.

Cada prueba fue ejecutada de manera aislada para verificar las reacciones específicas del controlador y asegurar cobertura total de todos los escenarios posibles. Las simulaciones se realizaron utilizando herramientas estándar como Icarus Verilog para observar el comportamiento del sistema ante cada conjunto de entradas.

4. Instrucciones de utilización de la simulación.

4.1. Comandos Necesarios.

El proceso de compilación y simulación de los módulos de lógica combinacional contenidos en `pruebas.v` se puede realizar manualmente a través de una serie de comandos en la terminal. Los pasos a seguir son los siguientes:

1. Compilar el testbench y los módulos de diseño con Icarus Verilog:

```
iverilog -o simulation testbench.v pruebas.v tester.v
```

2. Ejecutar la simulación para generar el archivo de ondas (`.vcd`):

```
vvp simulation
```

3. Abrir el archivo de ondas con GTKWave para visualizar la simulación:

```
gtkwave test.vcd C16042gtkwaveTarea1.gtkw
```

En caso de querer reiniciar el proceso, se deberán eliminar los archivos generados por la compilación y simulación con el comando:

```
rm -f simulation test.vcd
```

4.2. Makefile.

Para facilitar el proceso de compilación y simulación, se ha proporcionado un `Makefile`. Para ejecutar todos los comandos automáticamente, se debe correr el comando `make` en la terminal. Este comando compilará el testbench y los módulos de diseño, ejecutará la simulación para generar el archivo de ondas y abrirá GTKWave con la configuración predefinida para visualizar los resultados. Luego de revisar las ondas y cuando se desee limpiar el directorio de trabajo, se usa el comando `make clean` para eliminar todos los archivos generados durante la compilación y la simulación.

5. Ejemplos de los resultados.

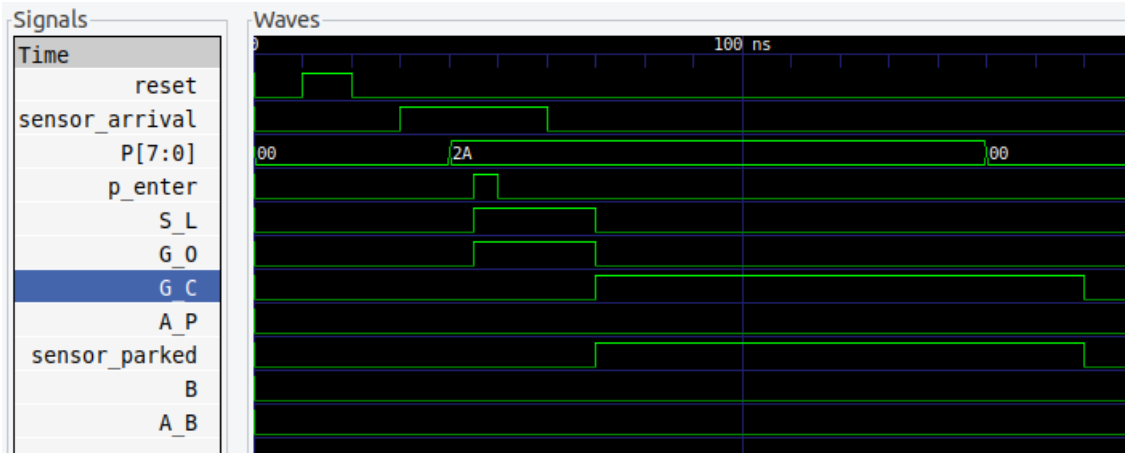

Figura 4: Prueba número 1, funcionamiento normal básico.

Durante la **Prueba #1**, el sistema se inicia sin ninguna señal activa, reflejando un estado inactivo inicial. Se emite un pulso de `reset` de manera breve; aunque no ejerce un cambio en el sistema ya que no existen errores o alarmas que resetear, su activación es por formalidad para garantizar un inicio limpio. A continuación, se activa la señal `sensor_arrival`, imitando la detección de un vehículo entrante. Seguidamente se introduce la contraseña correcta (`P[7:0]`), y con un pulso en `p_enter`, se produce la activación de la señal `S_L`, lo que señala que la contraseña ha sido verificada correctamente y que el sistema autoriza la entrada. Como consecuencia, la compuerta se abre (`G_O` se hace alto), facilitando el acceso del vehículo. A lo largo de esta secuencia, las alarmas (`A_P` por intentos fallidos y `A_B` por bloqueo) así como la señal de bloqueo (`B`) se mantienen inactivas, denotando un comportamiento adecuado debido a la ausencia de condiciones de error o bloqueo. Finalmente, la señal `sensor_parked` se activa haciendo que la señal `G_C` se active y que la señal `S_L` y `G_O` se hagan 0.

