Resiliencia en Sistemas Computacionales Complejos

Pedro R. D'Argenio

Dependable Systems Group
FaMAF, UNC - CONICET

http://dsg.famaf.unc.edu.ar

CONICET

Conferencia Gaviola, Noviembre 2015

UNC

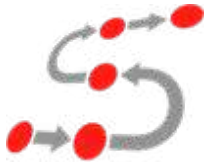
Resiliencia en Sistemas Computacionales Complejos

Pedro R. D'Argenio

Grupo de Sistemas Confiables
FaMAF, UNC - CONICET

http://dsg.famaf.unc.edu.ar

CONICET



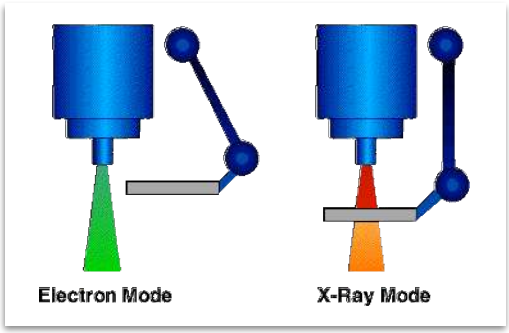
UNC

Conferencia Gaviola, Noviembre 2015

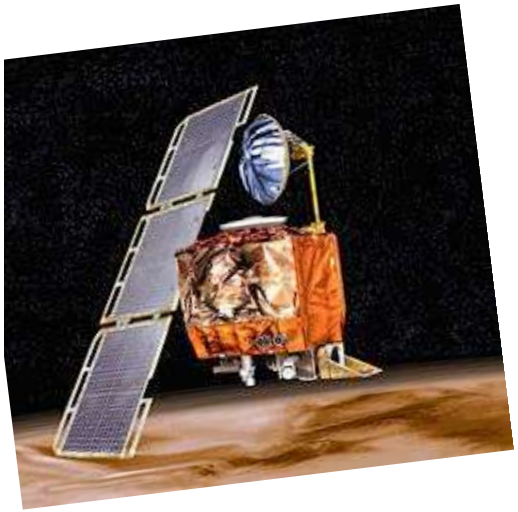
El problema de la corrección

Pentium:
FDIV

Ariane 5:
64 bits fp
vs 16 bits int



Therac-25:
Condición de
carrera



Mars Climate
Orbiter:
Métrico vs Imperial

Northeast blackout
en 2003:
Condición de carrera

Heartbleed:
Integridad/Confidencialidad

CONICET

UNC

El problema de la corrección

$$\mathit{Propiedad} \models \mathit{Sistema}$$

Describe lo que se espera del sistema (el criterio de corrección)

Usualmente una abstracción que describe su comportamiento

El problema de la corrección

$$Propiedad \models Sistema$$

Describe lo que se espera del sistema (el criterio de corrección)

Usualmente una abstracción que describe su comportamiento

Ejemplos:

- La palabra retornada es igual a la solicitada

Asercional:

```
{n = N & p = palabra}
 r := heartbeat(n,p)
{r = palabra}
```

CONICET

UNC

El problema de la corrección

$$Propiedad \models Sistema$$

Describe lo que se espera del sistema (el criterio de corrección)

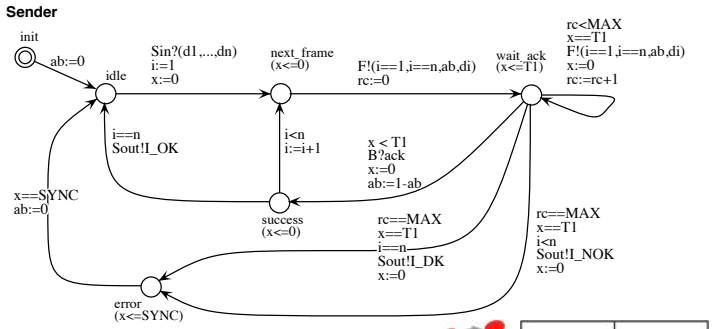
Usualmente una abstracción que describe su comportamiento

Ejemplos:

- La palabra retornada es igual a la solicitada
- El haz de electrones de alta potencia solo funciona bajo la protección del filtro difusor

Model Checking:

$$\Box ((haz = \text{on}) \Rightarrow (filtro = \text{activo}))$$



CONICET

UNC

El problema de la corrección

$$\textit{Propiedad} \models \textit{Sistema}$$

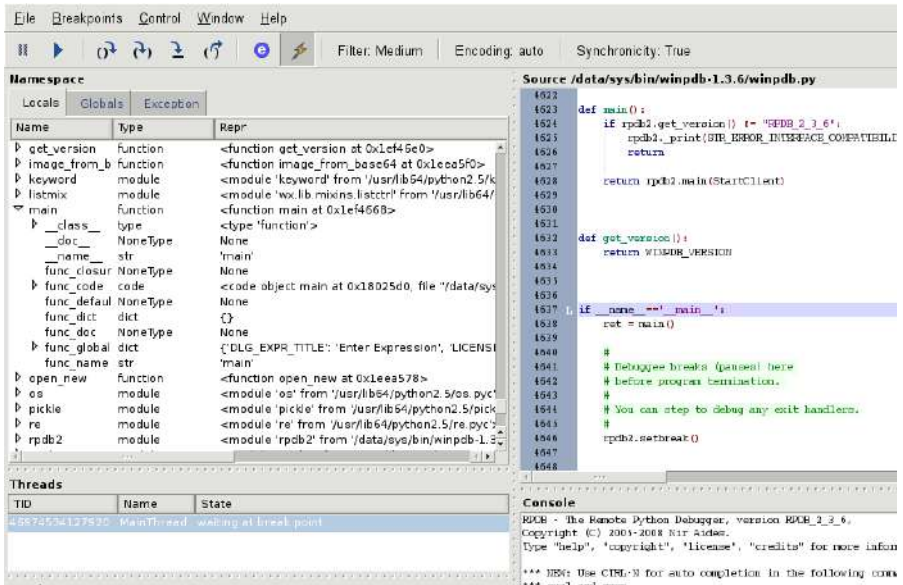
Describe lo que se espera del sistema (el criterio de corrección)

Usualmente una abstracción que describe su comportamiento

Ejemplos:

- La palabra retornada es igual a la solicitada
- El haz de electrones de alta potencia solo funciona bajo la protección del filtro difusor
- Los datos de la trayectoria leído se corresponden con los reales

Testing y simulación:



CONICET

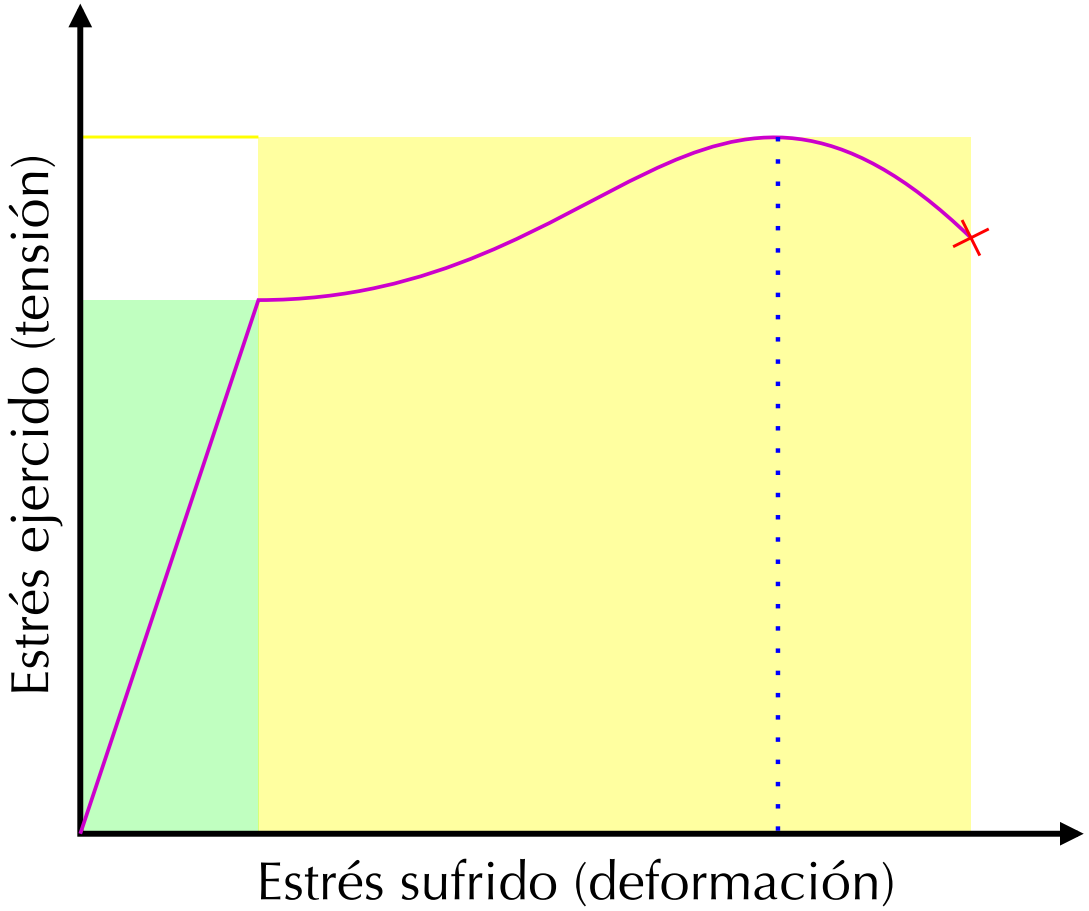
Sin embargo…

CONICET

… las fallas ocurren

UNC

Resiliencia

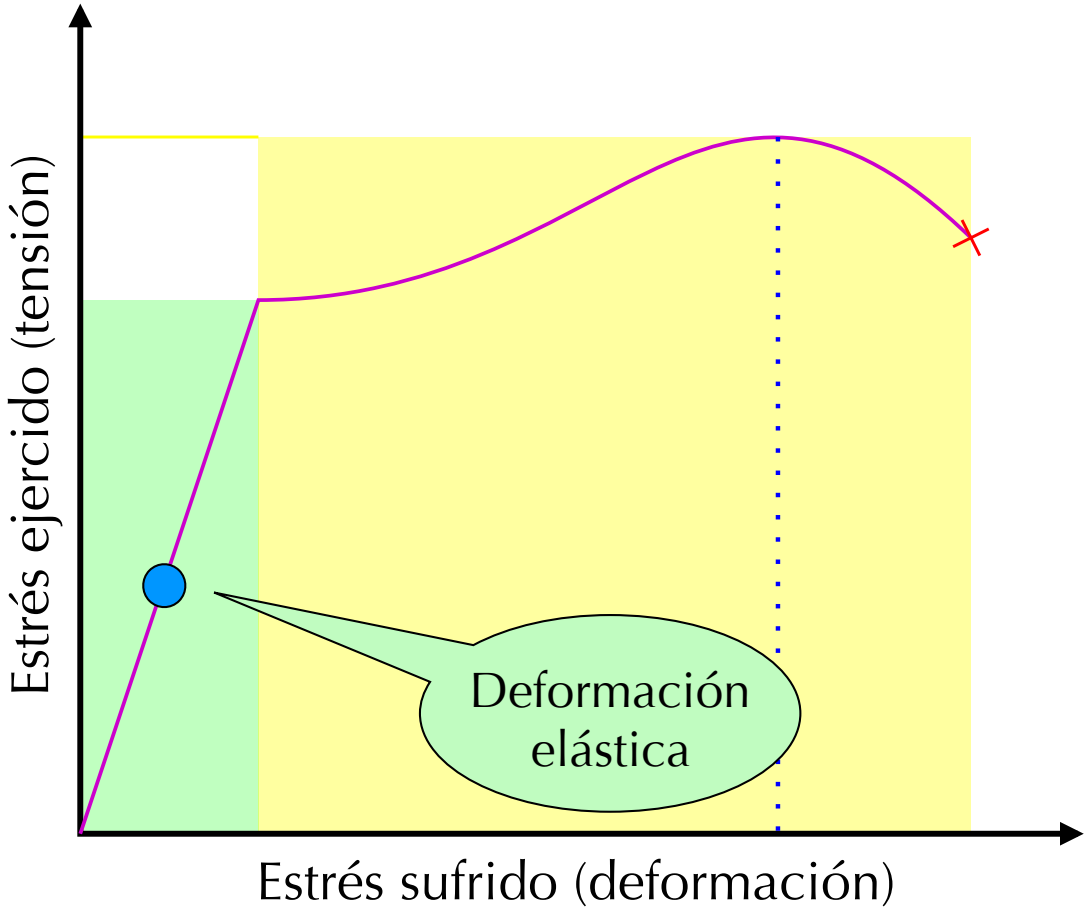


Curva resultante de un ensayo de tracción en algún material (ej: acero)

