

# Diseño y Construcción de una Computadora de Vuelo para Vehículos Autónomos con Tolerancia a Fallas

Federico Ignacio Nuñez Frau - 98211

Director: Dr. Ing. Claudio Pose (FIUBA)

Co-Director: Ing. Leonardo Garberoglio (UTN-FRSN)

DD/MM/2024



# Contenidos

- 1 Introducción y Motivación**
- 2 Sistemas Tolerantes a Fallas**
- 3 Diseño y Construcción de la Computadora de Vuelo**
- 4 Sistema Implementado**
- 5 Resultados**
- 6 Conclusiones**

# Introducción y Motivación

# Vehículos Autónomos

# Vehículos Autónomos

- Los vehículos autónomos no cuentan con una tripulación ni un piloto a bordo. Estos son comandados de forma remota, o bien tienen la capacidad de hacerlo por sí solos.

# Vehículos Autónomos

- Los vehículos autónomos no cuentan con una tripulación ni un piloto a bordo. Estos son comandados de forma remota, o bien tienen la capacidad de hacerlo por sí solos.
- Gran variedad de sensores + computadora central = sistema de navegación y reconocimiento del entorno.

# Vehículos Autónomos

- Los vehículos autónomos no cuentan con una tripulación ni un piloto a bordo. Estos son comandados de forma remota, o bien tienen la capacidad de hacerlo por sí solos.
- Gran variedad de sensores + computadora central = sistema de navegación y reconocimiento del entorno.



# Vehículos Autónomos

- Originalmente desarrollados para uso en aplicaciones militares.

# Vehículos Autónomos

- Originalmente desarrollados para uso en aplicaciones militares.



# Vehículos Autónomos

- Originalmente desarrollados para uso en aplicaciones militares.
- Desarrollo y mantenimiento menos costoso frente a vehículos tripulados.



# Vehículos Autónomos

- Originalmente desarrollados para uso en aplicaciones militares.
- Desarrollo y mantenimiento menos costoso frente a vehículos tripulados.
- Motivación: Realizar tareas que de otra forma pondrían en riesgo a la tripulación.



# Vehículos Autónomos



# Vehículos Autónomos

- Cada vez tienen mayor presencia en zonas civiles.
  
- COMPLETAR CON EJEMPLOS DE ACCIDENTES DE DRONES

# Vehículos Autónomos

- Cada vez tienen mayor presencia en zonas civiles.
- La incorporación de drones permite realizar tareas costosas, riesgosas o críticas de forma segura.
  
- COMPLETAR CON EJEMPLOS DE ACCIDENTES DE DRONES

# Vehículos Autónomos

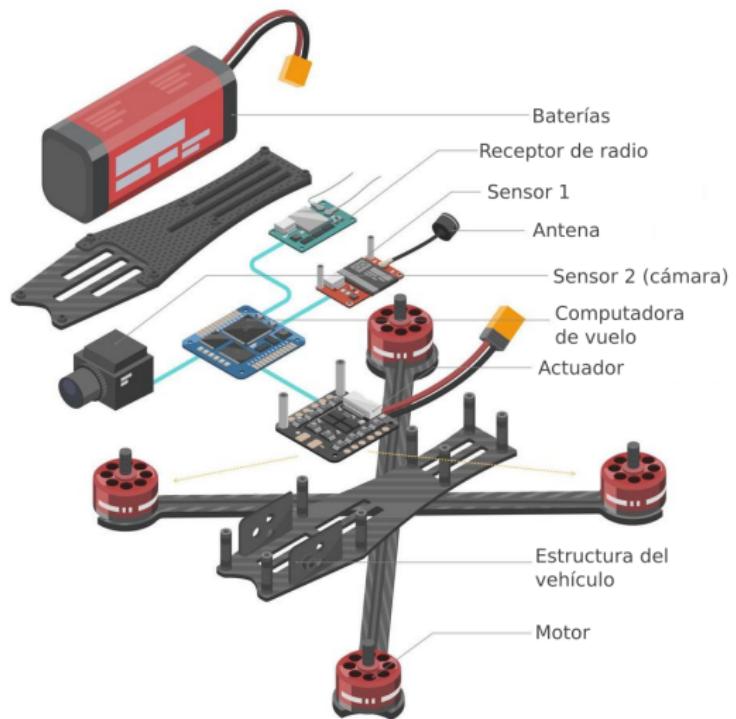
- Cada vez tienen mayor presencia en zonas civiles.
- La incorporación de drones permite realizar tareas costosas, riesgosas o críticas de forma segura.
- Teniendo esto en cuenta, la confiabilidad es un aspecto que toma mayor relevancia.
- COMPLETAR CON EJEMPLOS DE ACCIDENTES DE DRONES

# Computadora de Vuelo

- Los drones se componen de varios elementos.