Figura 5: Prueba número 2, ingreso de pin incorrecto menos de 3 veces.

En la **Prueba #2**, se verifica la robustez del sistema ante intentos de acceso no autorizados. Se inicia la prueba con el sistema en reposo y se activa la señal `sensor_arrival` para simular la llegada de un vehículo. Procedemos con el ingreso de una primera contraseña incorrecta (`7F`), seguida de un pulso en `p_enter`. Como se espera, la señal `S_L` no se activa, indicando que el sistema deniega el acceso. A continuación, se introduce una segunda contraseña errónea (`F7`) y se pulsa `p_enter` una vez más. La inactividad de `S_L` y el hecho de que `G` permanezca en estado bajo confirman que la seguridad del sistema no se ve comprometida a pesar de múltiples intentos de acceso con contraseñas incorrectas. Las alarmas `A_P` y `A_B`, así como la señal de bloqueo `B`, se mantienen inalteradas, evidenciando que no se ha llegado al umbral necesario para activar una alerta. Luego, en el tercer intento, el usuario coloca bien la contraseña, haciendo que `S_L` y `G_O` se activen, y justo cuando `sensor_parked` se activa, las señales `S_L` y `G_O` se vuelven a hacer 0.

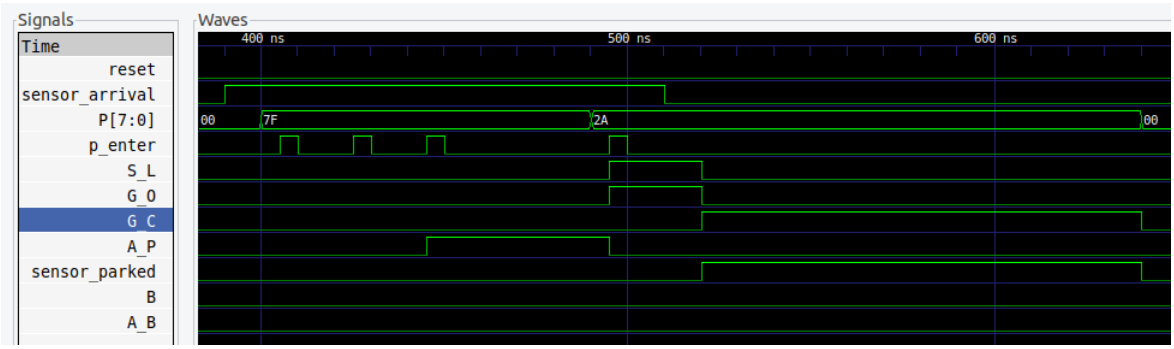

Figura 6: Prueba número 3, ingreso de pin incorrecto 3 o más veces.

En la **Prueba #3**, se verifica que se inserte la misma contraseña incorrecta 3 veces, y que al darle 3 veces a `p_enter`, se active la señal de alarma `A_P`, lo cual sucede. Luego, en el cuarto intento, el usuario coloca bien la contraseña, haciendo que `A_P` se apague, `S_L` y `G` se activen, y justo cuando `sensor_parked` y `G_C` se activan, las señales `S_L` y `G_O` se vuelven a hacer 0.

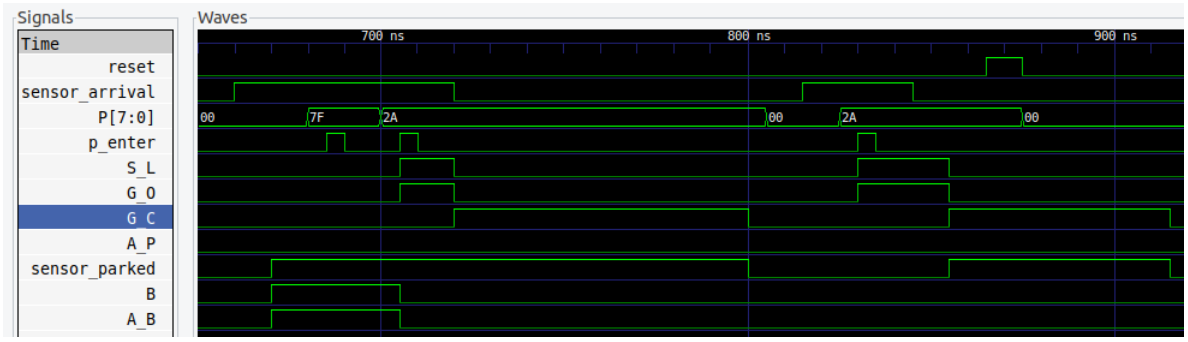

Figura 7: Prueba número 4, alarma de bloqueo.