CONICET

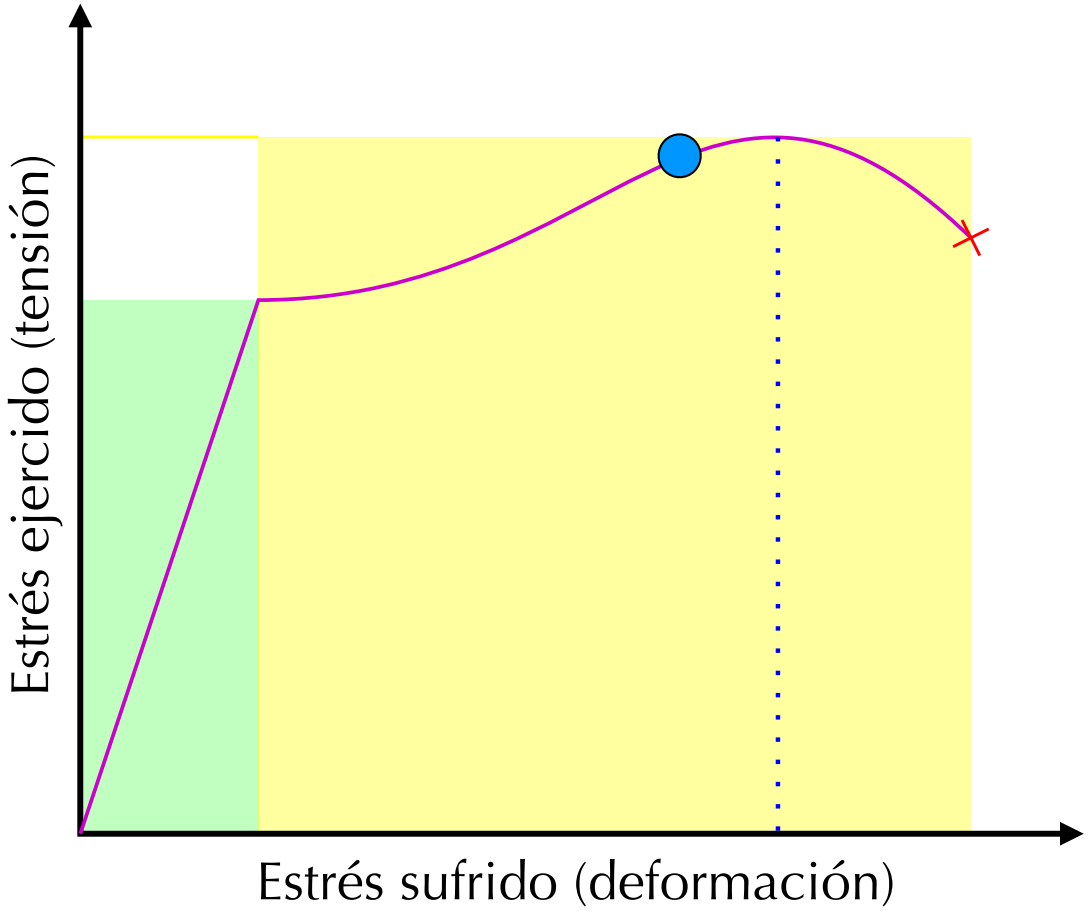
UNC

Resiliencia



Curva resultante de un ensayo de tracción en algún material (ej: acero)

Resiliencia

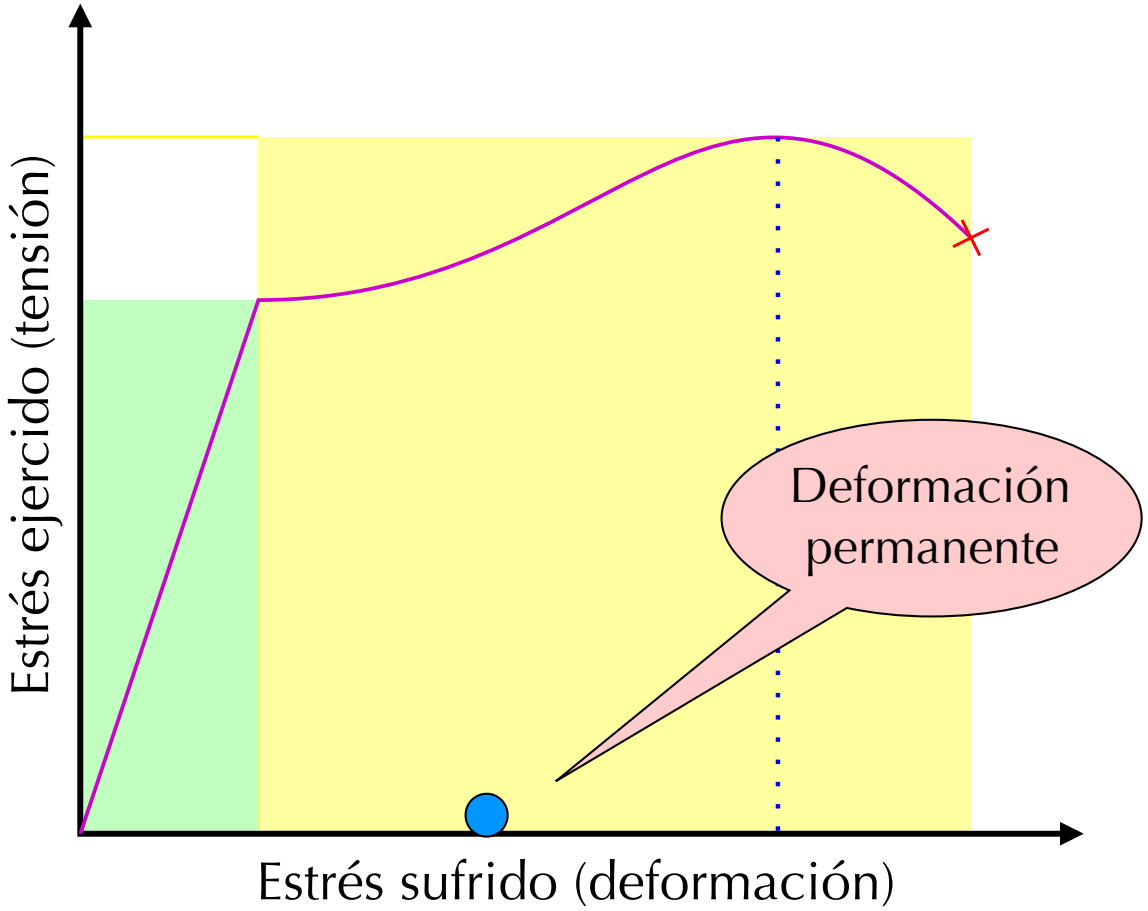


Curva resultante de un ensayo de tracción en algún material (ej: acero)

CONICET

UNC

Resiliencia



Curva resultante de un ensayo de tracción en algún material (ej: acero)

Resiliencia

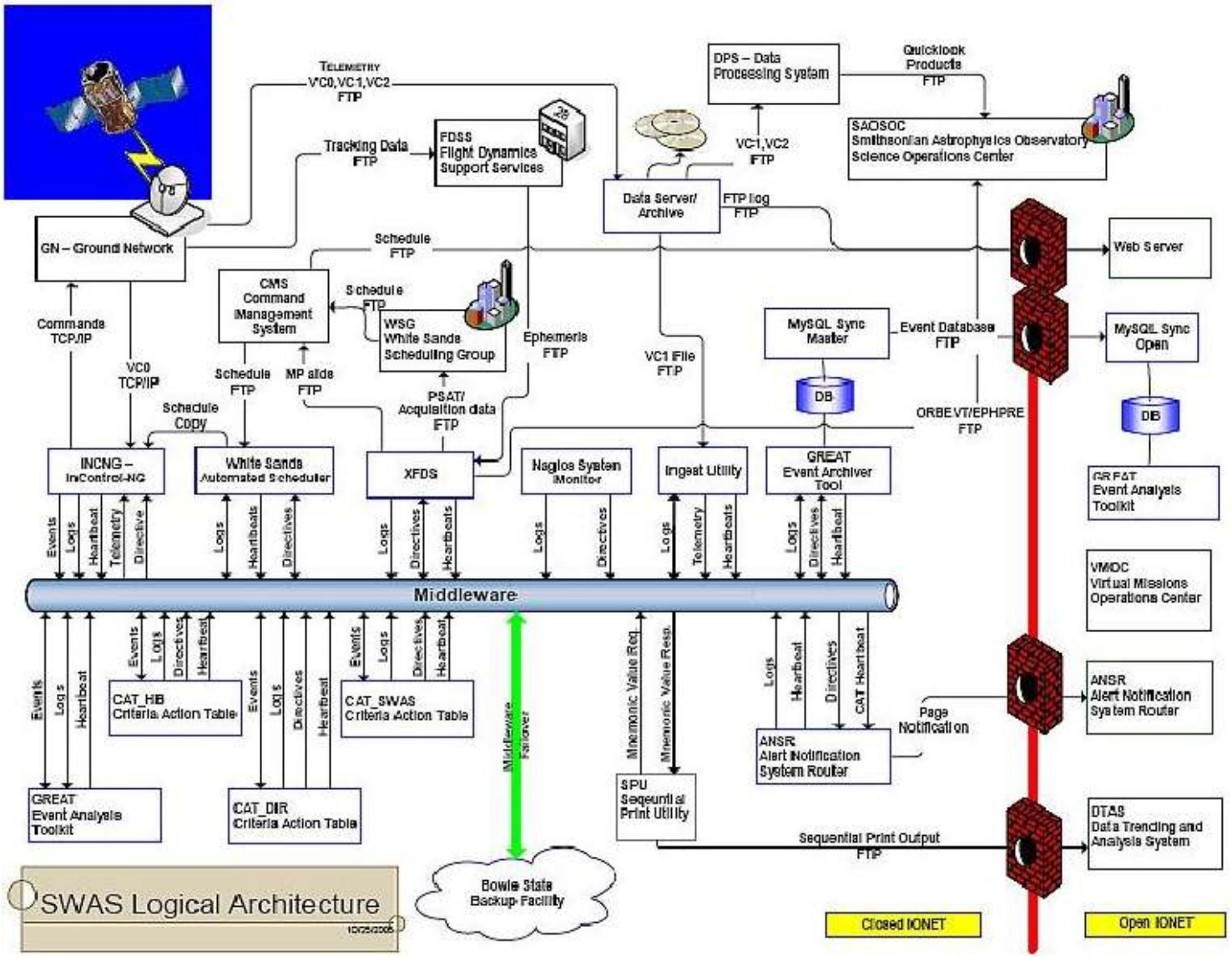
(en Sistemas Computacionales)

La habilidad de proveer y mantener un nivel de servicio aceptable aún bajo la presencia de fallas y otros inconvenientes que puedan surgir y presentar un desafío al funcionamiento normal del sistema.

