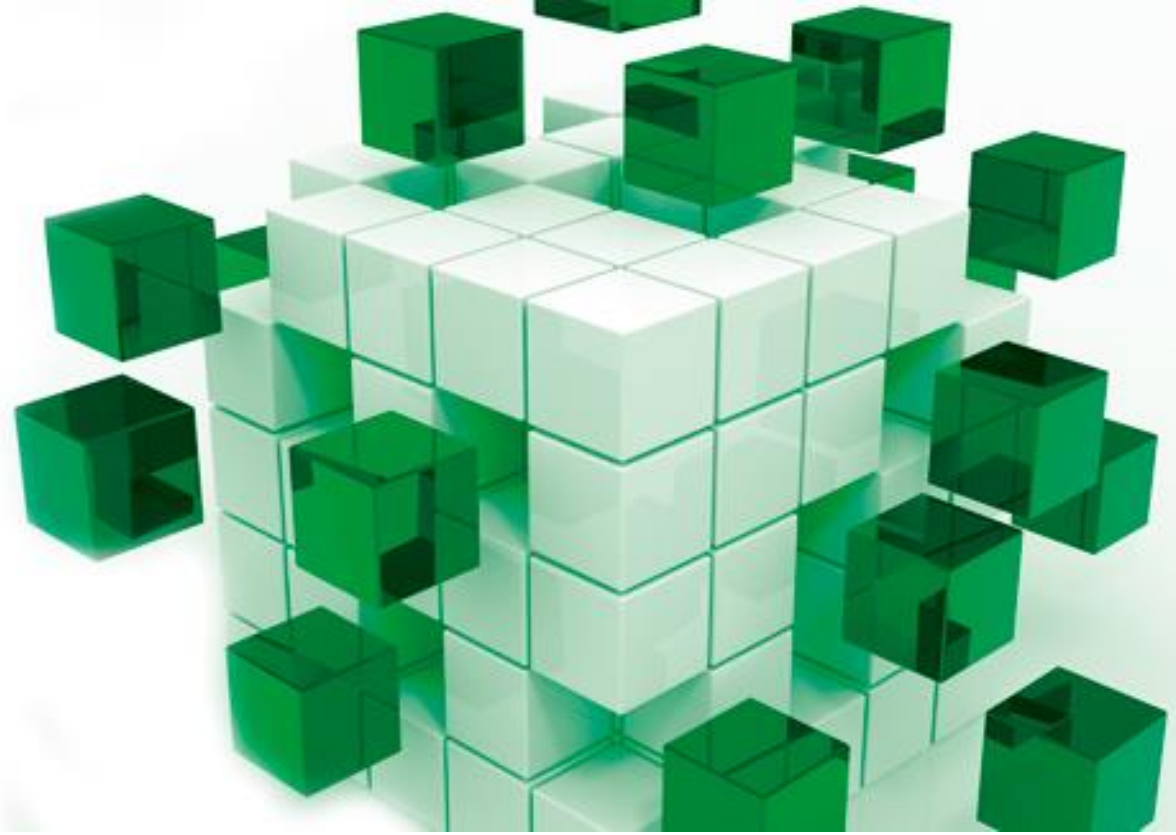


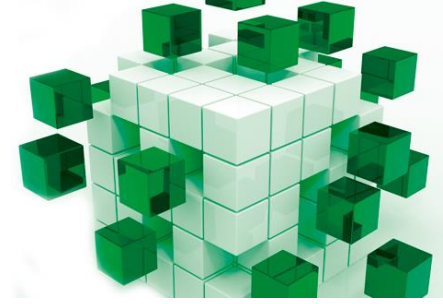
XVIII Congreso de Confiabilidad

Madrid. 23 y 24 de noviembre de 2016



Organiza:





DESARROLLO DE UN MODELO DE ERRORES HUMANOS EN EL SECTOR DE ESPACIO

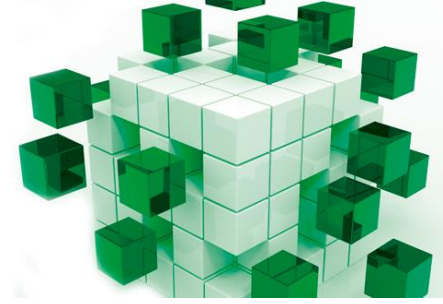
María Alonso López

Ingeniera de RAMS, GMV

INTRODUCCIÓN

PLANTEAMIENTO DEL PROBLEMA

Errores humanos

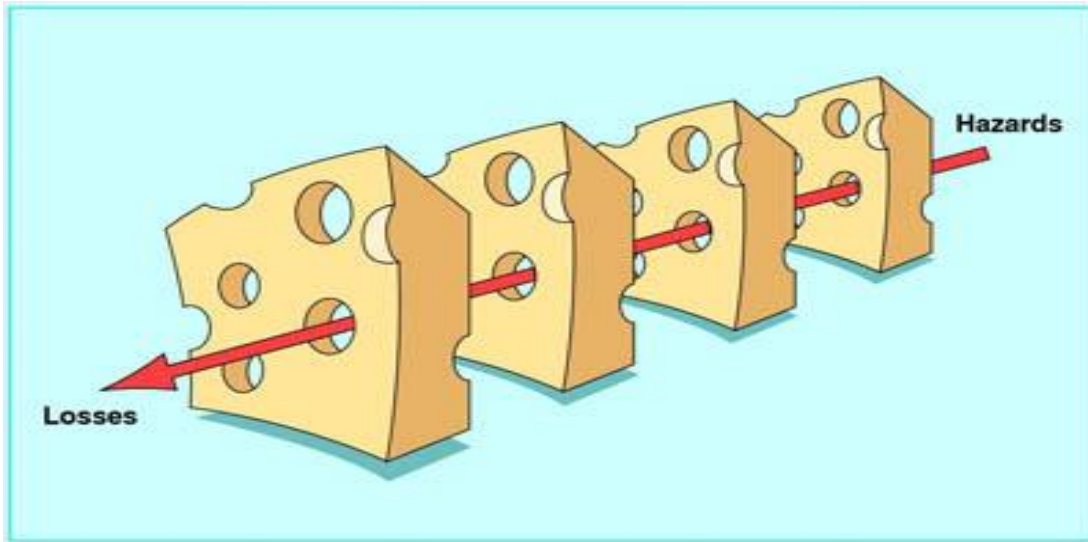
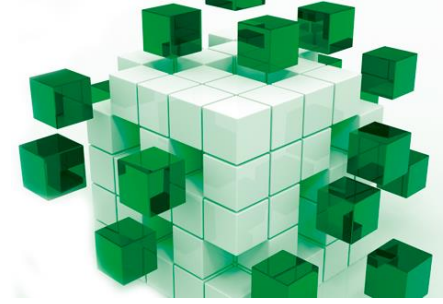


60% - 90% de los fallos de sistema están **causados por errores humanos**.

- ¿Error humano o error de diseño?
- ¿La automatización es la solución?



¿Por qué ocurren los errores?



- Alta temperatura
- Errores de mantenimiento
- No había alarmas
- Error del piloto (flaps)
- No hay checklist



UN ACERCAMIENTO AL

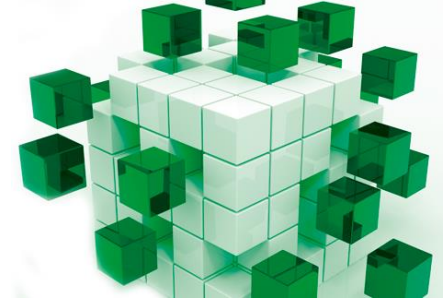
ANÁLISIS DE ERRORES HUMANOS

“Errar es humano, pero los errores pueden prevenirse.”