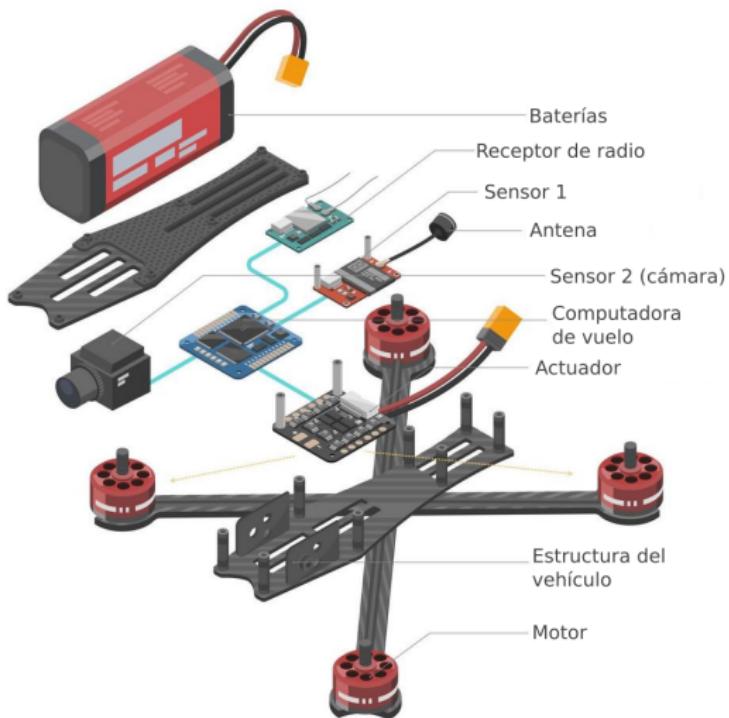
# Computadora de Vuelo

- Los drones se componen de varios elementos.



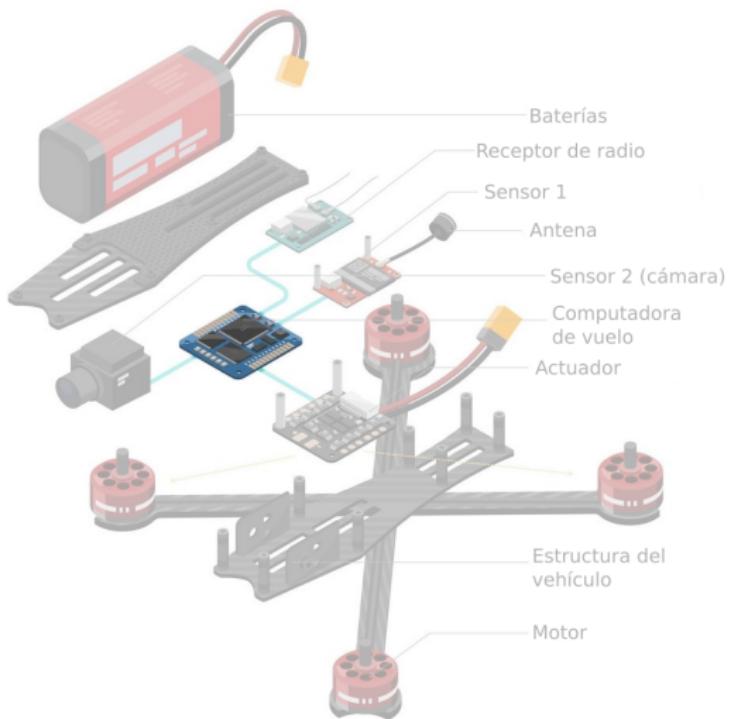
# Computadora de Vuelo

- Los drones se componen de varios elementos.
- Todos ellos son susceptible de manifestar fallas.



# Computadora de Vuelo

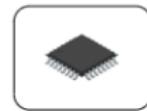
- Los drones se componen de varios elementos.
- Todos ellos son susceptible de manifestar fallas.
- En este trabajo se abordan aspectos relacionados a la **computadora de vuelo**.



# Computadora de Vuelo

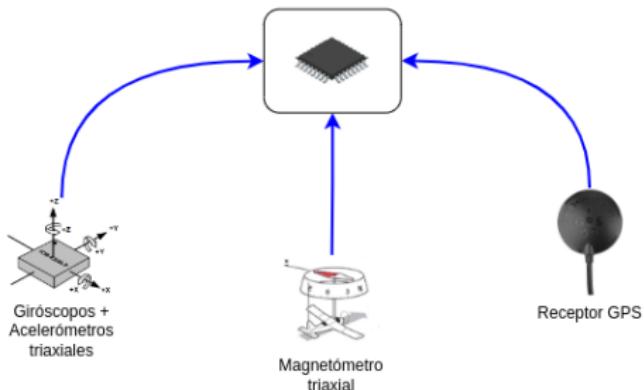
# Computadora de Vuelo

- Se encarga de ejecutar los algoritmos de guiado, navegación y control para estabilizar el vehículo y guiarlo en su trayectoria.



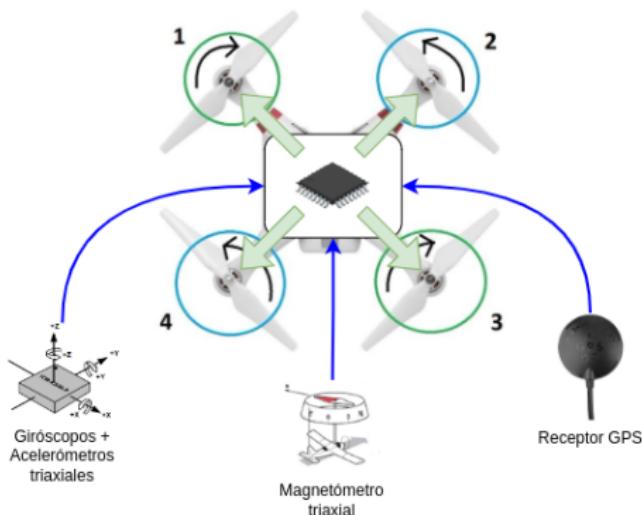
# Computadora de Vuelo

- Se encarga de ejecutar los algoritmos de guiado, navegación y control para estabilizar el vehículo y guiarlo en su trayectoria.
- Adquiere datos de los sensores del vehículo.