CONICET

UNC

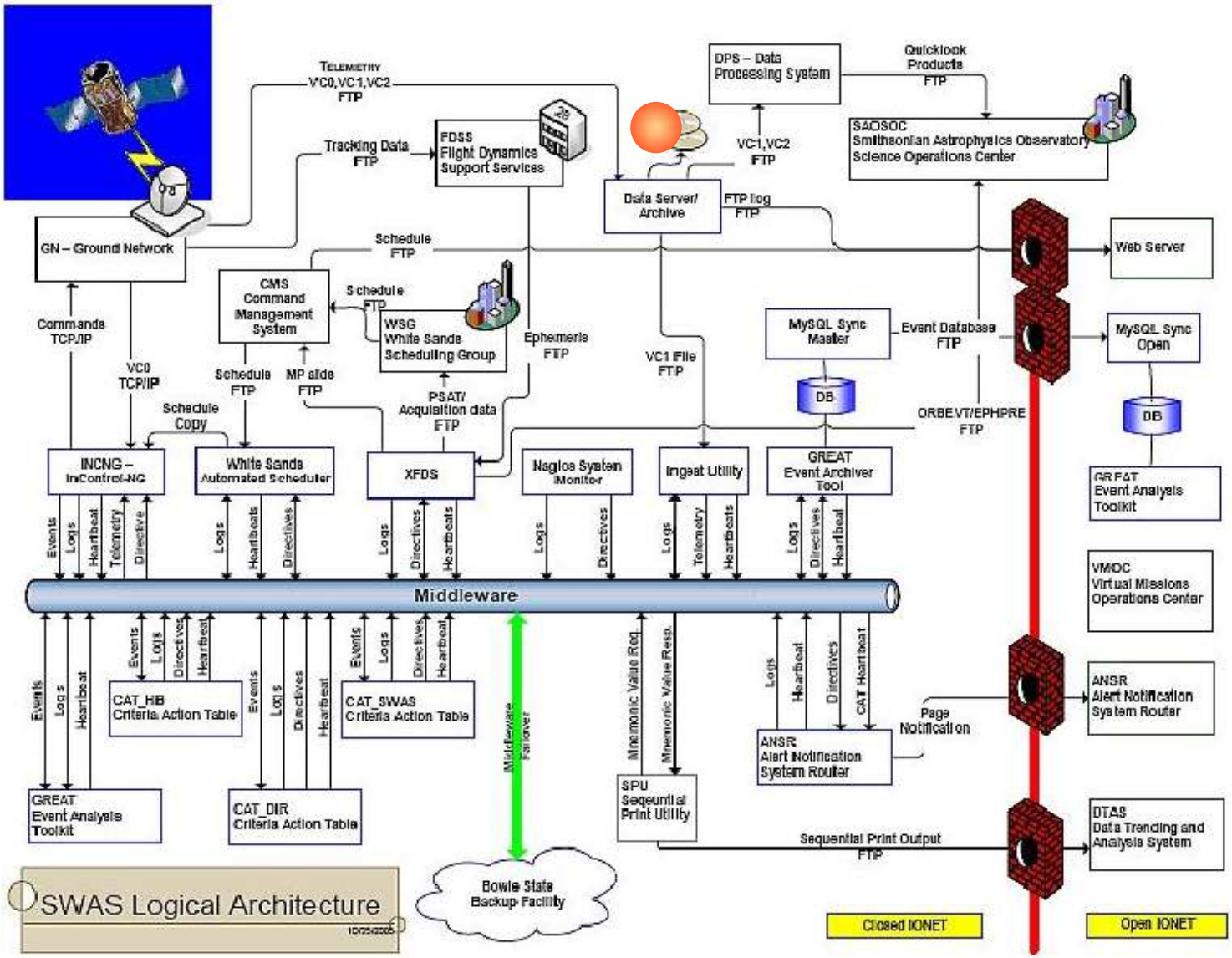
Resiliencia



CONICET

UNC

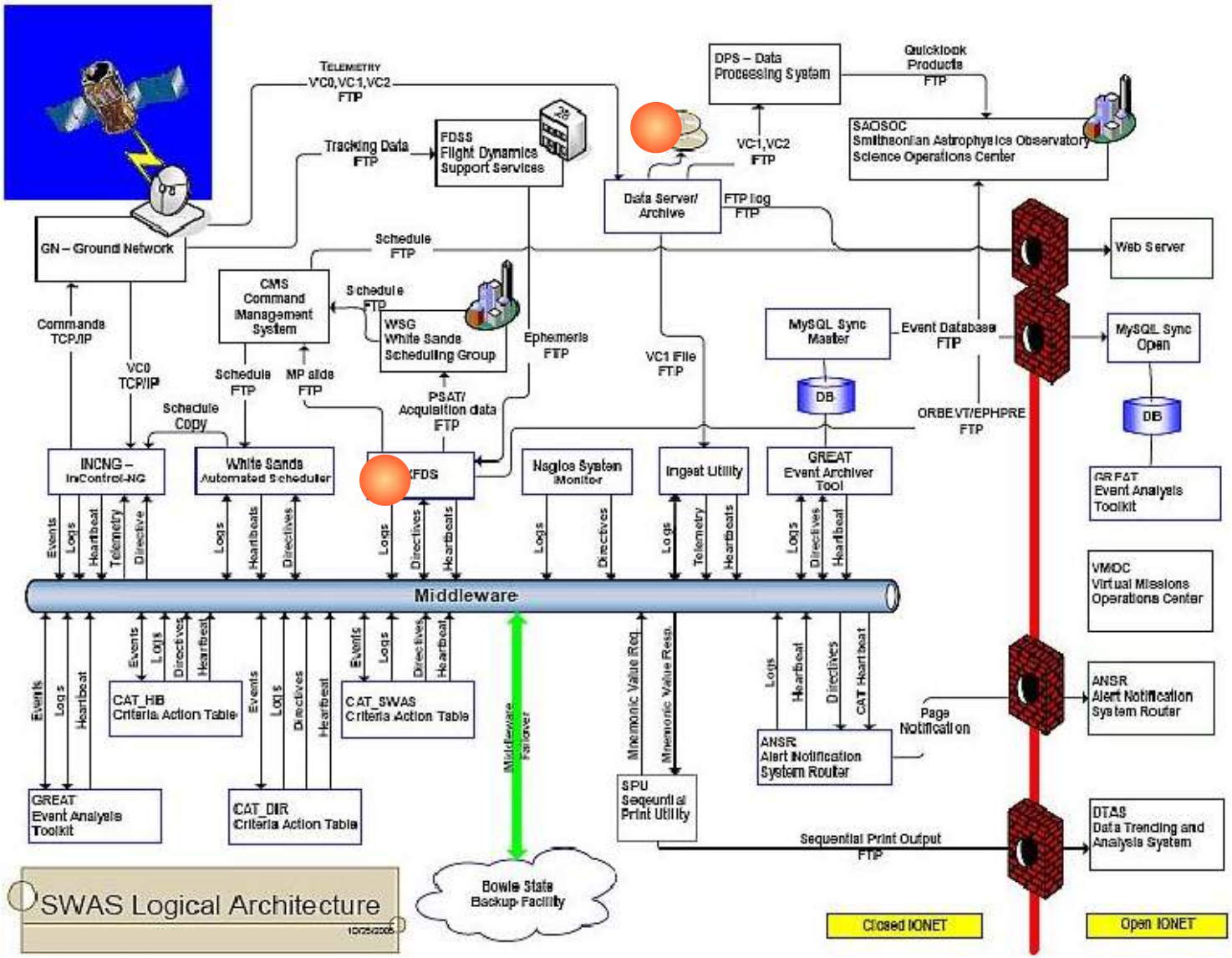
Resiliencia



CONICET

UNC

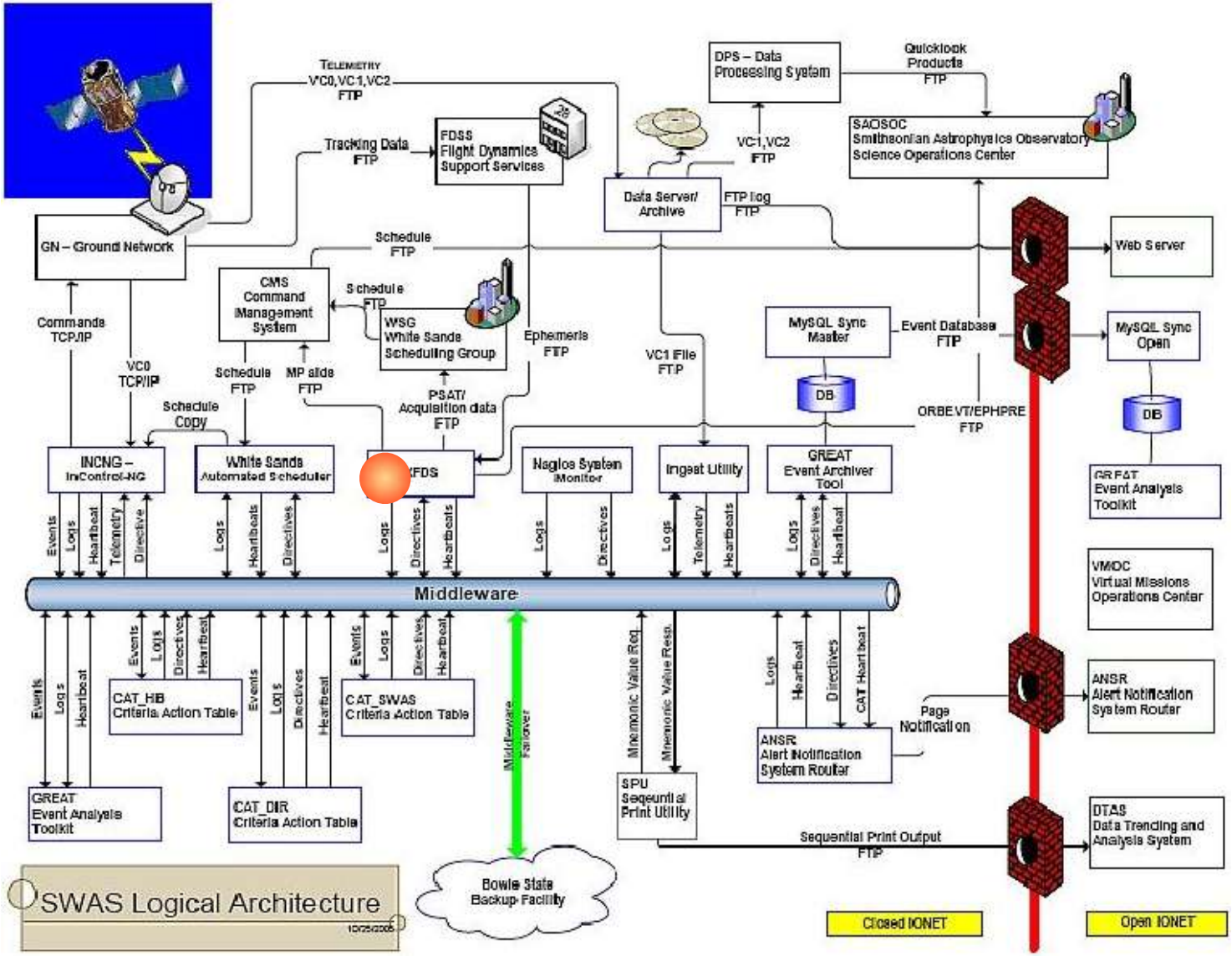
Resiliencia



CONICET

UNC

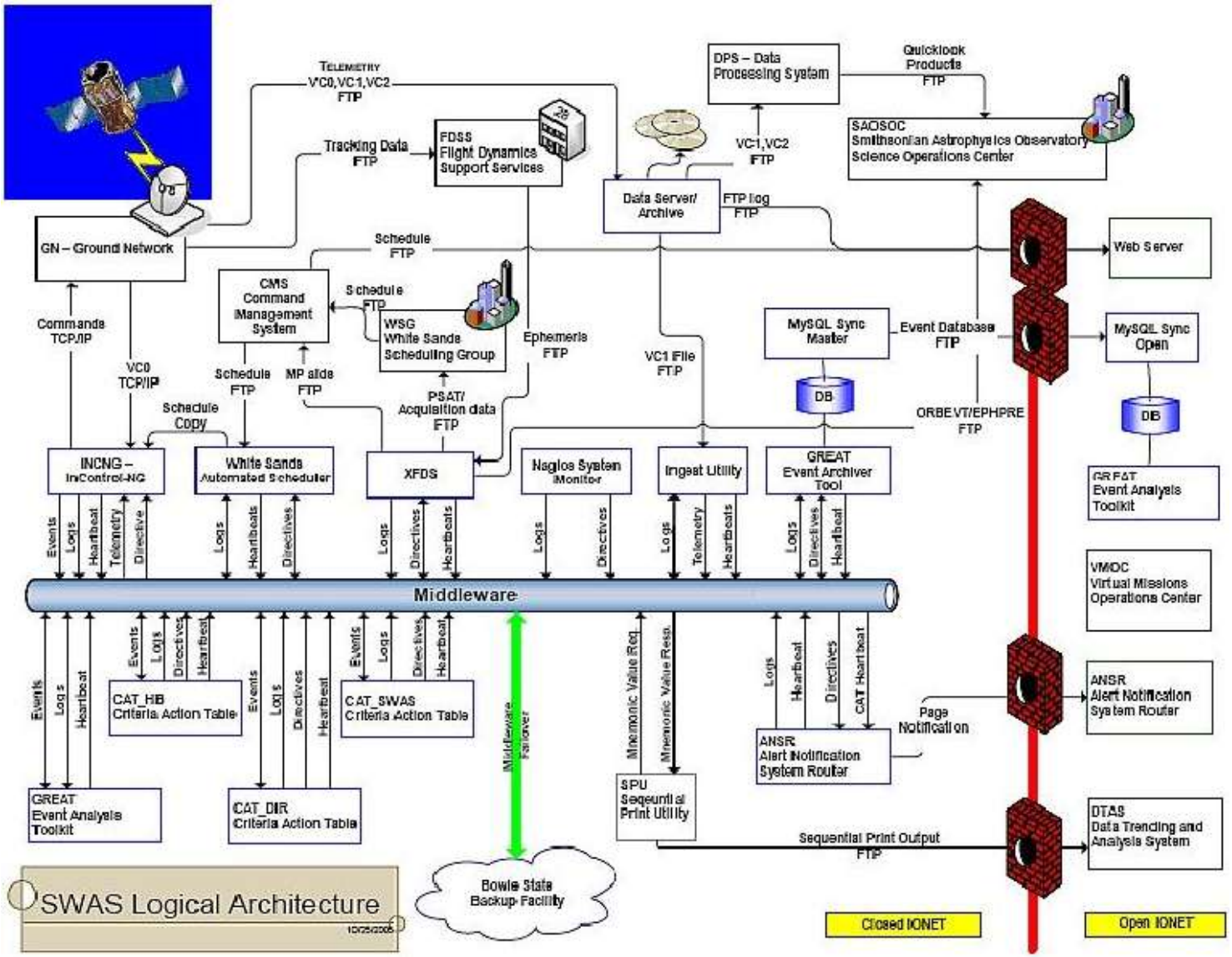
Resiliencia



CONICET

UNC

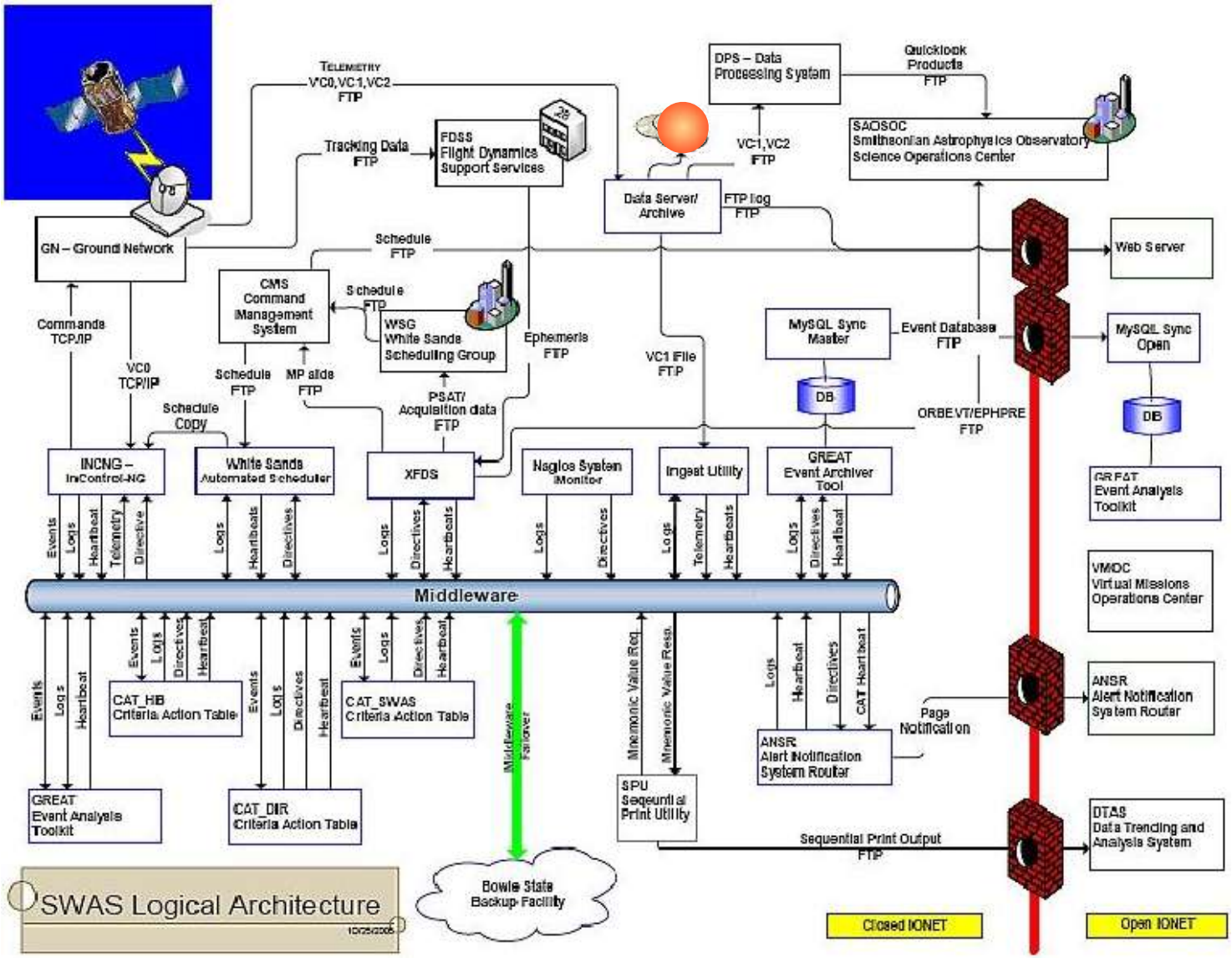