US National Institute of Medicine



Resumen de la metodología



Describir el proceso por el que ocurren los errores, identificando las causas de los errores humanos



Definir los escenarios de fallos humanos teniendo en cuenta la propagación de errores (condiciones dinámicas)

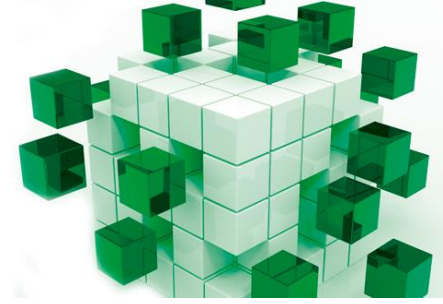


Crear una base de datos de errores humanos con modos de fallo, precursores y recomendaciones



Definir un proceso que integre el análisis de errores humanos en el ciclo de vida del proyecto

Análisis de causas de errores humanos



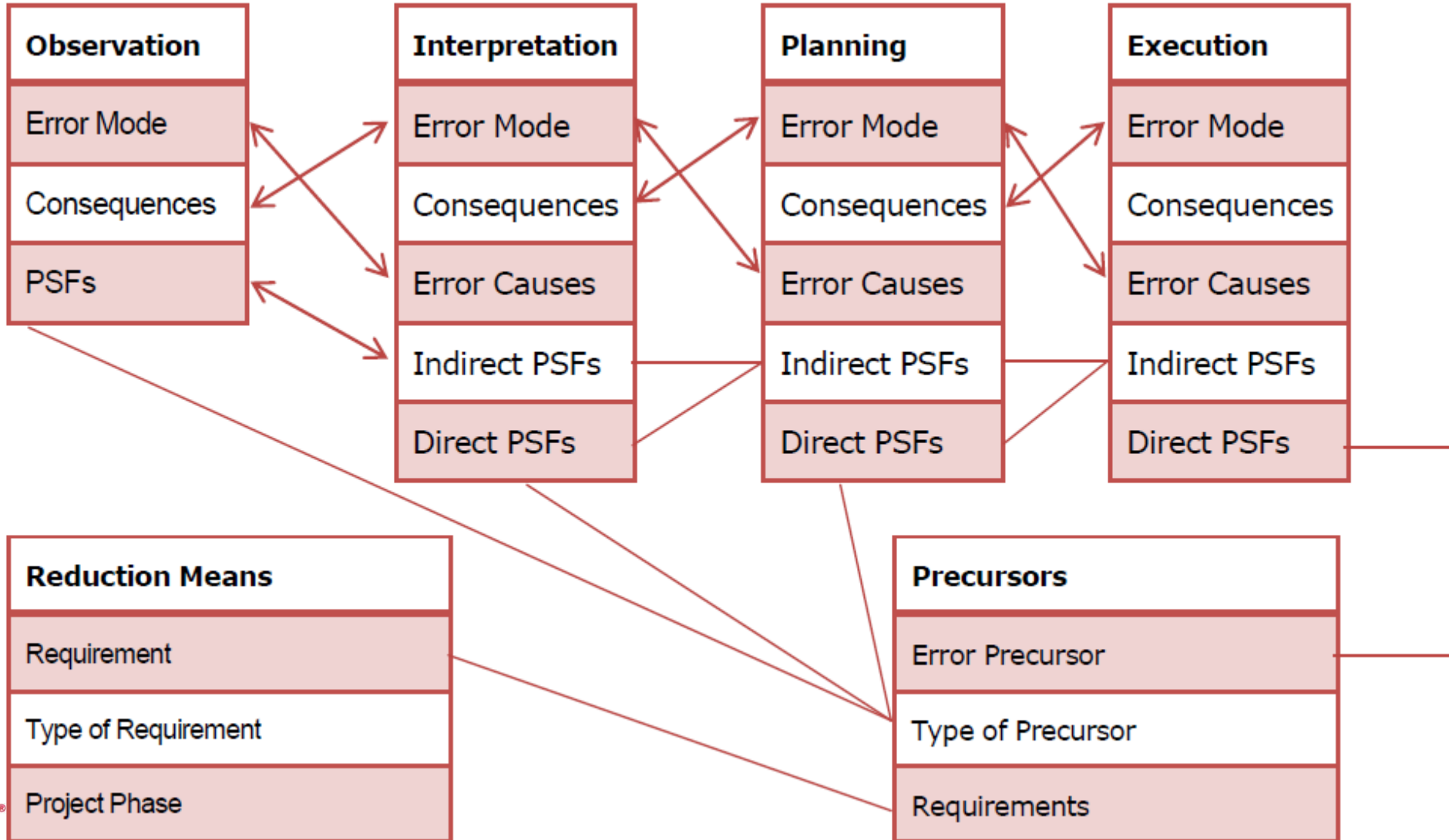
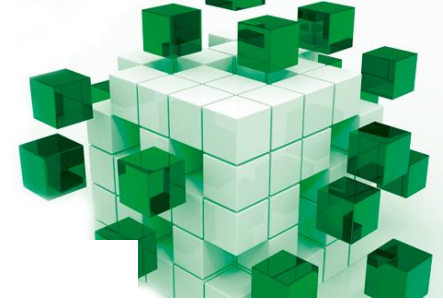
¿Por qué ocurren errores? → Modelo de la cognición humana