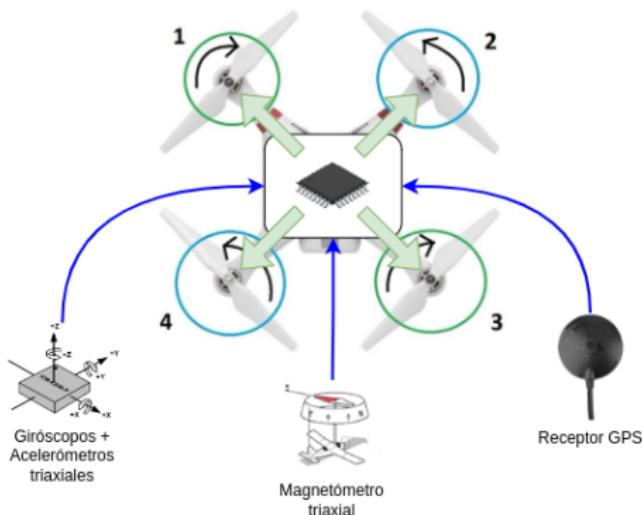
# Computadora de Vuelo

- Se encarga de ejecutar los algoritmos de guiado, navegación y control para estabilizar el vehículo y guiarlo en su trayectoria.
- Adquiere datos de los sensores del vehículo.
- Actúa sobre los motores.



# Computadora de Vuelo

- Se encarga de ejecutar los algoritmos de guiado, navegación y control para estabilizar el vehículo y guiarlo en su trayectoria.
- Adquiere datos de los sensores del vehículo.
- Actúa sobre los motores.
- La computadora de vuelo es el elemento central en un vehículo aéreo no tripulado.



# Tolerancia a Fallas

- Cada vez tienen mayor presencia en zonas civiles.

# Tolerancia a Fallas

- Cada vez tienen mayor presencia en zonas civiles.
- Teniendo esto en cuenta, la **confiabilidad** es un aspecto que toma mayor relevancia.

# Tolerancia a Fallas

- Cada vez tienen mayor presencia en zonas civiles.
- Teniendo esto en cuenta, la **confiabilidad** es un aspecto que toma mayor relevancia.
- En vehículos aéreos como aviones comerciales y militares se utilizan técnicas de **tolerancia a fallas**.

# Tolerancia a Fallas

- Cada vez tienen mayor presencia en zonas civiles.
- Teniendo esto en cuenta, la **confiabilidad** es un aspecto que toma mayor relevancia.
- En vehículos aéreos como aviones comerciales y militares se utilizan técnicas de **tolerancia a fallas**.



# Tolerancia a Fallas

- Cada vez tienen mayor presencia en zonas civiles.
- Teniendo esto en cuenta, la **confiabilidad** es un aspecto que toma mayor relevancia.
- En vehículos aéreos como aviones comerciales y militares se utilizan técnicas de **tolerancia a fallas**.
- También en drones de uso militar.



# Tolerancia a Fallas

- Cada vez tienen mayor presencia en zonas civiles.
- Teniendo esto en cuenta, la **confiabilidad** es un aspecto que toma mayor relevancia.
- En vehículos aéreos como aviones comerciales y militares se utilizan técnicas de **tolerancia a fallas**.
- También en drones de uso militar.



- El aspecto más importante en aviones comerciales:  $10^{-9}/h$  de vuelo.

# Tolerancia a Fallas

- Cada vez tienen mayor presencia en zonas civiles.
- Teniendo esto en cuenta, la **confiabilidad** es un aspecto que toma mayor relevancia.
- En vehículos aéreos como aviones comerciales y militares se utilizan técnicas de **tolerancia a fallas**.
- También en drones de uso militar.



- El aspecto más importante en aviones comerciales:  $10^{-9}/h$  de vuelo.
- Aviones militares:  $10^{-7}/h$  de vuelo.

# Tolerancia a Fallas

- Cada vez tienen mayor presencia en zonas civiles.
- Teniendo esto en cuenta, la **confiabilidad** es un aspecto que toma mayor relevancia.
- En vehículos aéreos como aviones comerciales y militares se utilizan técnicas de **tolerancia a fallas**.
- También en drones de uso militar.



- El aspecto más importante en aviones comerciales:  $10^{-9}/h$  de vuelo.
- Aviones militares:  $10^{-7}/h$  de vuelo.
- Drones militares:  $10^{-5}/h$  de vuelo.

# Tolerancia a Fallas

- Cada vez tienen mayor presencia en zonas civiles.
- Teniendo esto en cuenta, la **confiabilidad** es un aspecto que toma mayor relevancia.
- En vehículos aéreos como aviones comerciales y militares se utilizan técnicas de **tolerancia a fallas**.
- También en drones de uso militar.



- El aspecto más importante en aviones comerciales:  $10^{-9}/h$  de vuelo.
- Aviones militares:  $10^{-7}/h$  de vuelo.
- Drones militares:  $10^{-5}/h$  de vuelo.
- ¿Drones civiles/comerciales?

# Objetivos

- 1 Estudiar** las características de los sistemas con tolerancia a fallas aplicados en vehículos aéreos, tanto tripulados como no tripulados.
- 2 Entender** los requerimientos para implementar un sistema con tolerancia a fallas.
- 3 Diseñar** una computadora de vuelo para vehículos aéreos no tripulados, para ser enviada a fabricar.
- 4 Desarrollar** un firmware que demuestre la capacidad de ser utilizada en un sistema con tolerancia a fallas.

