# Training on CLC TS 50701


Jesus Molina

Director of Industrial Security
Waterfall Security Solutions

Lecturer
Universitat Politecnica de Catalunya

# AGENDA

- Course Details
- Exercises
- TS-50701 Takeaways
- Other Industries



waterfall

# The Course

- Taught at UPC Vilanova I la Geltru Campus
- Financed by the Ministry of Transportation
- Hybrid format
- Focus on Rail Professional
- Postgraduate degree in Cybersecurity in Rail Networks, issued by the Universitat Politècnica de Catalunya.

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
School of Professional & Executive Development

GOBIERNO DE ESPAÑA
MINISTERIO DE TRANSPORTES Y MOVILIDAD SOSTENIBLE

Plan de Recuperación, Transformación y Resiliencia

Financiado por la Unión Europea
NextGenerationEU



waterfall

# Teaching Staff

Miquel Soriano

Josep M. Pegueroles

Juan Hernández

Jesus Molina

Omar Benjumea


Lluís Monjo

Maite Morillo + Noé Jimenez

# Next to the Museo del Ferrocarril



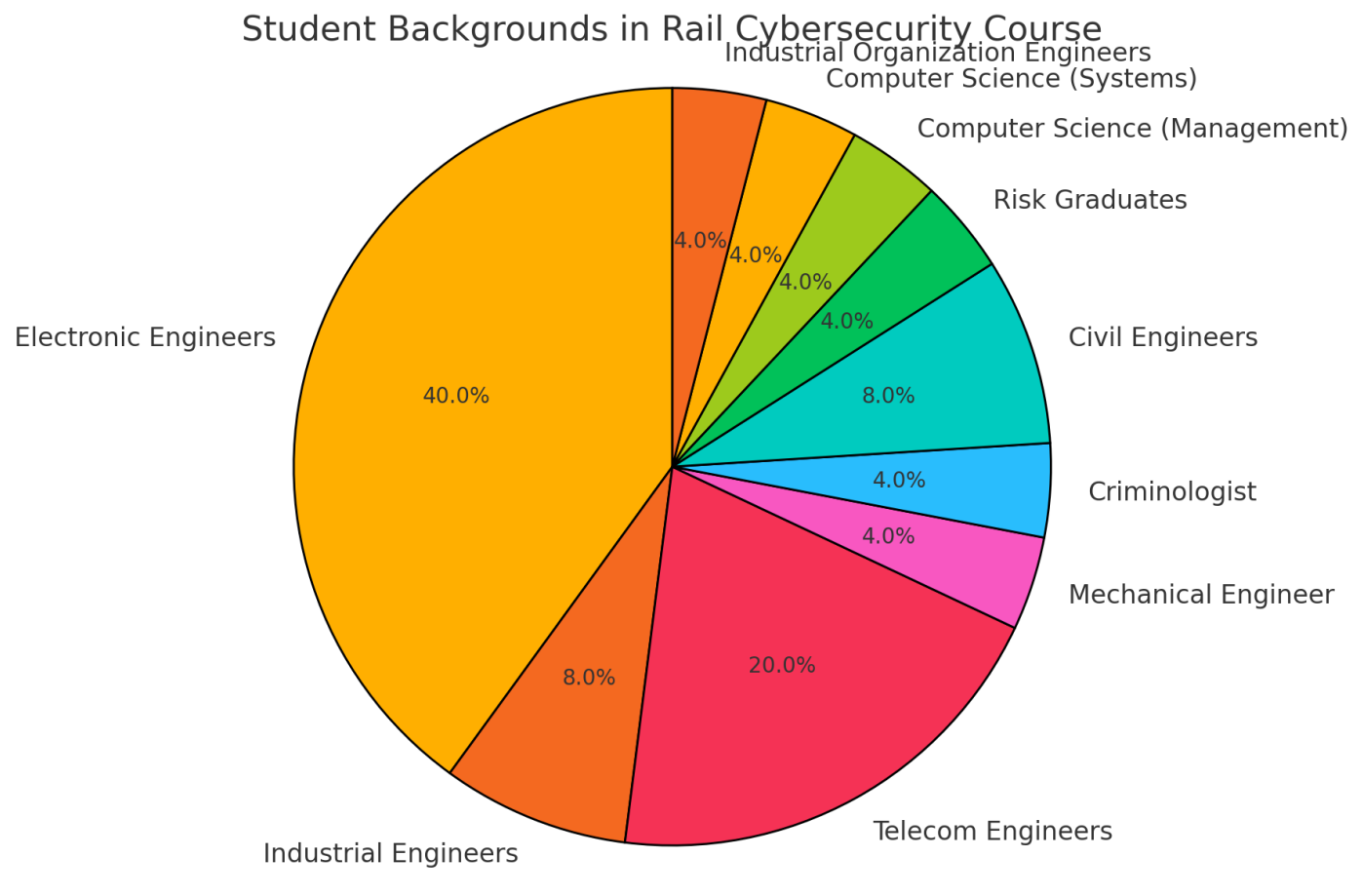

waterfall

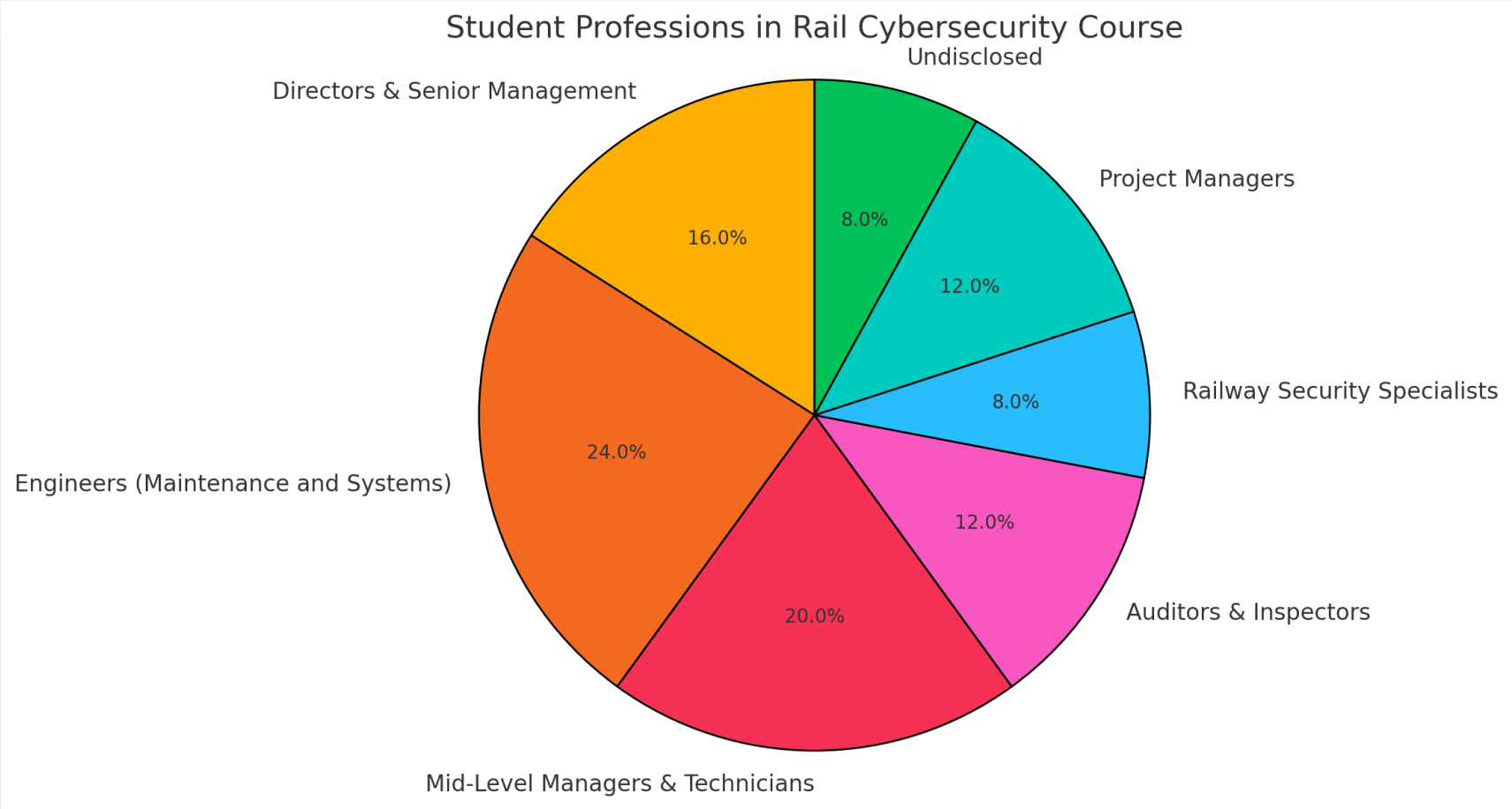
# The Students

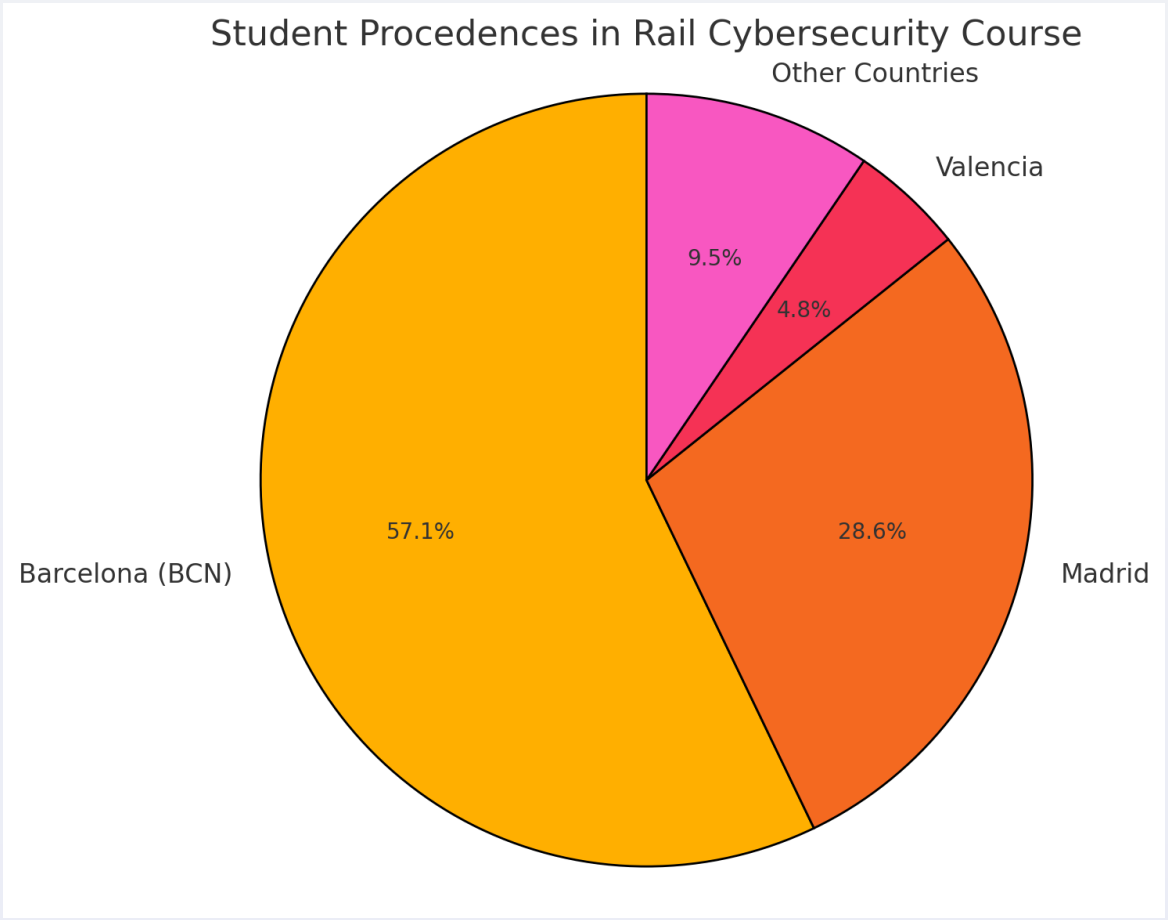
- **23 Students**
- **Professional Backgrounds**
- **Mostly from Spain**