- 1 • Eliminación de los errores
- 2 • Minimización de las consecuencias
- 3 • Medidas de control

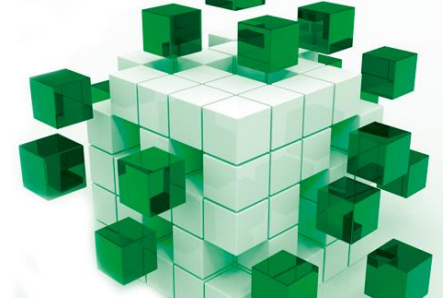
Foco de atención: **LOS PRECURSORES**



Estructura de la base de datos



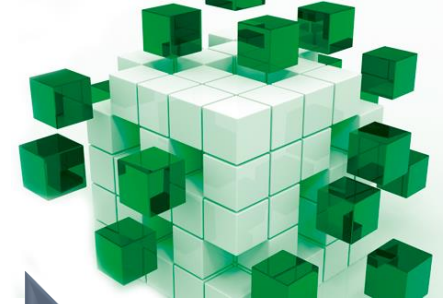
Fases de un proyecto de espacio



- Fase 0 – Identificación de necesidades y análisis de misión
- Fase A – Factibilidad
- Fase B – Definición preliminar
- Fase C – Definición detallada
- Fase D – Producción y cualificación
- Fase E – Utilización
- Fase F – Desactivación

Activities	Phases						
	Phase 0	Phase A	Phase B	Phase C	Phase D	Phase E	Phase F
Mission/Function	↓ MDR		↓ PRR				
Requirements	↓ SRR			↓ PDR			
Definition			↓ CDR				
Verification				↓ QR			
Production					↓ AR ↓ ORR		
Utilization					↓ FRR	↓ CRR	↓ ELR
Disposal						↑ LRR	↓ MCR