# Sistemas Tolerantes a Fallas

# Confiabilidad

## Confiabilidad

Probabilidad de que un sistema pueda cumplir con su función de manera correcta en un intervalo de tiempo  $[t_0; t]$ , dado que sí podía hacerlo en  $t_0$ .

- $R(t) = \mathbb{P}(\text{no ocurra ninguna falla en } [t_0; t])$
- Incrementar esta probabilidad equivale a incrementar la confiabilidad.
- Se busca **evitar** la ocurrencia de fallas en el sistema.
- Esto tiene algunos inconvenientes:
  - 1 Uso de componentes que pueden ser muy costosos.
  - 2 Dificultades en la etapa de diseño del sistema.
  - 3 Errores de diseño no tenidos en cuenta pueden llegar a causar fallas.

# Tolerancia a Fallas

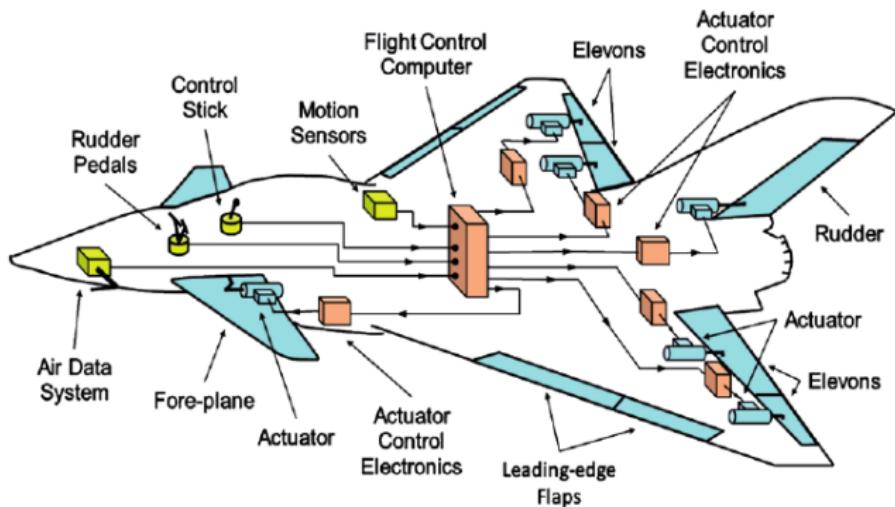
- Una decisión más conservadora consiste en **tolerar** fallas.

## Sistema Tolerante a Fallas

No es aquel donde no ocurren fallas. Al contrario, se acepta que las fallas pueden ocurrir. En consecuencia, incluyen mecanismos para que, a pesar de la ocurrencia de una falla, el sistema pueda seguir cumpliendo su función.

- Una de las técnicas más comunes es el uso de **redundancias**.
- Esta consiste en el uso de varias réplicas que realicen las mismas tareas dentro del sistema.
- Por ejemplo, sensores, actuadores, computadoras de vuelo, etc.

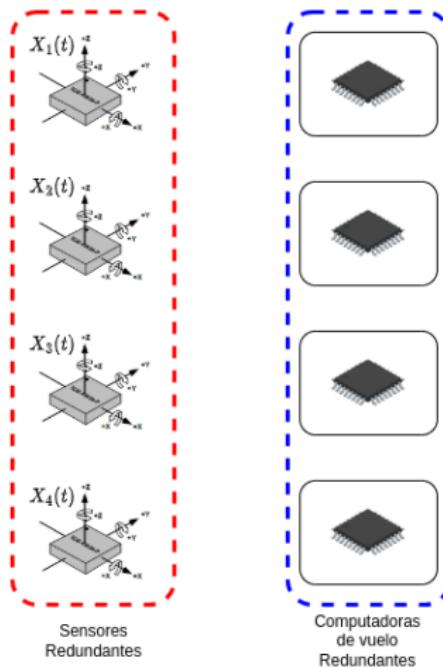
# Tolerancia a Fallas: Avión



- Sensores x4
- Actuadores x4
- Computadora de vuelo x4

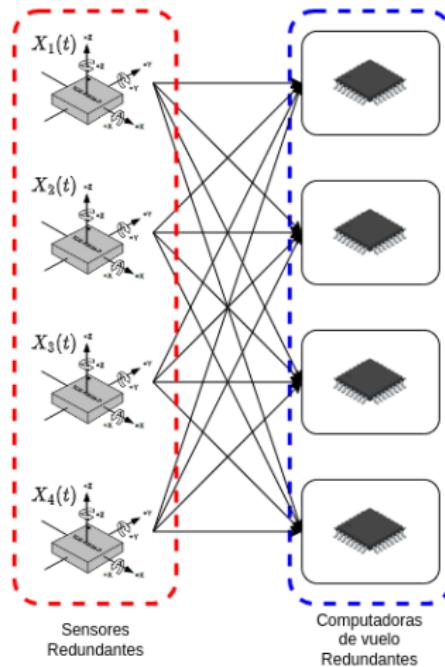
# Tolerancia a Fallas: Avión

# Tolerancia a Fallas: Avión



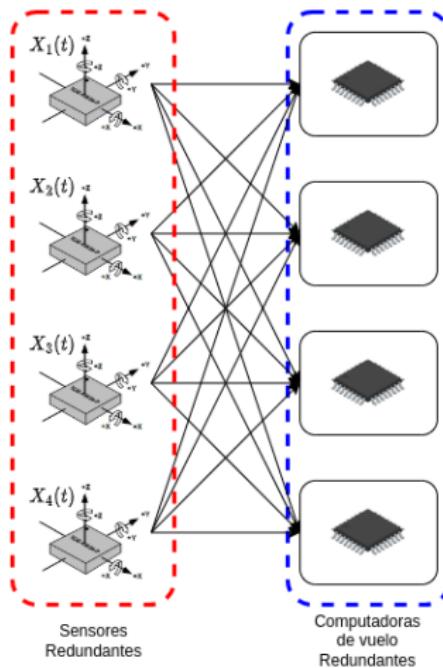
# Tolerancia a Fallas: Avión

- Todas las computadoras de vuelo adquieren datos de **todos** los sensores redundantes.