Resiliencia



CONICET

UNC

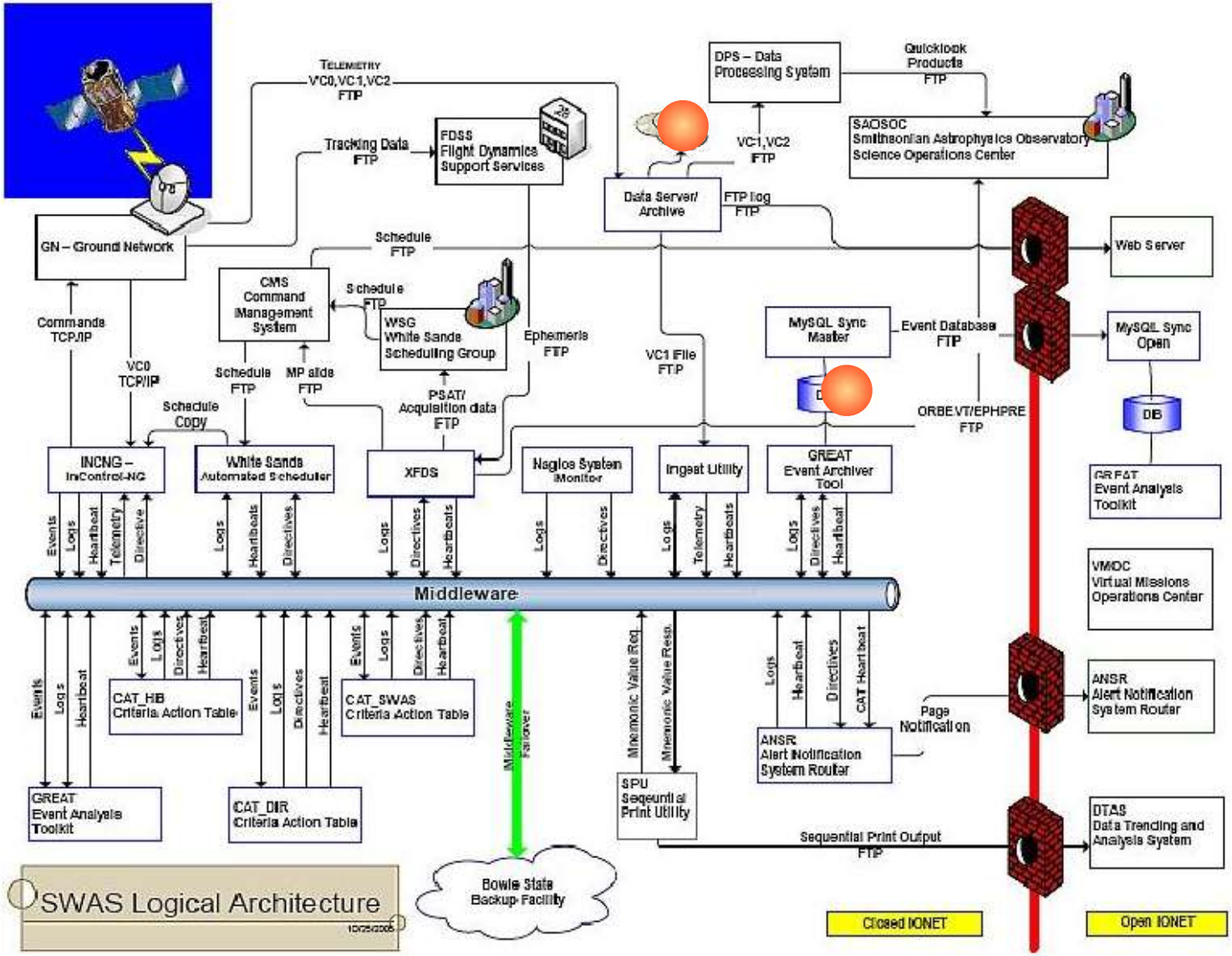
Resiliencia



CONICET

UNC

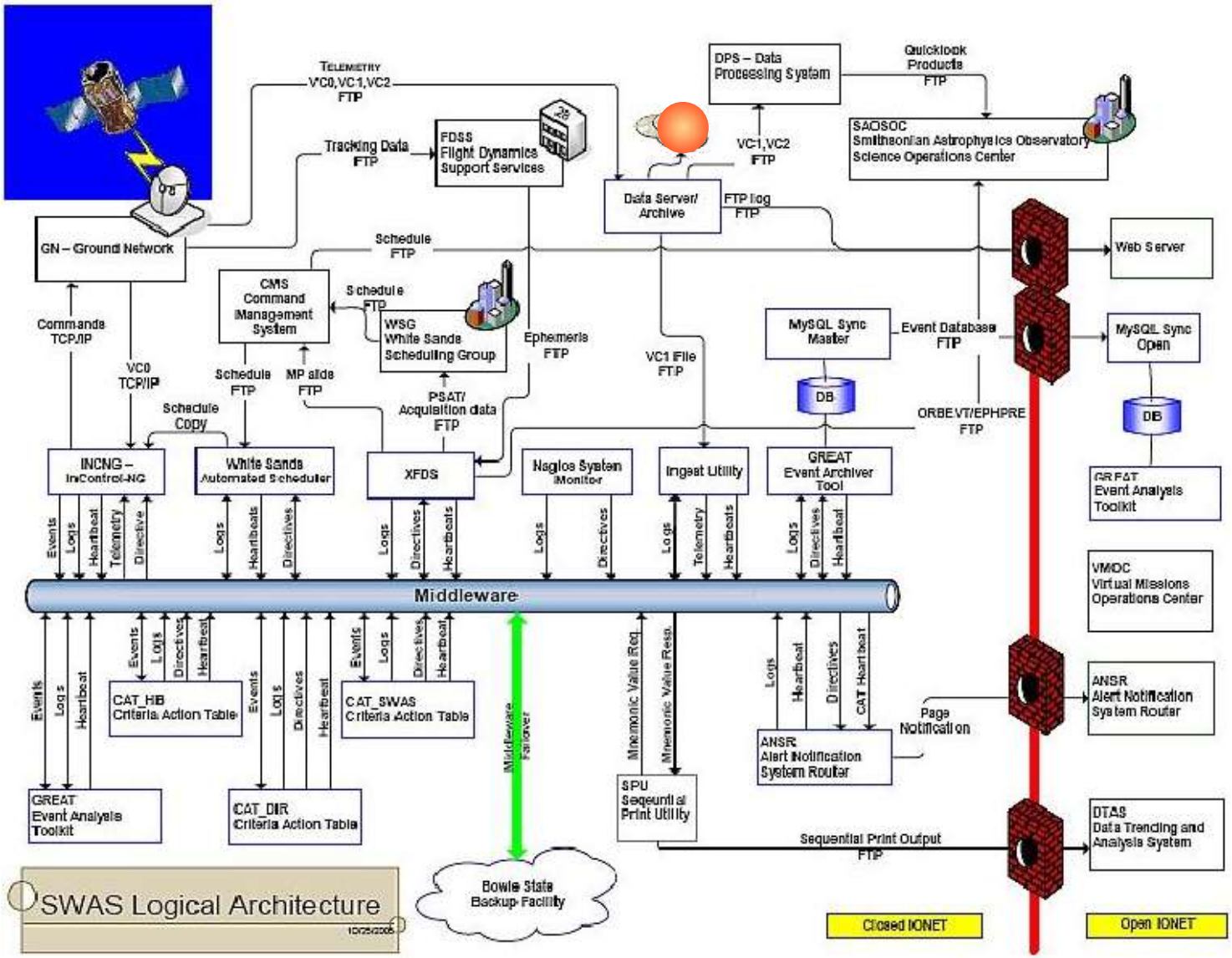
Resiliencia



CONICET

UNC

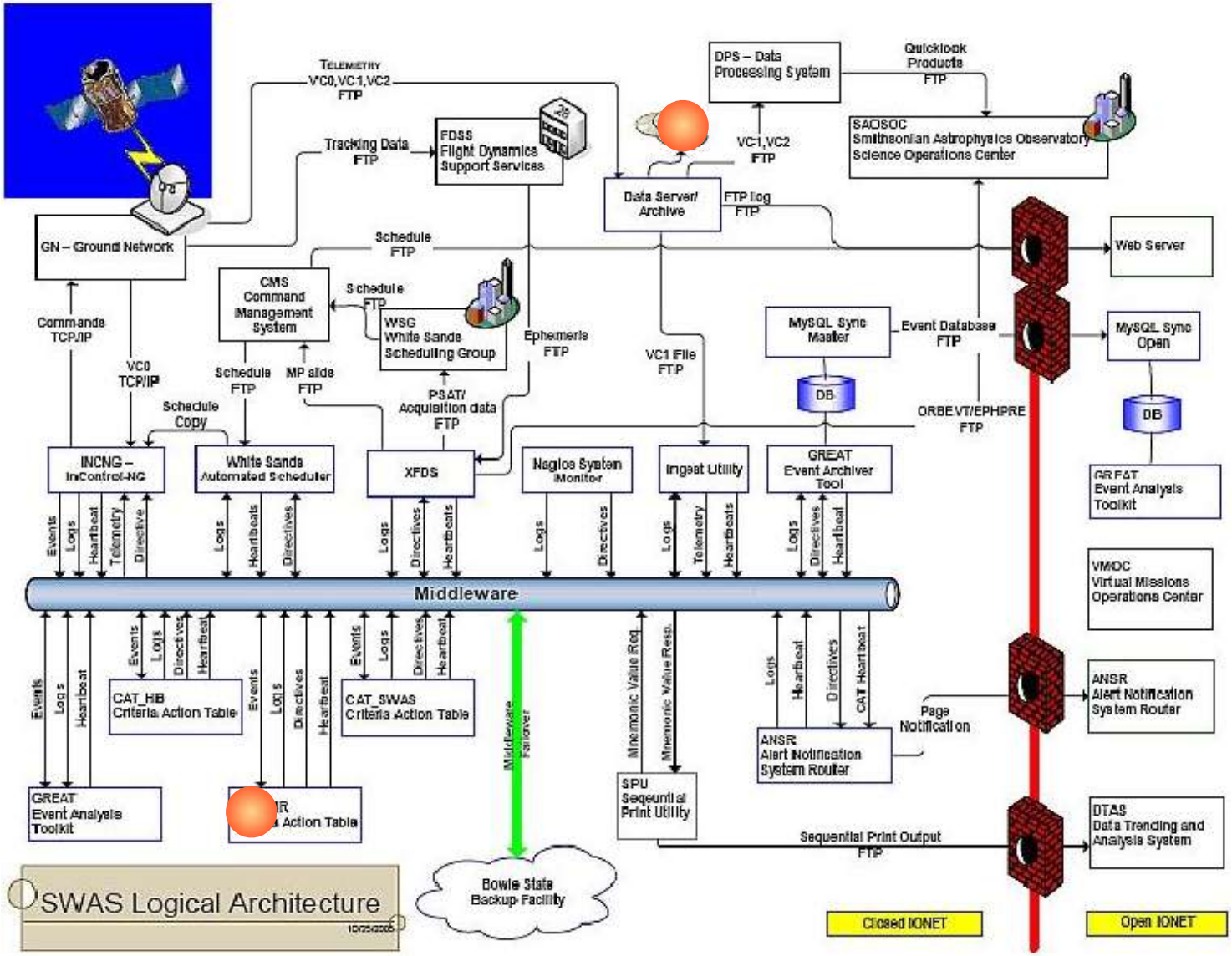
Resiliencia



CONICET

UNC

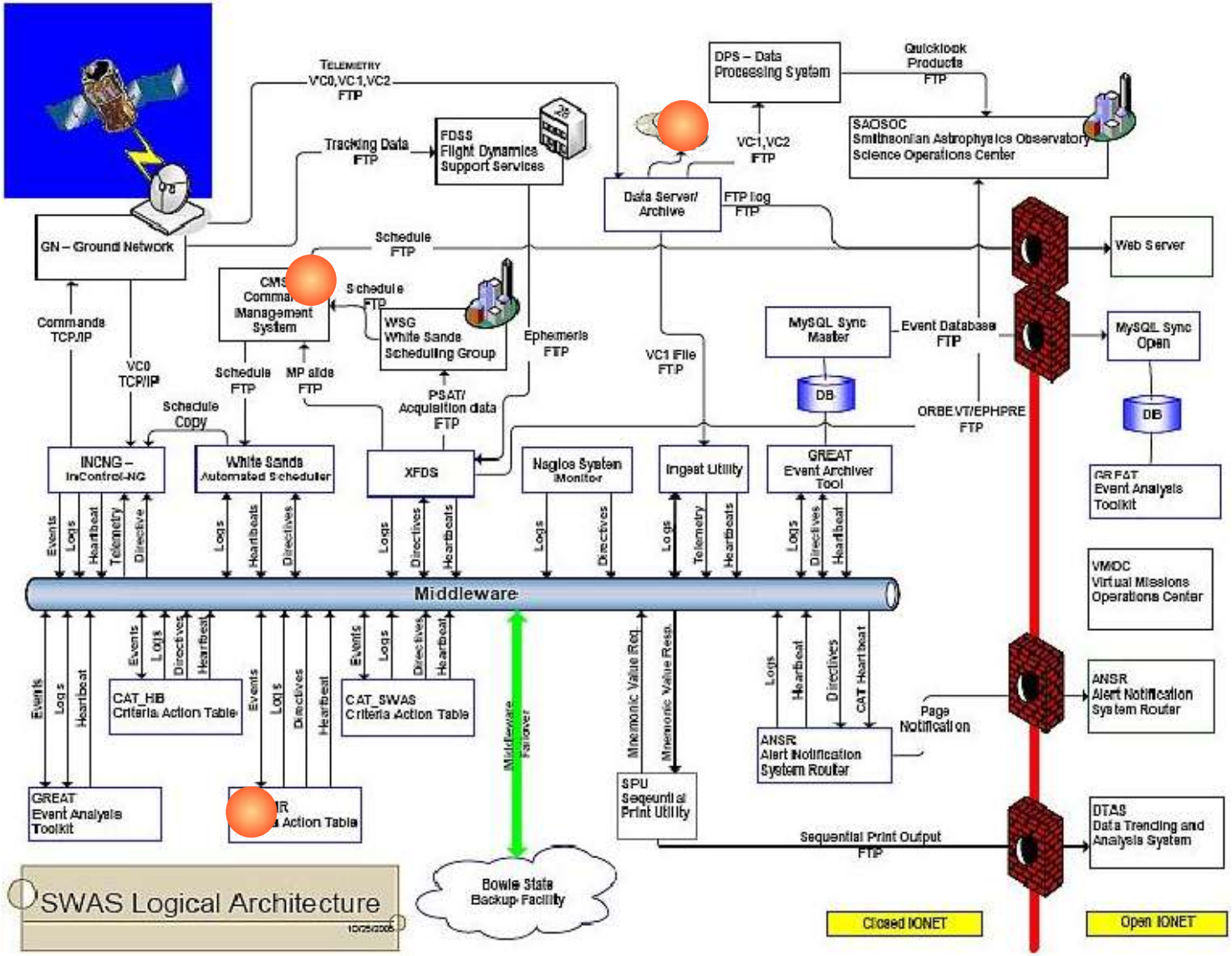
Resiliencia



CONICET

UNC