Análisis de errores humanos en el ciclo de vida



HUMAN FACTORS ENGINEERING

Phase 0

Phase A

Phase B

Phases C-D

Lessons Learnt
from missions

Preliminary
Human Error
Analysis

Update Human
Error Analysis

Collect Human
Error Data

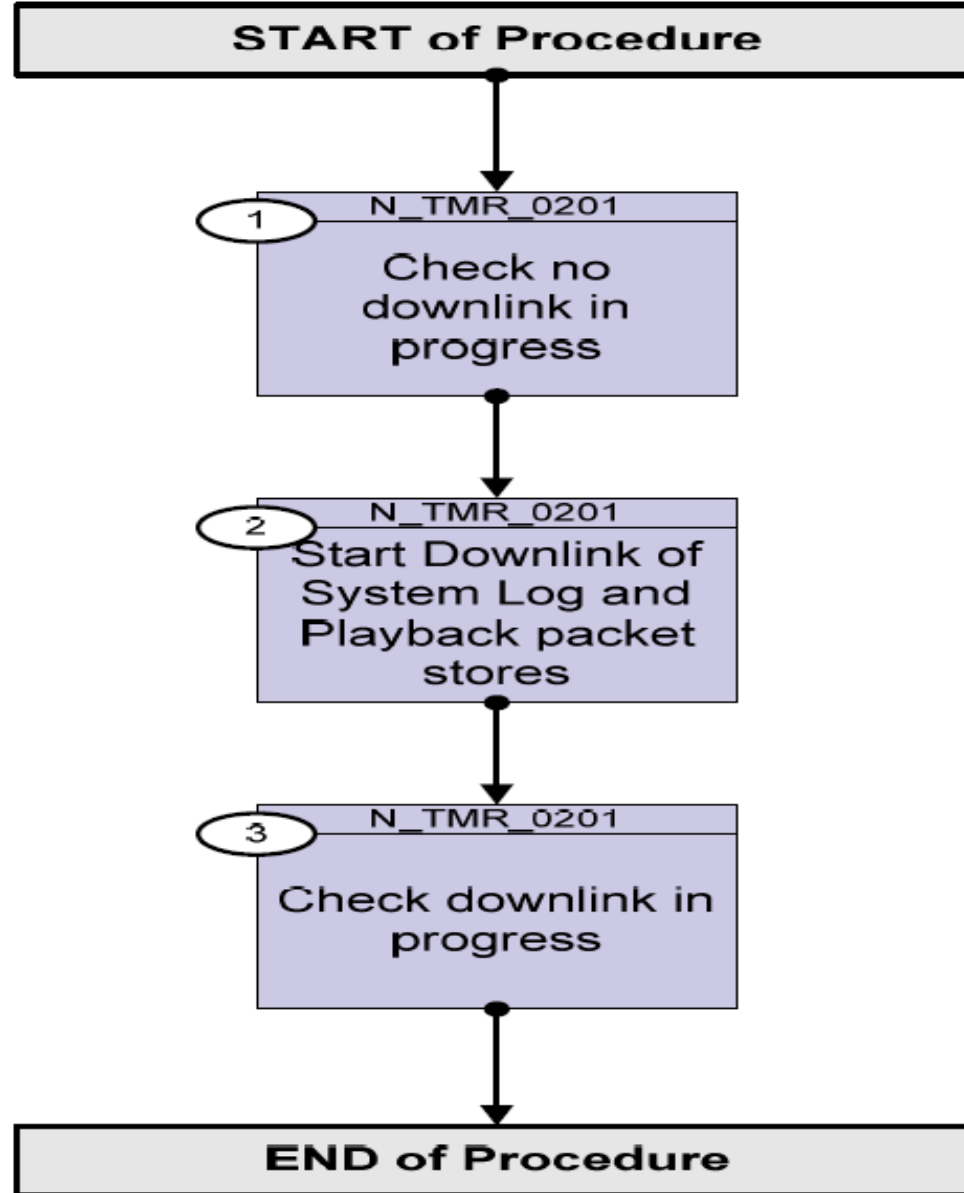
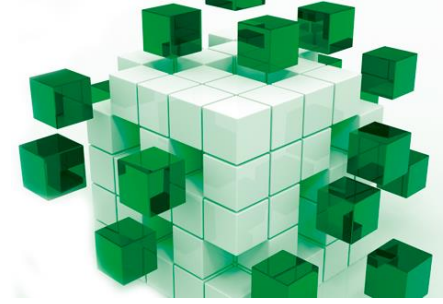
PROCEDIMIENTO OPERACIONAL