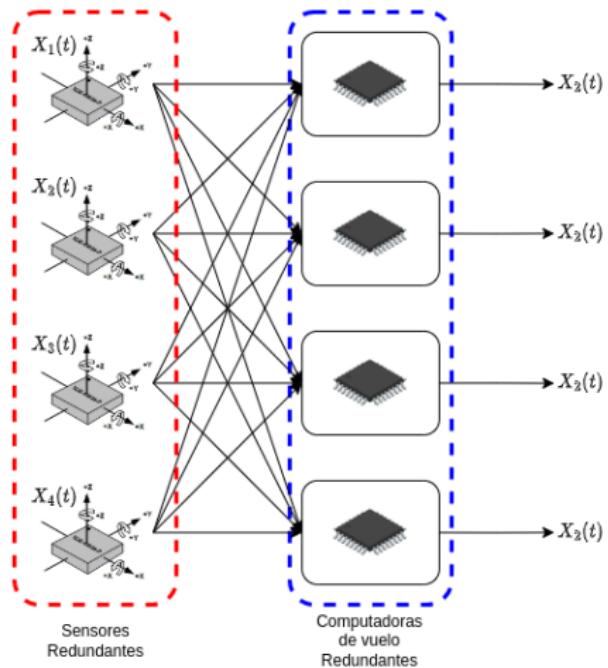
# Tolerancia a Fallas: Avión

- Todas las computadoras de vuelo adquieren datos de **todos** los sensores redundantes.
- A partir de la **comparación de valores**, se detectan fallas de los sensores.



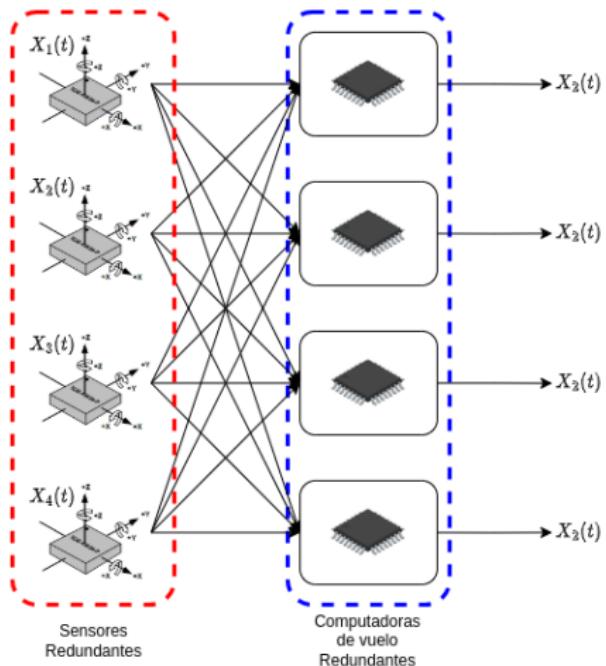
# Tolerancia a Fallas: Avión

- Todas las computadoras de vuelo adquieren datos de **todos** los sensores redundantes.
- A partir de la **comparación de valores**, se detectan fallas de los sensores.
- Para tolerar la falla, cada computadora de vuelo selecciona **un único valor**.

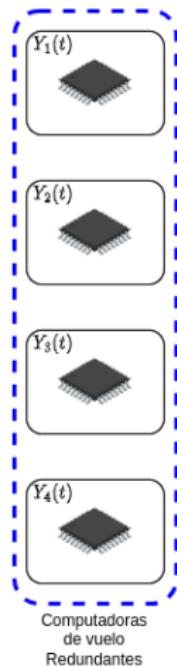


# Tolerancia a Fallas: Avión

- Todas las computadoras de vuelo adquieren datos de **todos** los sensores redundantes.
- A partir de la **comparación de valores**, se detectan fallas de los sensores.
- Para tolerar la falla, cada computadora de vuelo selecciona **un único valor**.
- Para ello hay un intercambio entre las 4 computadoras de vuelo.

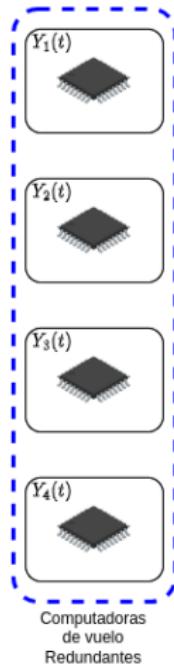


# Tolerancia a Fallas: Avión



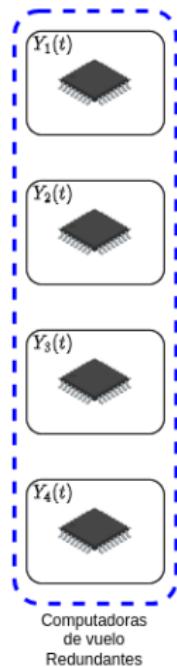
# Tolerancia a Fallas: Avión

- Se calcula la señal a aplicar a los actuadores.