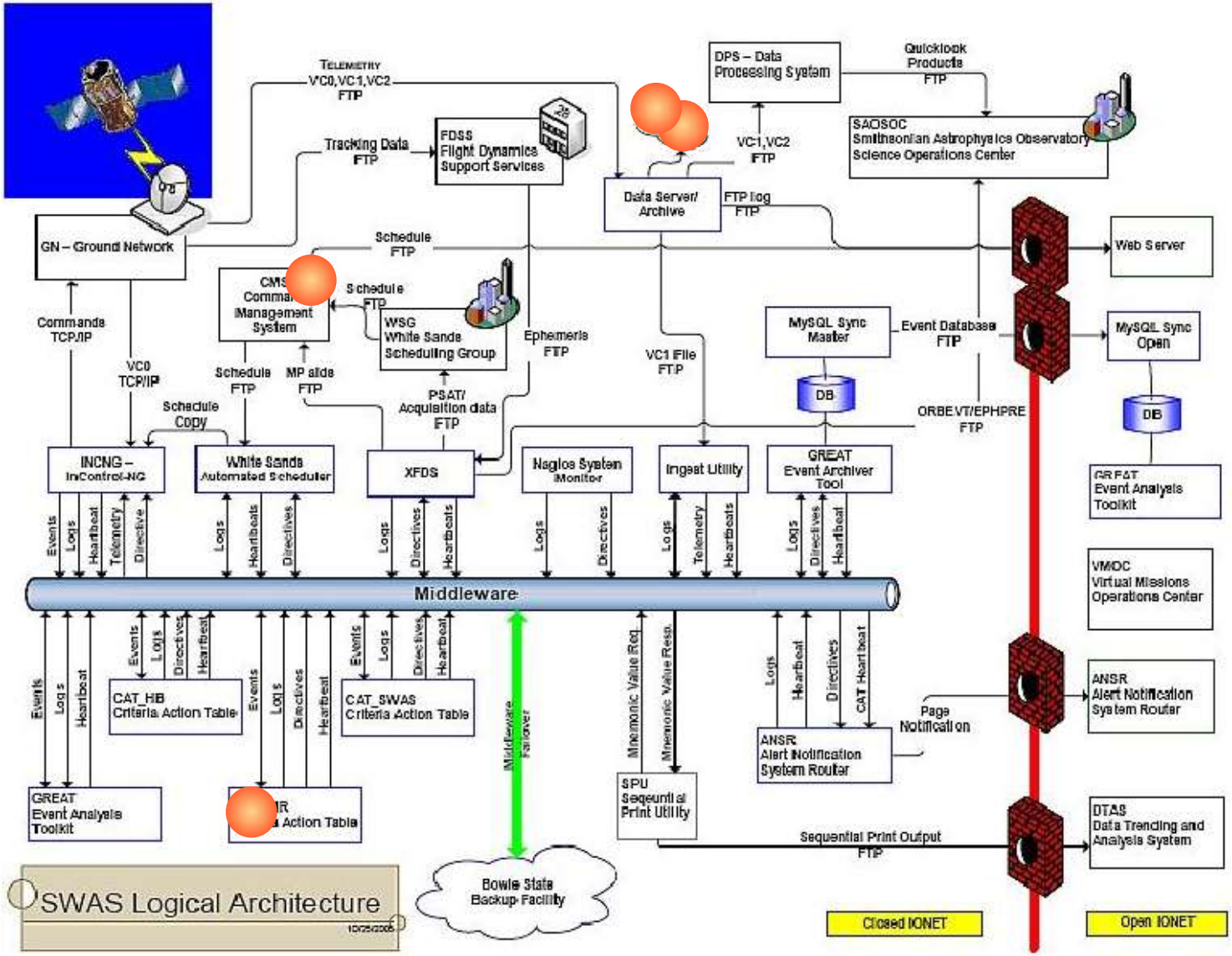
Resiliencia



CONICET

UNC

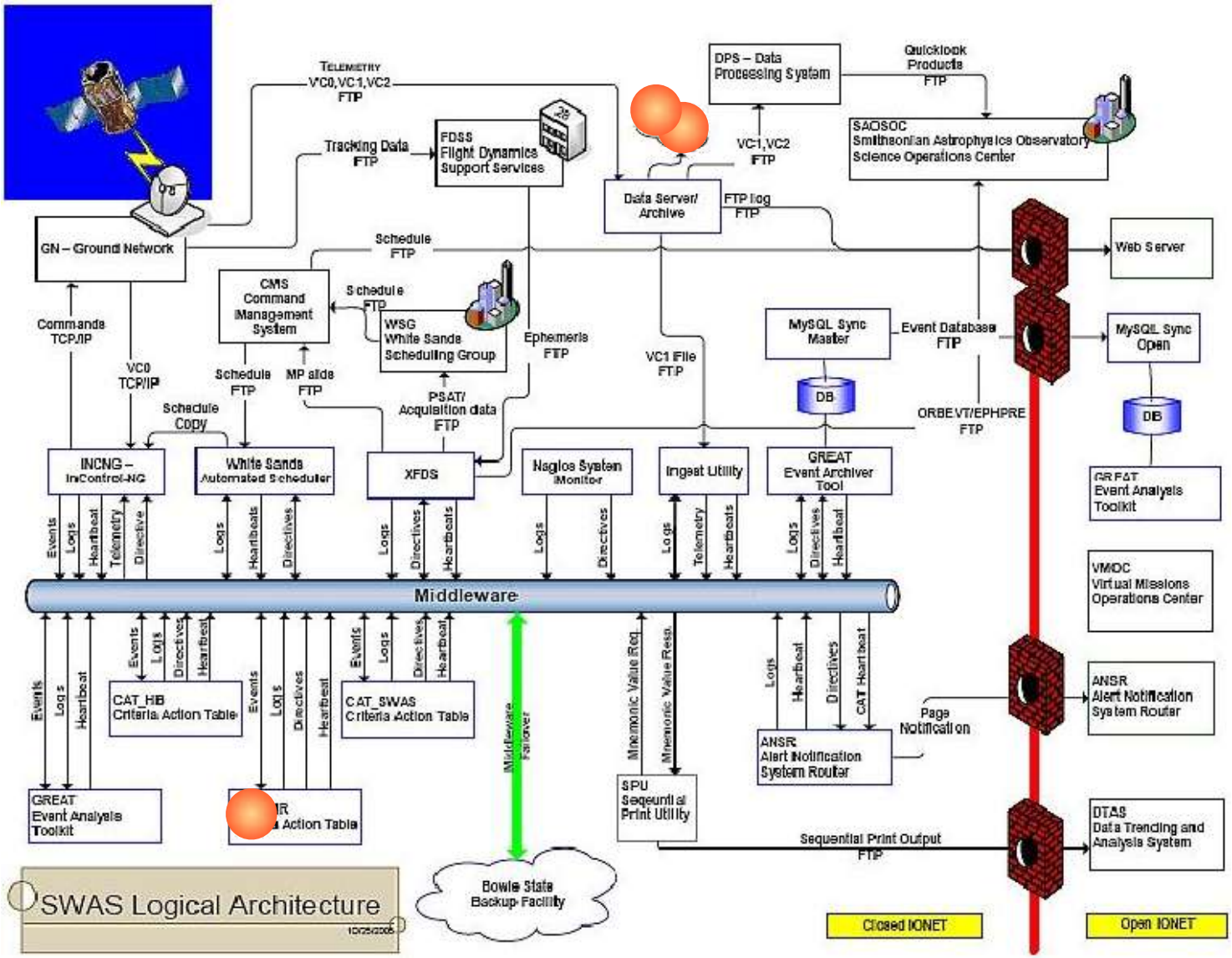
Resiliencia



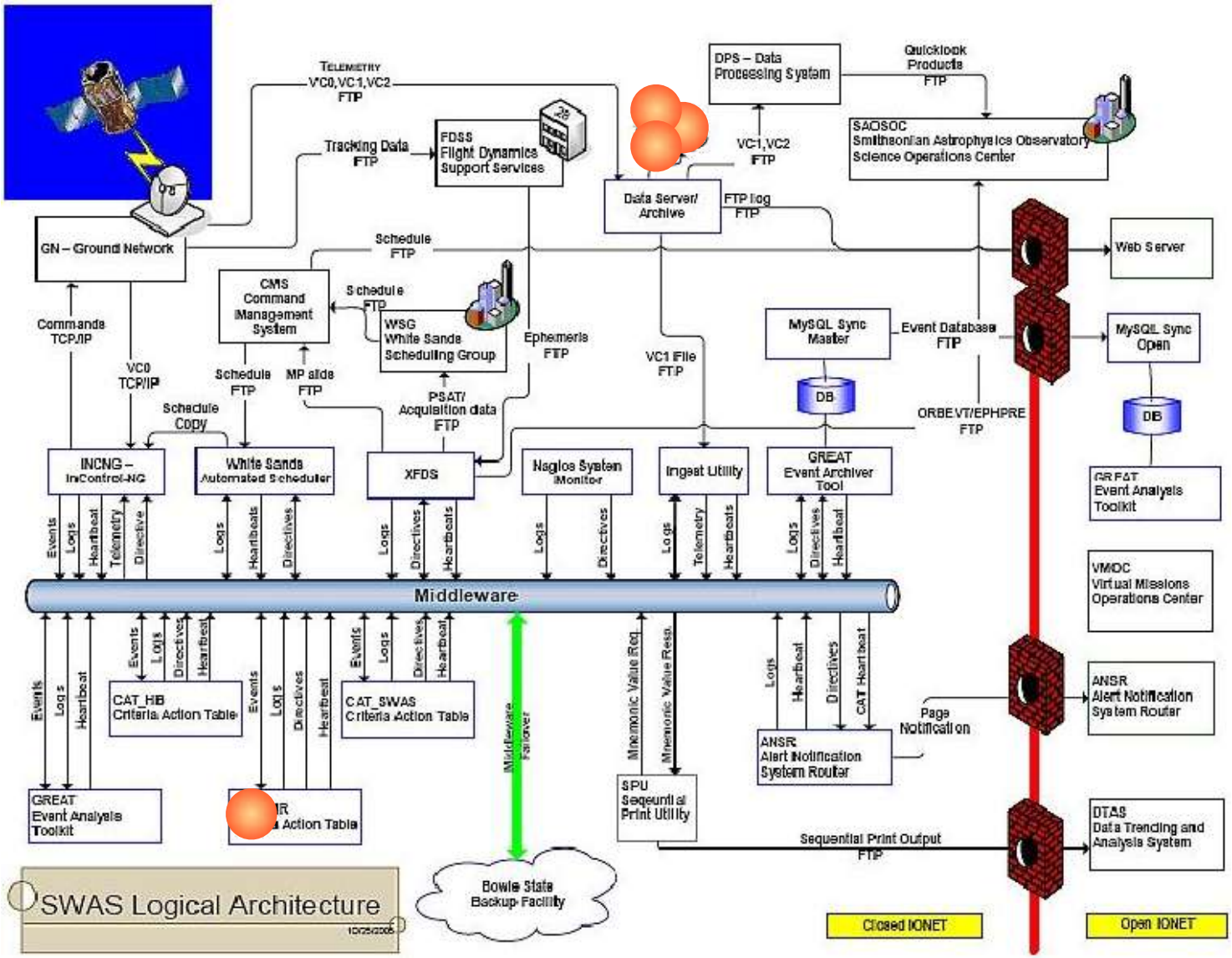
CONICET

UNC

Resiliencia



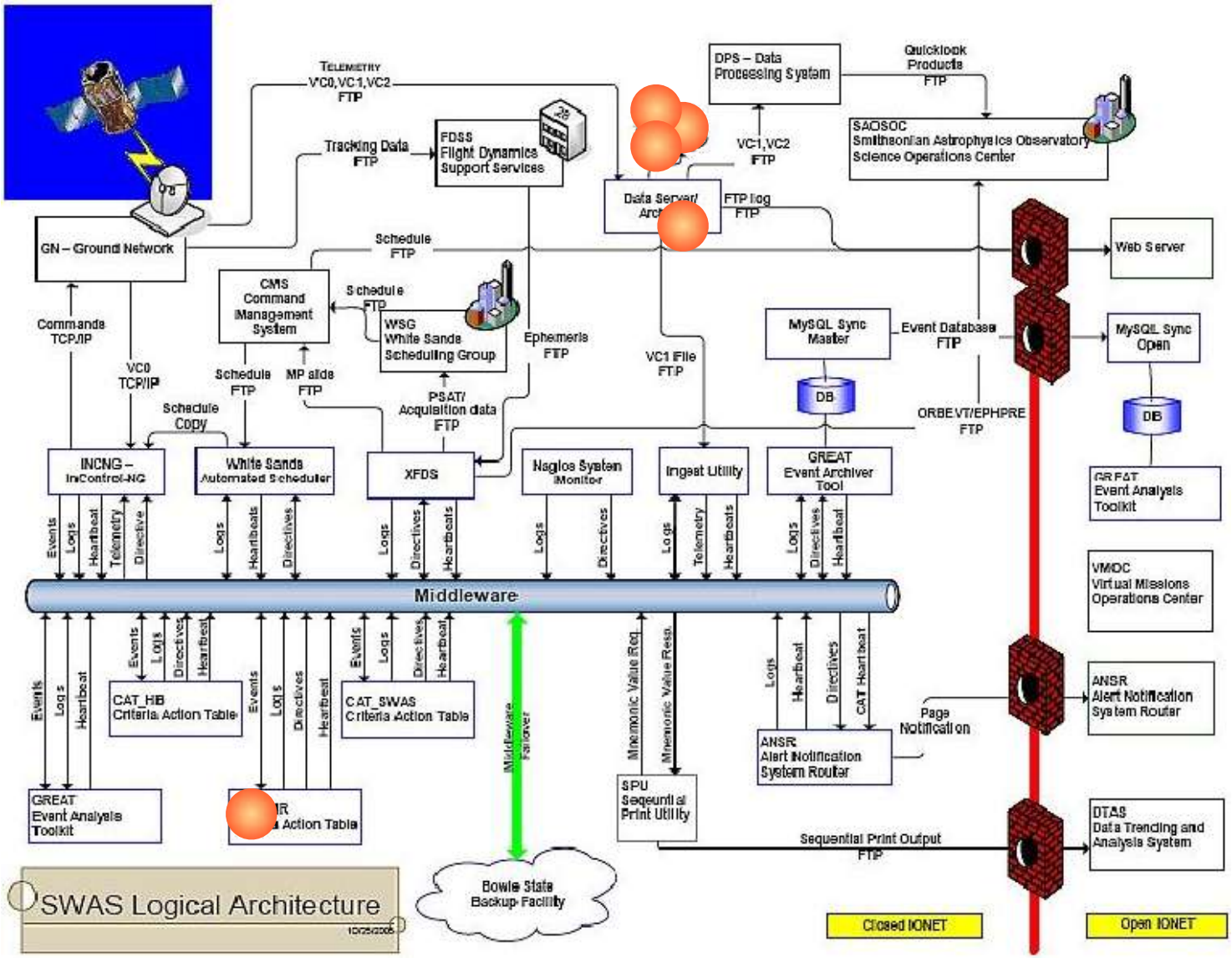
Resiliencia



CONICET

UNC

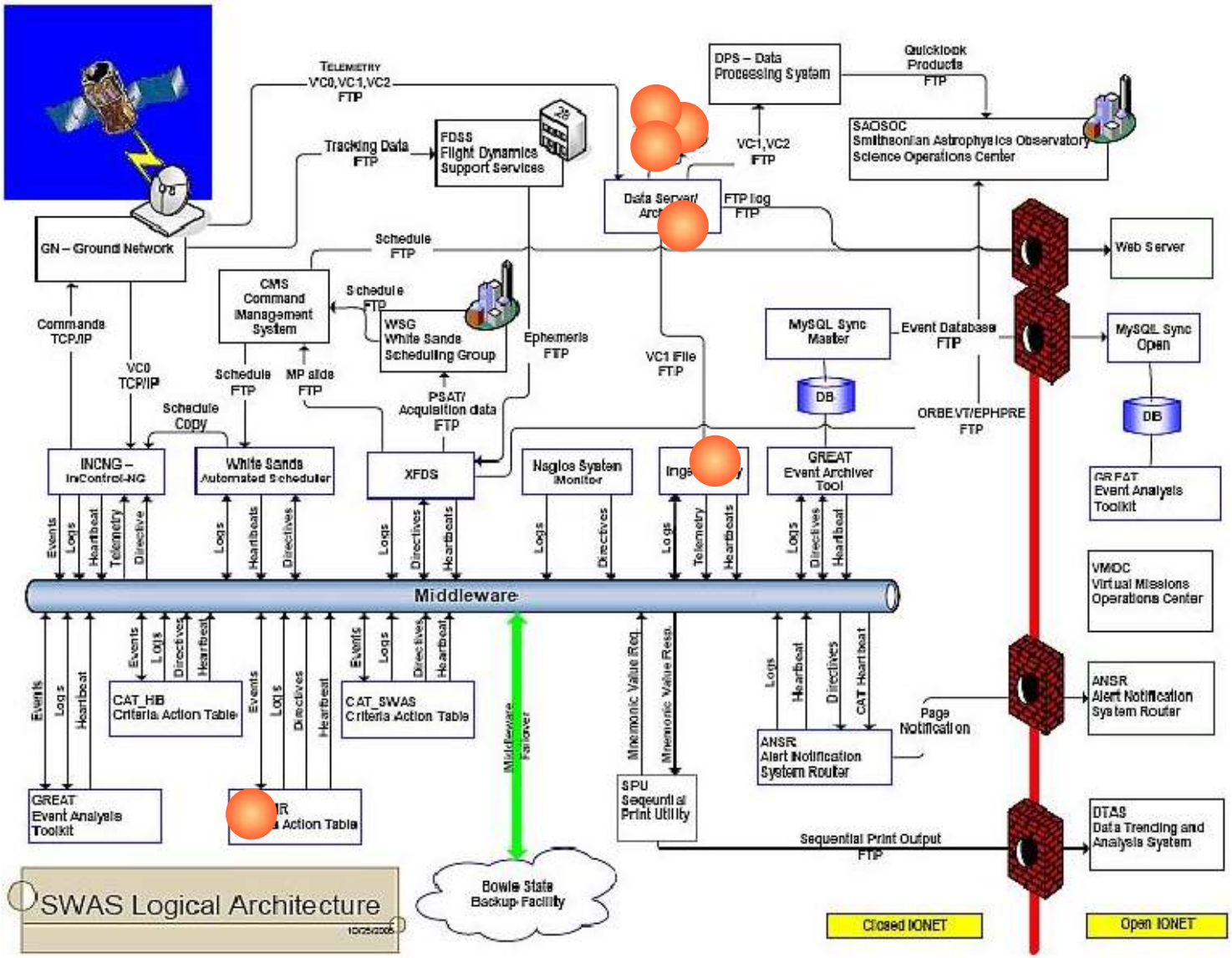
Resiliencia