En la **Prueba #4**, se verifica el sistema de bloqueo, donde los 2 sensores `sensor_arrival` y `sensor_parked`) están activos al mismo tiempo. Como se esperó, las señales `B` y `A_B` se activan hasta que el usuario coloque la contraseña correcta y pulse la señal `p_enter`. Luego de los 800 ns, se vuelve a hacer la prueba número 1, donde todo funcionó con normalidad. Por último se aplica un reset por formalidad.

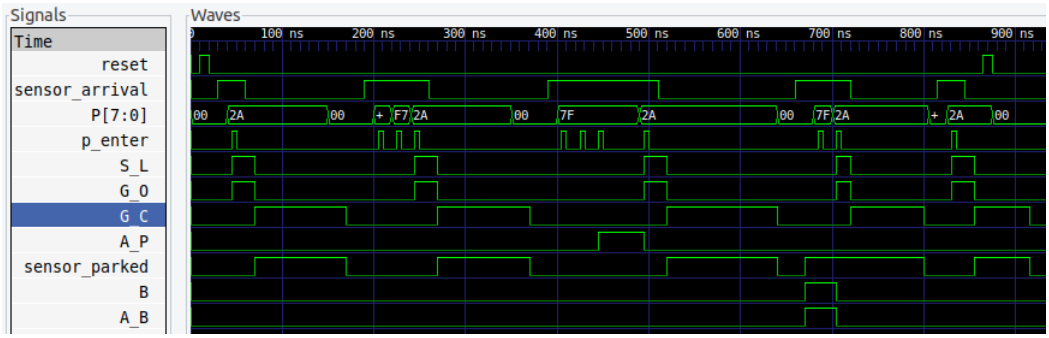

Figura 8: Simulación completa del sistema.

6. Retos y complicaciones durante la solución.

Uno de los retos más complicados durante la solución fue lograr que a pesar de que se intentaba probar la misma contraseña inválida, el contador de intentos no aumentaba. Esto se dio a que como la señal de ingreso de contraseña no cambiaba, el módulo pensaba que se mantenía constante, por lo que el contador se mantenía en 1. Para solucionarlo se decidió crear la señal p_enter, similar a un botón de enter para confirmar el valor deseado. Esto solucionó el problema tanto para valores distintos como iguales para la contraseña.

7. Conclusiones y recomendaciones.

A través de las pruebas realizadas, se ha demostrado que el sistema de control de acceso cumple eficientemente con los requisitos establecidos. Durante la **Prueba #1**, se verificó el correcto funcionamiento del sistema ante la entrada válida de un vehículo, donde las señales `S_L` y `G` (O y C) respondieron como se esperaba. La **Prueba #2** confirmó la seguridad del sistema al denegar el acceso con contraseñas incorrectas y validar correctamente la entrada con la contraseña adecuada. En la **Prueba #3**, el sistema demostró su capacidad para detectar y reaccionar ante intentos de acceso fallidos repetidos, activando la alarma correspondiente, lo

cual resalta la efectividad del mecanismo de alarma `A_P`. La **Prueba #4** ejerció con éxito la lógica de bloqueo ante la activación simultánea de ambos sensores, lo cual es una condición anómala, y el sistema mostró un comportamiento adecuado.

Las recomendaciones para futuros desarrollos o mejoras incluyen:

- Implementar un sistema de log que registre los intentos de acceso, tanto exitosos como fallidos, para un seguimiento detallado de la seguridad.
- Considerar la incorporación de un temporizador que limite el tiempo de respuesta tras la activación de `sensor_arrival`, para mejorar la eficiencia del sistema.
- Evaluar la integración de un mecanismo de respaldo que permita el acceso en casos de emergencia, aun cuando el sistema principal falle.