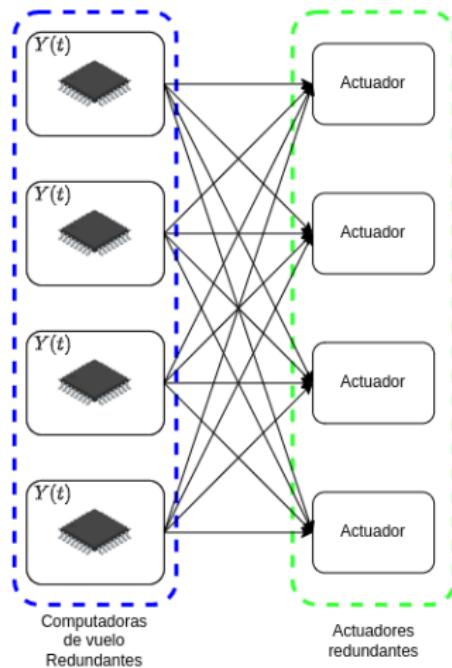
# Tolerancia a Fallas: Avión

- Se calcula la señal a aplicar a los actuadores.
- Se realiza un nuevo intercambio para tolerar fallas de las computadoras de vuelo.



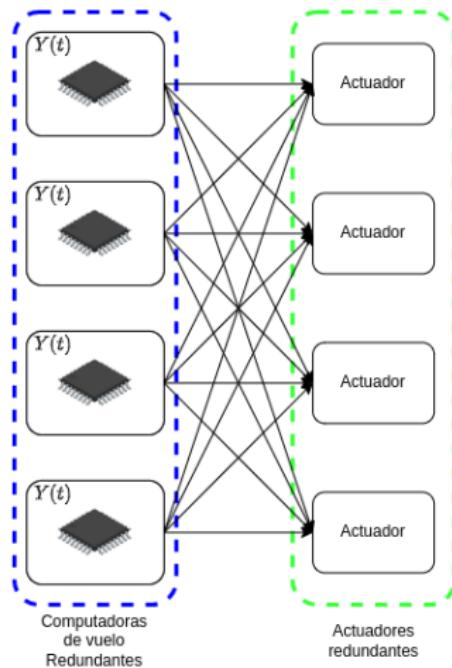
# Tolerancia a Fallas: Avión

- Se calcula la señal a aplicar a los actuadores.
- Se realiza un nuevo intercambio para tolerar fallas de las computadoras de vuelo.
- Se decide por **un único valor** de señal  $Y(t)$ .

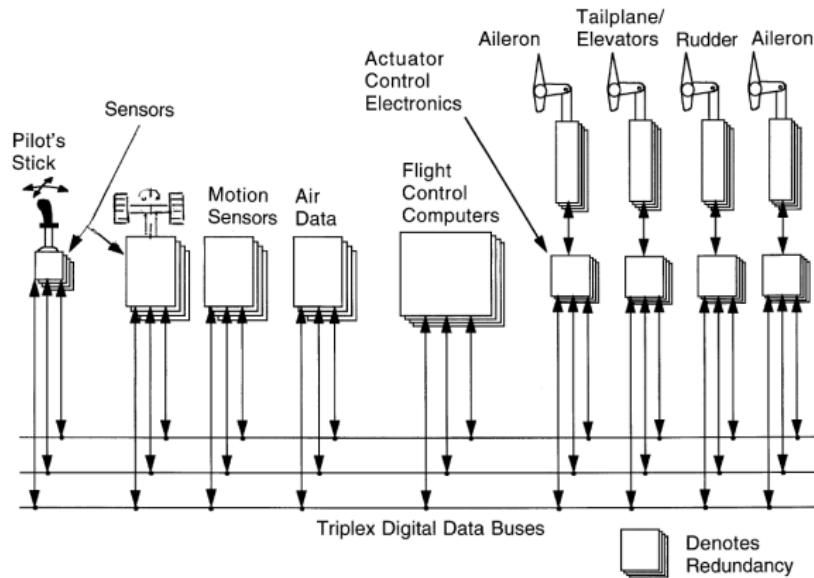


# Tolerancia a Fallas: Avión

- Se calcula la señal a aplicar a los actuadores.
- Se realiza un nuevo intercambio para tolerar fallas de las computadoras de vuelo.
- Se decide por **un único valor** de señal  $Y(t)$ .
- Se aplica la señal a los actuadores.



# Tolerancia a Fallas: Avión



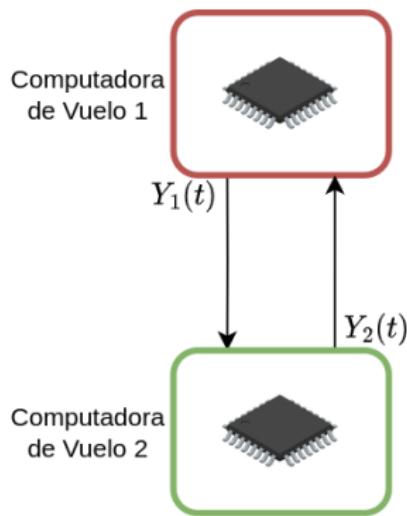
- Se utiliza un **bus de comunicaciones** redundante.
- Acceso al medio por turnos: *time-division multiple access*.

# Tolerancia a Fallas: Drones

- Existen algunas computadoras de vuelo comerciales que ofrecen la posibilidad de trabajar con redundancias.
- Sin embargo sus costos son muy elevados.
- Pueden encontrarse varios trabajos de computadoras de vuelo redundantes que utilizan componentes económicos y accesibles.
- Los trabajos que se tomaron como referencia utilizan configuraciones variadas: redundancia doble, triple y cuádruple.
- Se mencionan las características comunes.