CONICET

UNC

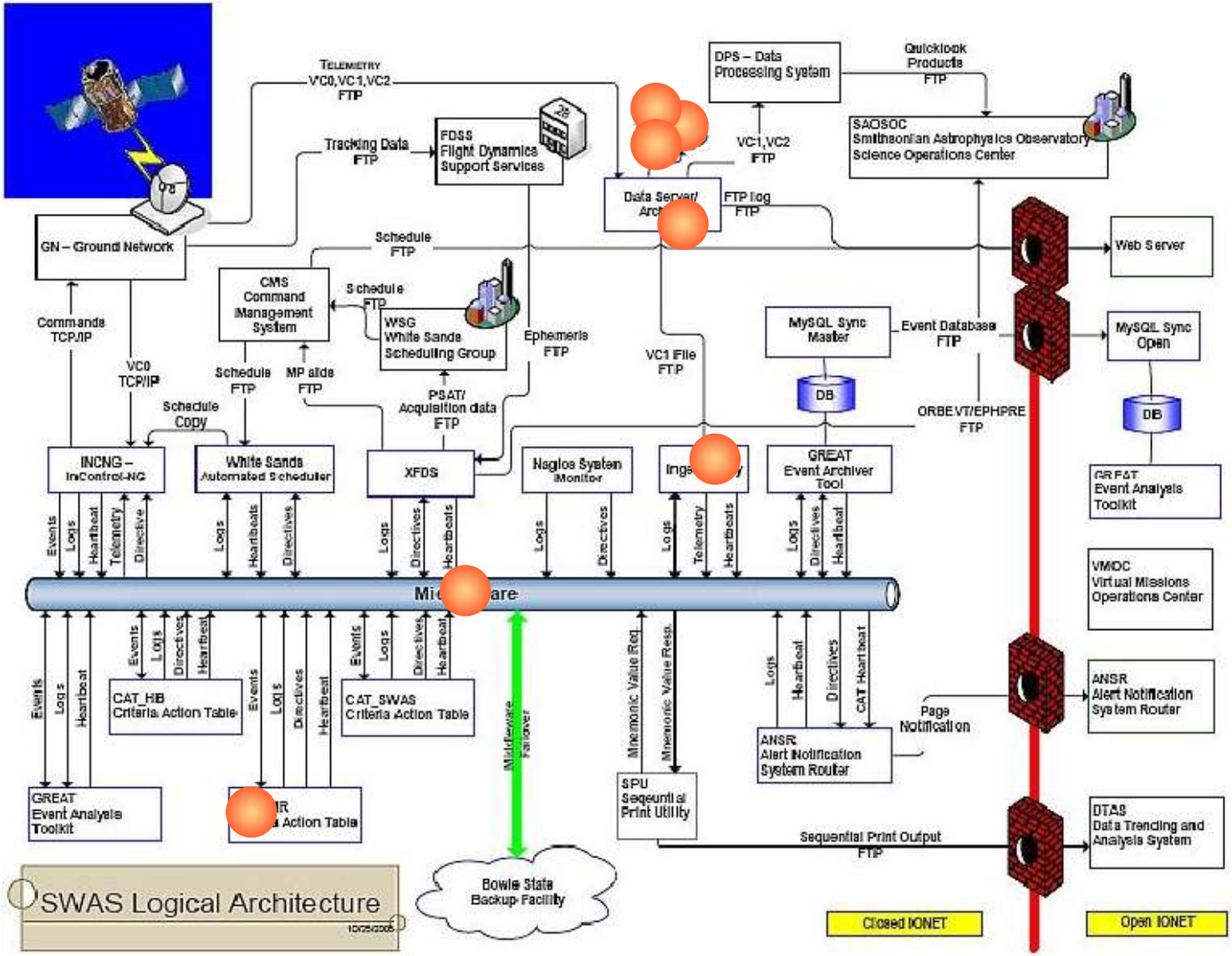
Resiliencia



CONICET

UNC

Resiliencia



Cómo confrontar las fallas

CONICET

UNC

Cómo confrontar las fallas

1. Failover: Varias componentes idénticas de respaldo. Cuando la componente principal falla el sistema lo detecta y cambia a una de las de respaldo.