CASO DE ESTUDIO

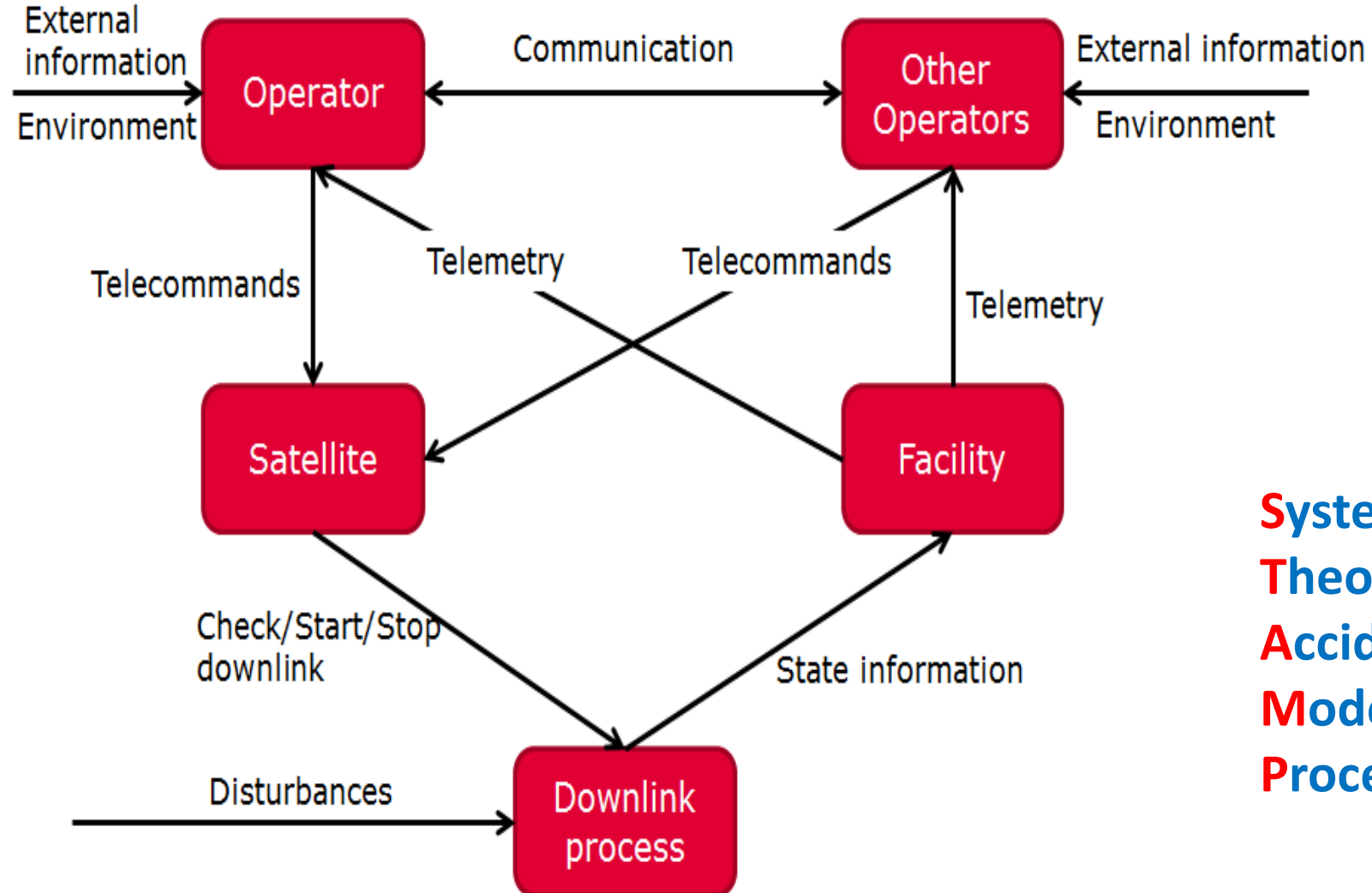
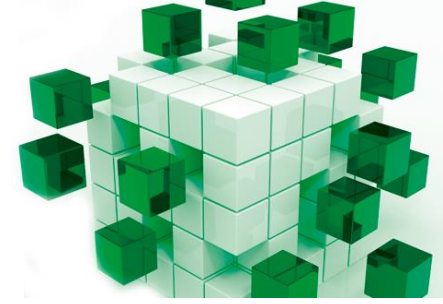