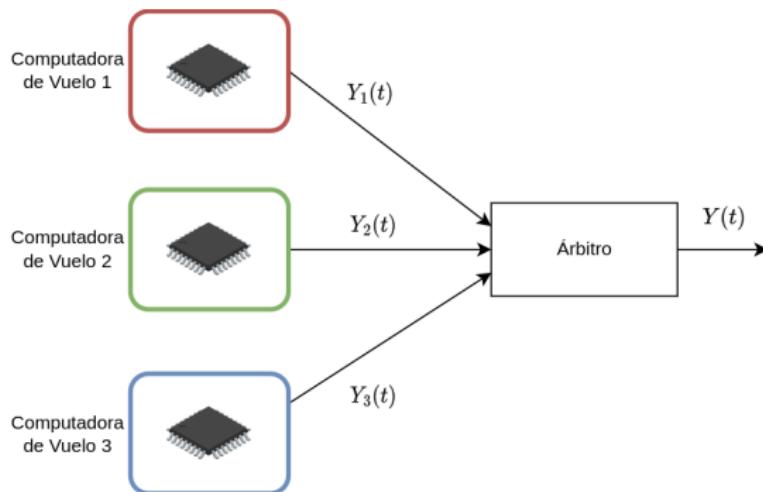
# Tolerancia a Fallas: Redundancia Doble

- Configuración Simple.
- La comparación permite detectar si ocurrió una falla o no.
- Pero **no se puede saber cuál de ellas lo hizo!**
- Cada réplica debería ejecutar una rutina para detectar la falla.
- Esto puede perjudicar el determinismo temporal del sistema de control.



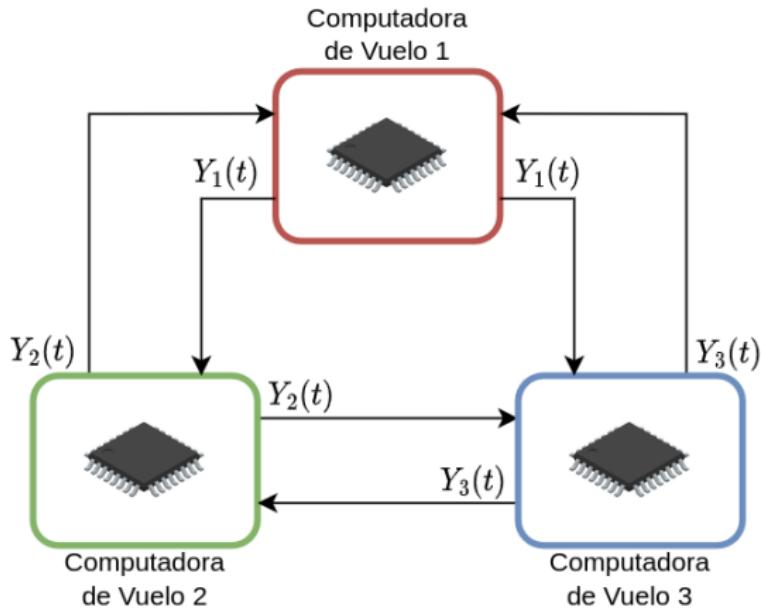
# Tolerancia a Fallas: Redundancia Triple

- Se asume que una sola de ellas fallará de forma simultánea.
- La comparación sí permite detectar cuál falló: 2 de 3.
- Punto Singular de Falla: ¿Qué sucede si falla el Árbitro?
- Este debe ser altamente confiable, volviéndolo muy costoso.



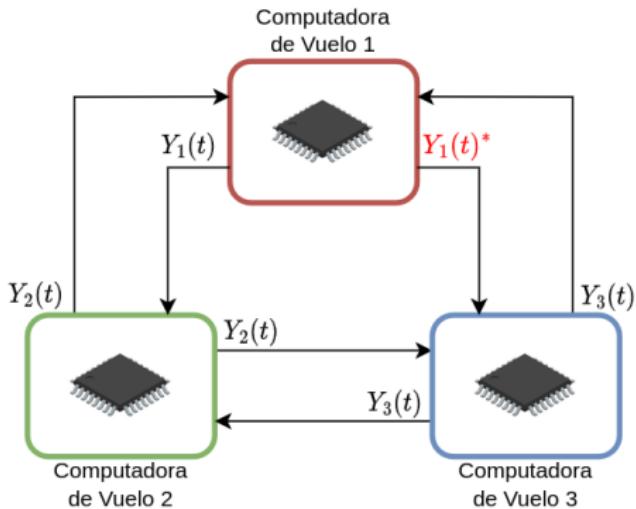
# Tolerancia a Fallas: Redundancia Triple

- Puede eliminarse el árbitro utilizando la siguiente configuración.
- Esta configuración es como la del caso del avión.