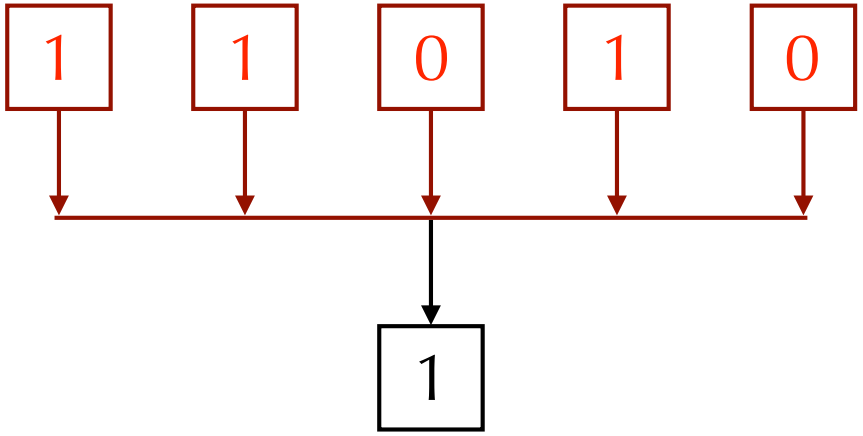
A veces la reparación es posible

CONICET

Cómo confrontar las fallas

2. Votación: Varias componentes idénticas activas. La información correcta se decide por votación.

Reparación mediante refrescado periódico



Cómo confrontar las fallas

3. Detección y corrección de errores:

Detección:

0 1 0 1 1 1 0 0 0

(0 + 1 + 0 + 1 + 1 + 1 + 0 + 0) mod 2 = 0

Cómo confrontar las fallas

3. Detección y corrección de errores:

Detección:

0 1 0 1 1 1 0 0 **0**

(0 + 1 + 0 + 1 + 1 + 1 + 0 + 0) mod 2 = 0

0 1 0 1 1 **0** 0 0 **0**

(0 + 1 + 0 + 1 + 1 + **0** + 0 + 0) mod 2 = **1**

CONICET

UNC

Cómo confrontar las fallas

3. Detección y corrección de errores:

Corrección:

0 1 0 1 1 1 0 0

Cómo confrontar las fallas

3. Detección y corrección de errores:

Corrección:

0 1 0 1 1 1 0 0 0 1 0 1 1 1 0 0 0 1 0 1 1 1 0 0

Cómo confrontar las fallas

3. Detección y corrección de errores:

Corrección:

0 1 0 1 1 1 0 0 0 1 0 1 1 1 0 0 0 1 0 1 1 1 0 0

0 1 0 1 1 1 1 0 0 1 0 0 1 1 0 0 0 1 0 1 1 1 0 0

Cómo confrontar las fallas

3. Detección y corrección de errores:

Corrección:

0 1 0 1 1 1 0 0 0 1 0 1 1 1 0 0 0 1 0 1 1 1 0 0

0 1 0 1 1 1 1 0 0 1 0 0 1 1 0 0 0 1 0 1 1 1 0 0

0 1 0 1 1 1 1 0

0 1 0 0 1 1 0 0

0 1 0 1 1 1 0 0

0 1 0 1 1 1 0 0

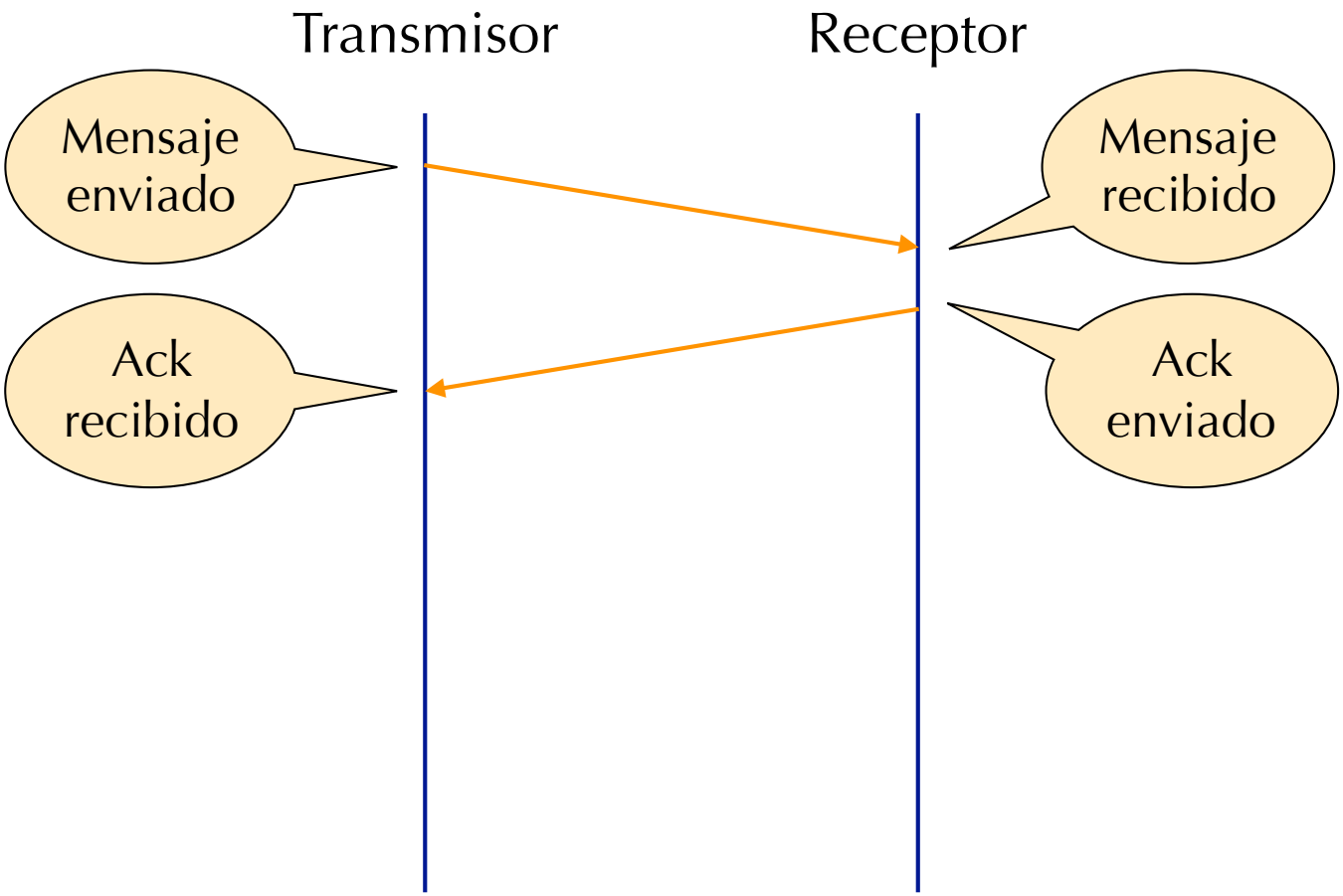
Votación bit a bit

CONICET

UNC

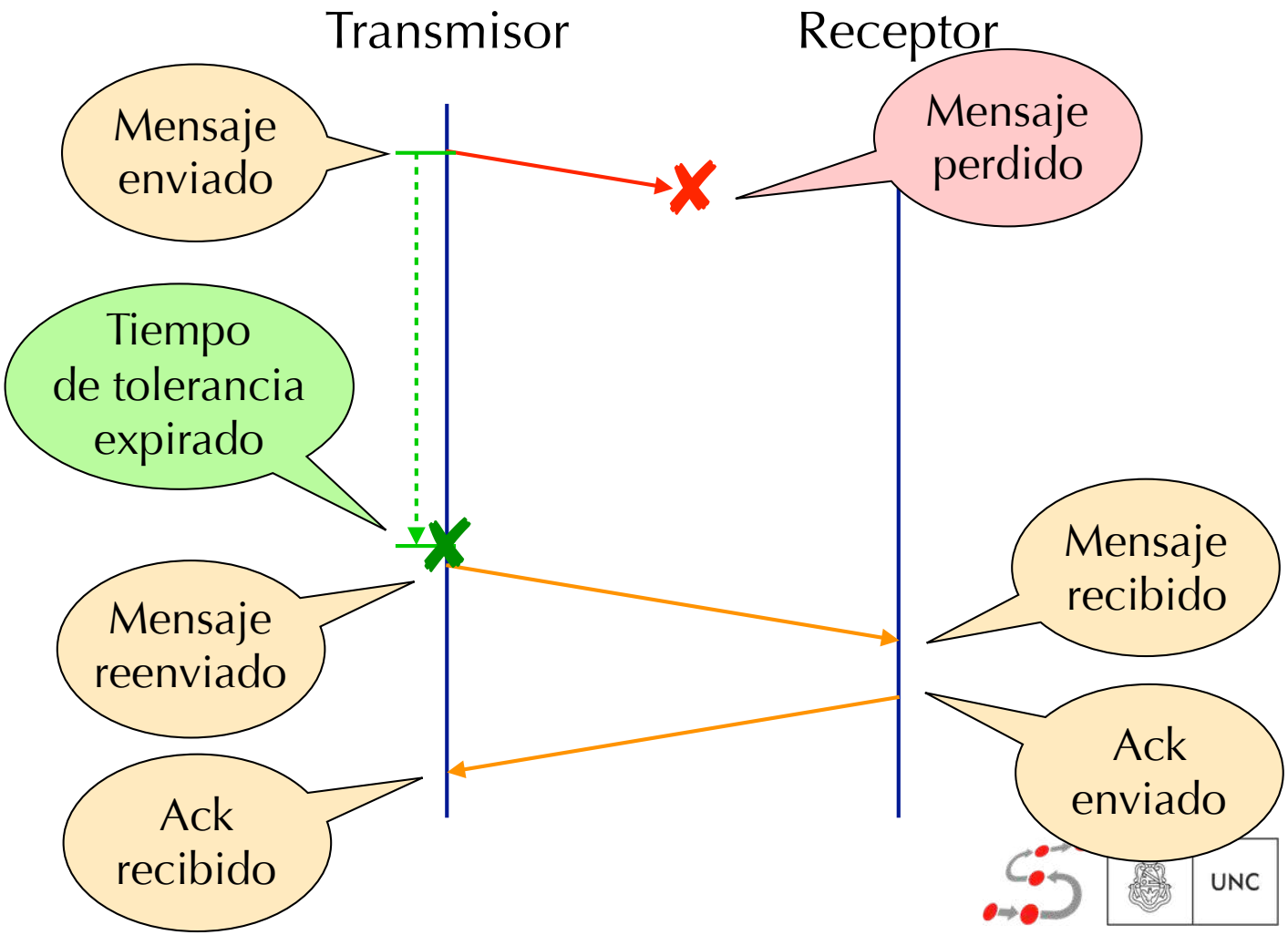
Cómo confrontar las fallas

4. Reconocimientos (Acks) y timeouts:



Cómo confrontar las fallas

4. Reconocimientos (Acks) y timeouts:



CONICET

UNC

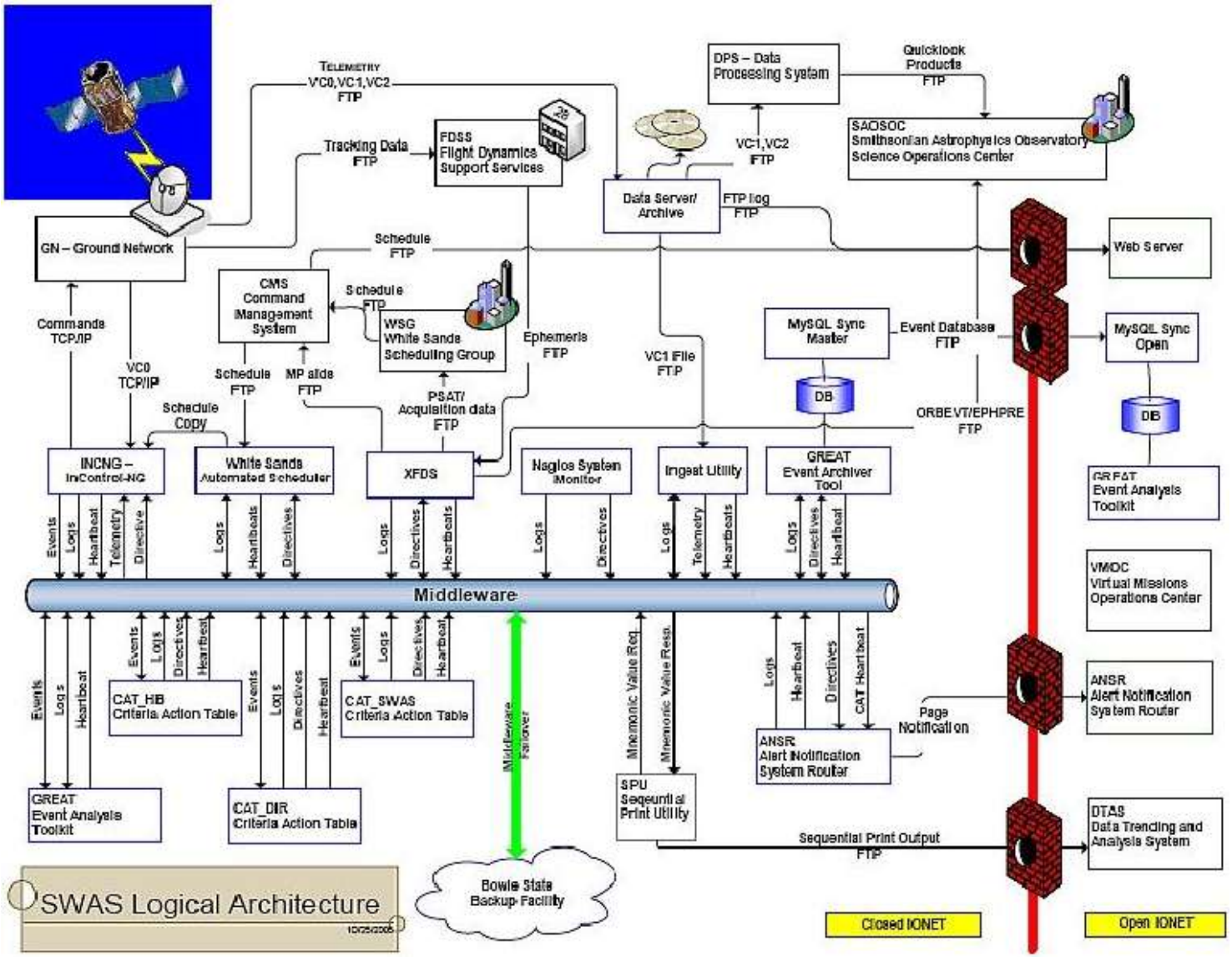
Eventos

Los eventos pueden cuantificarse probabilísticamente

Ejemplos:

- Probabilidad de pérdida de un mensaje
- Tiempo esperado de vida de una fuente de alimentación
- Tiempo esperado de reparación del disco rígido
- Tiempo esperado de transmisión tierra-satélite
- Probabilidad de alteración de un bit bajo radiación
- Tiempo esperado de refrescado de memoria

Resiliencia



CONICET

UNC

Análisis de resiliencia

- Se requiere gran confiabilidad.

  Ej:
  - Disponibilidad del 99.999% (“cinco nueves”)
  - Tiempo esperado de falla de 6 años

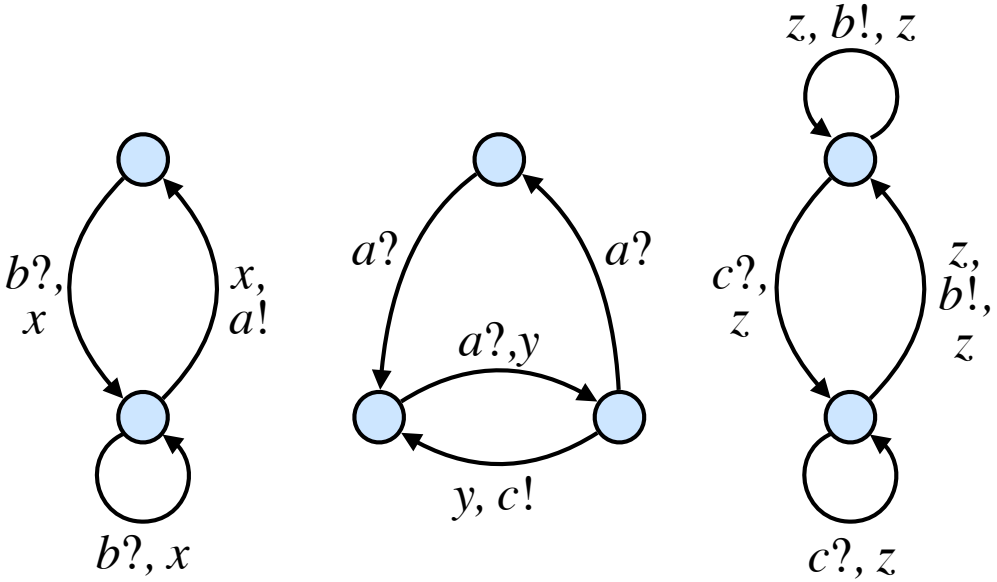
- Determinadas por eventos raros:

  El evento combinado que determina esa tipo de propiedades suele tener probabilidad muy baja de ocurrir.

Análisis de resiliencia

Un par de desafíos

Modelado composicional



Redes de
autómatas estocásticos
con entradas y salidas
(IOSA)

Simulación de eventos raros

CONICET

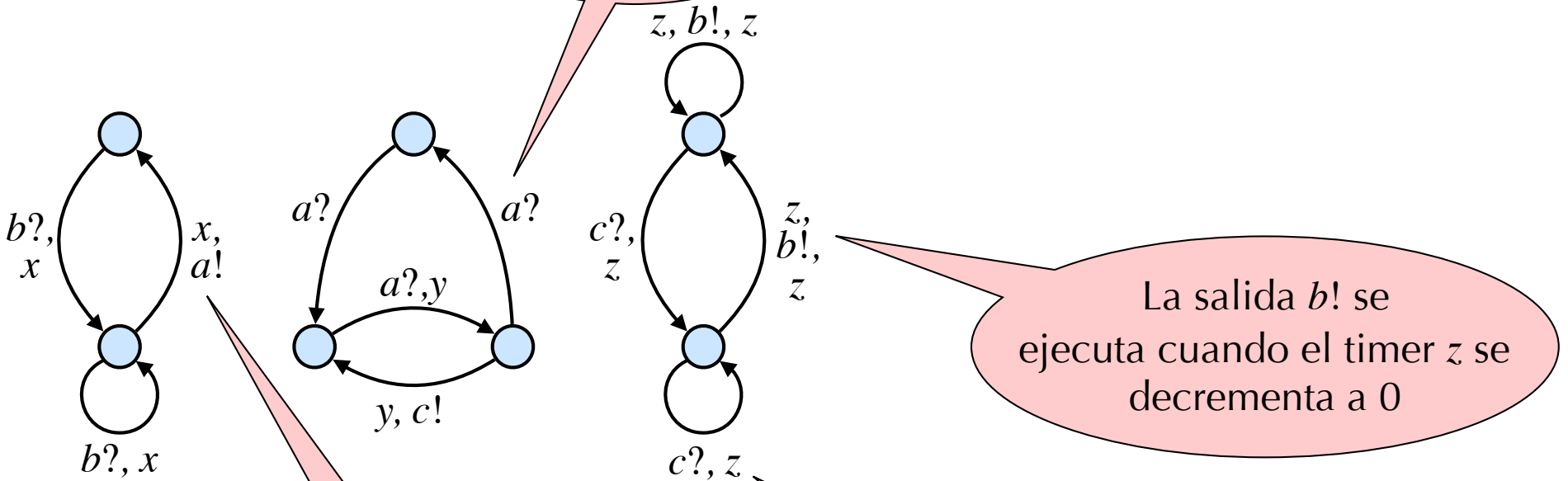
UNC

Análisis de resiliencia

Un par de desafíos

Modelado compo

Simulación de eventos raros



autom[illegible]ásticos con entradas y salidas (IOSA)

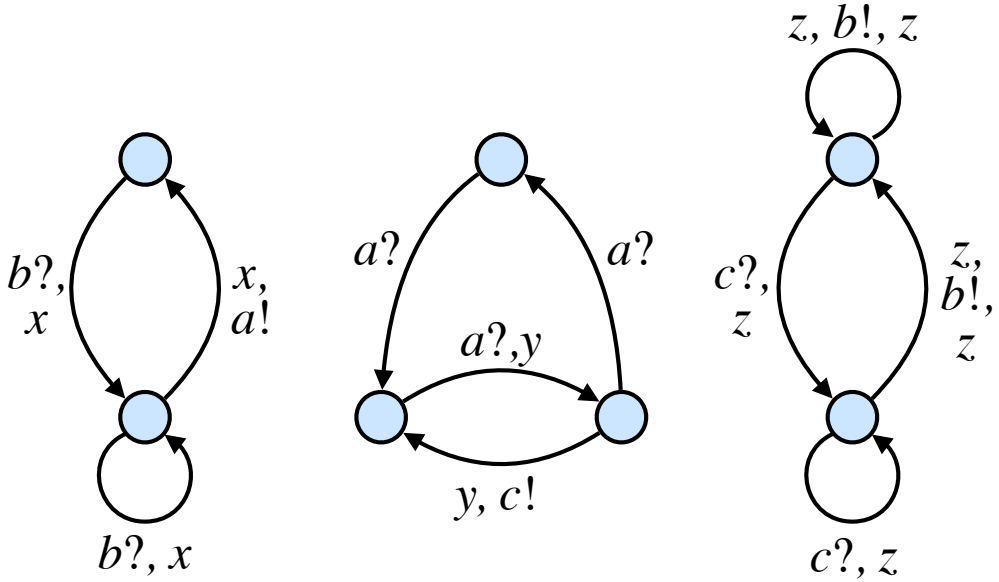
CONICET

UNC

Análisis de resiliencia

Un par de desafíos

Modelado composicional



Redes de autómatas estocásticos con entradas y salidas (IOSA)

Simulación de eventos raros

- Preparado para Simulación por Eventos Discretos
- El problema de realizarla siguiendo la técnica de simulación Monte Carlo

…

CONICET

UNC

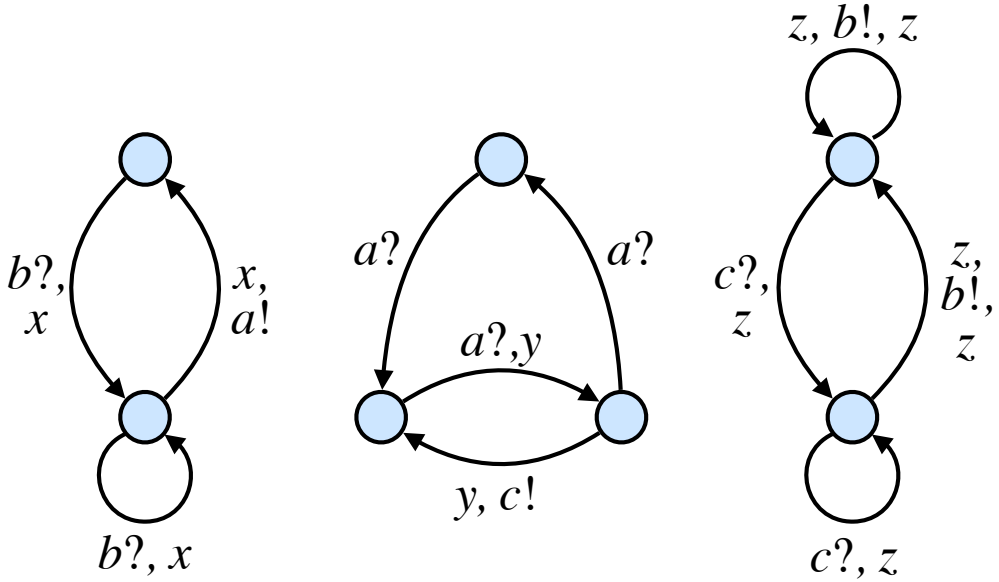
Análisis de resiliencia

Raúl E. Monti

Un par de desafíos

Carlos E. Budde

Modelado composicional



Redes de autómatas estocásticos con entradas y salidas (IOSA)

Simulación de eventos raros

- Preparado para Simulación por Eventos Discretos
- El problema de realizarla siguiendo la técnica de simulación Monte Carlo

…

Holger Hermanns
Matías D. Lee
Damián Barsotti

CONICET

UNC

Resiliencia en Sistemas Computacionales Complejos

Pedro R. D'Argenio

Dependable Systems Group
FaMAF, UNC - CONICET

http://dsg.famaf.unc.edu.ar

CONICET

Conferencia Gaviola, Noviembre 2015

UNC