gmv[®]
INNOVATING SOLUTIONS

Resumen del Procedimiento



STAMP: Diagrama de control



Systems-
Theoretic
Accident
Modelling and
Processes

Fallos del procedimiento



- El **tiempo necesario** para realizar cada tarea (comprobación, descarga) no está descrito.
- No queda claro si existe un **orden específico** para llevar a cabo las tareas de cada paso. No hay restricciones de secuencia.
- El tiempo requerido y el **momento de realización** de las acciones no queda descrito en el procedimiento.
- No se especifica **cuándo se debe detener la descarga** en proceso y cuándo se debe rechazar la descarga nueva.
- El procedimiento para detener la descarga no está claramente identificado.
- No está descrito con claridad **cuándo concluye una acción** y cuándo se debe iniciar la siguiente.

Tabla del análisis



Id	Task	Human Error Mode	Effect	Conseq.	Sever.	Human Cause Error	Precursors	Error Reduction Means
E31	Comenzar descarga de los paquetes.	El telecontrol de descarga no se ejecuta.	No hay descarga	Sin datos de telemetría	2	No se toma una decisión.	El tiempo necesario para realizar cada tarea (comprobación, descarga) no está descrito	Describir claramente el proceso de descarga en términos de: <ul style="list-style-type: none"> • Objetivos • Necesidades de tiempo. • Pasos para llevarlos a cabo. • Restricciones. • Momento de inicio y finalización.

Recommendations



- Describir cada tarea de forma clara: Objetivos, necesidades de tiempo, pasos para llevarla a cabo, restricciones, momentos de inicio y finalización.
- Las acciones a llevar a cabo cuando los outputs no son los esperados deben ser claramente. Describir las condiciones para abortar el procedimiento.
- Describir el tiempo mínimo y máximo para cada tarea.
- Debe quedar claro cuándo el operador debe abortar la nueva descarga.
- Caracterizar la tarea de detención.
- La información proporcionada por las interfaces debe ser completa, clara y sin ambigüedades. Todos los botones deben estar etiquetados para indicar su efecto.
- Los datos de telemetría deben ser fáciles de interpretar y los telecontroles deben ser intuitivos.

CONCLUSIONES

WORK SUMMARY



- El ser humano está presente e interacciona con sistemas críticos. Esto hace el **análisis de errores humanos necesario**.
- Hemos desarrollado un modelo de ***Human Dependability*** a partir de un handbook de la ESA que va paralelo al ciclo de vida del proyecto con el objetivo de completar los análisis de RAMS de todo sistema, permitiéndonos **identificar, mitigar y controlar los errores humanos**.
- Este modelo es una **combinación de diferentes técnicas de análisis de RAMS**; está basado en el proceso de cognición humano y nos permite diseñar el sistema y los procedimientos operacionales en base a las necesidades de *Human Safety* y *Human Dependability*.
- Hemos aplicado nuestro modelo a un **caso de estudio**, un **procedimiento operacional de un sistema de control de satélites**, estudiando sus beneficios y aplicabilidad.



¡Gracias!

María Alonso López
Isabel Bachiller Martínez
Marta López Caamaño
Marta Fernández Campo

www.gmv.com

gmv[®]
INNOVATING SOLUTIONS