# Problema del Consenso

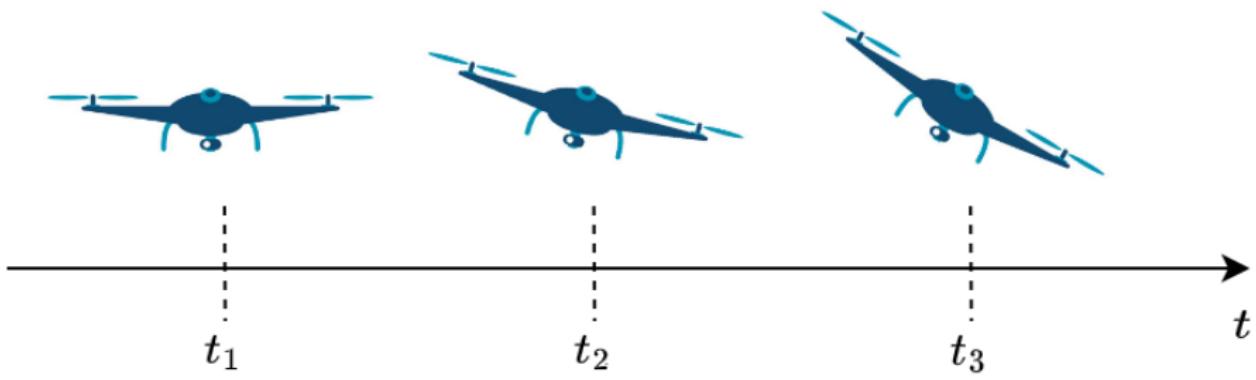
- Si todas las réplicas utilizan los mismos valores de entrada.
- Entonces llegan a la misma conclusión acerca del valor seleccionado.
- Que pasa si...



- La configuración no tolera este comportamiento.
- Este problema se denomina: *The Byzantine General's Problem*.
- Leslie Lamport, Rober Shostak y Marshall Pease, 1982.
- Se requieren  $3m + 1$  réplicas para tolerar  $m$  “traidores”.

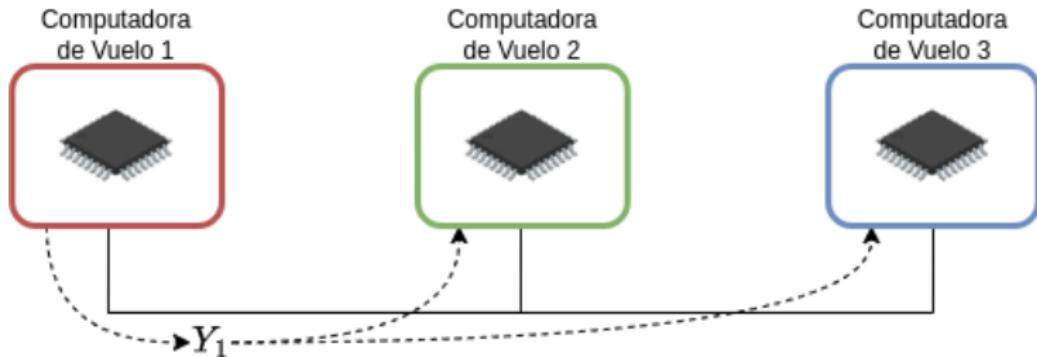
# Problema del Sincronismo

- Las tareas de estimación de la pose del vehículo, y de cálculo de la señal a aplicar sobre los motores tienen requerimientos temporales fuertes.
- Periódicamente debe obtenerse un nuevo valor, acorde al estado en el que se encuentra el vehículo para mantenerlo estable y guiarlo.
- Para que las comparaciones entre réplicas tengan sentido, los resultados deben corresponder al mismo instante temporal.
- Esto se logra a través de una **sincronización** entre las réplicas.



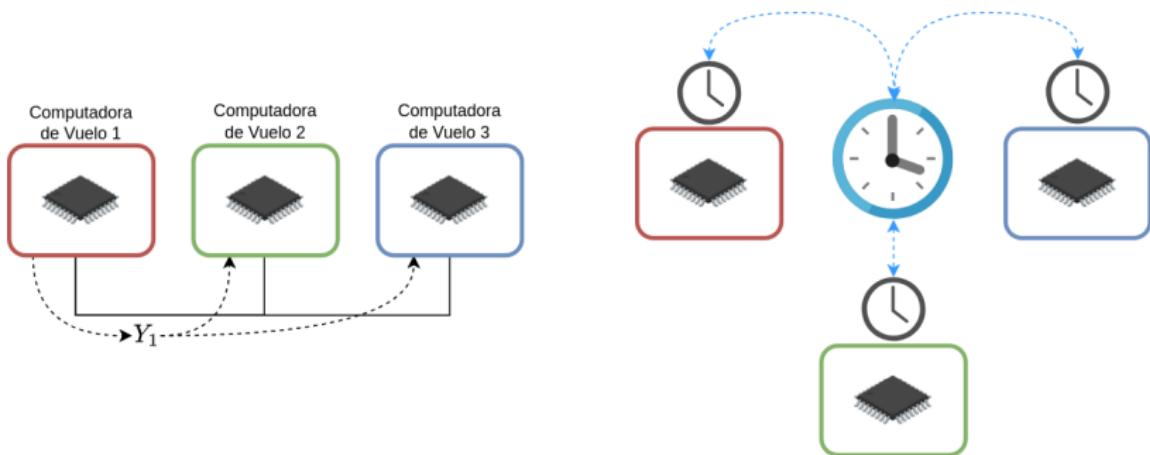
# Solución Sencilla: Bus de Comunicaciones + Sincronización

- Una solución sencilla es utilizar un bus de comunicaciones.
- Cada mensaje es recibido por todas las réplicas.
- No hay “traidores”.
- Las colisiones pueden perjudicar el determinismo.
- Se aprovecha la sincronización para ordenar el uso del bus, acceso al medio TDMA.
- Esto es lo que ocurría en el caso del avión.



# Requerimientos del Sistema

- 1 Uso de un bus de comunicaciones.
- 2 Funcionamiento sincronizado de las réplicas.



# Diseño y Construcción de la Computadora de Vuelo

# Sistema Implementado

# Resultados

# Conclusiones