waterfall







# Course Plan

- Introduction to Cybersecurity in Rail Systems
- Regulation of Rail Cybersecurity
- Cybersecurity Assessment in Rail Systems
- Cybersecurity Measures
- Practical Cases and Projects



waterfall

# The Course

- Theory and Practice
- Eight practical exercises plus final project
- Practical exercises for both train and infrastructure (Risk assessments, deployment of controls, etc)
- Use of Gen AI to create realistic complex target systems (e.g. on train network)




waterfall

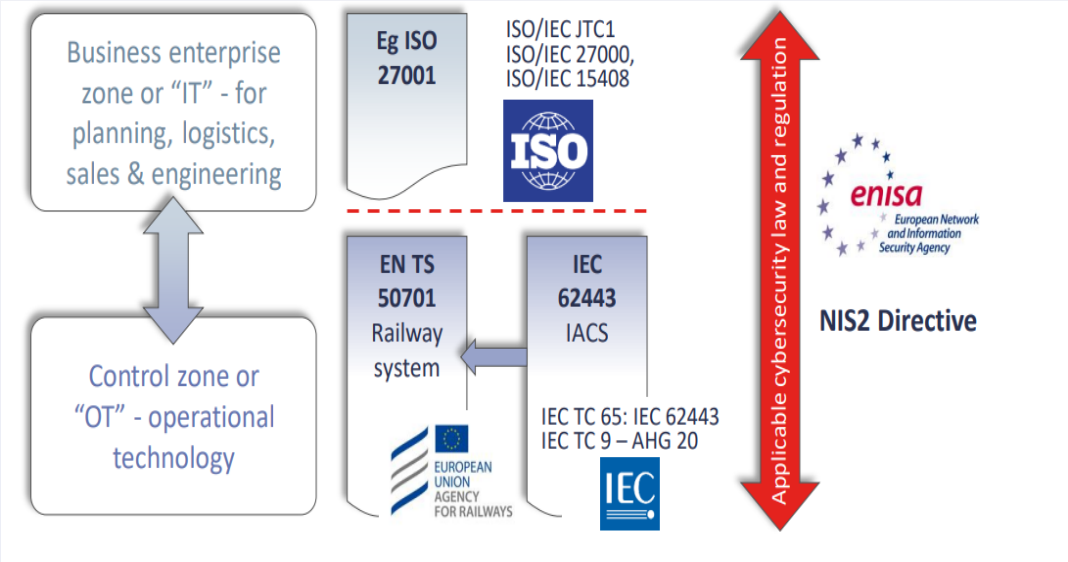
waterfall

# TS-50701 Takeaways

## Positive

# TS-50701 as an Effective Teaching Document

- **Helps create a structured learning path for cybersecurity in rail networks**
- **Ideal as a "textbook" for professionals entering cybersecurity**
- **Bridges the gap for students without a cybersecurity background by offering a practical understanding of 62443 standards**
- **Practical procedures make it easier for students to follow and apply in real-world scenarios.**






waterfall

# Bridging the Knowledge Gap

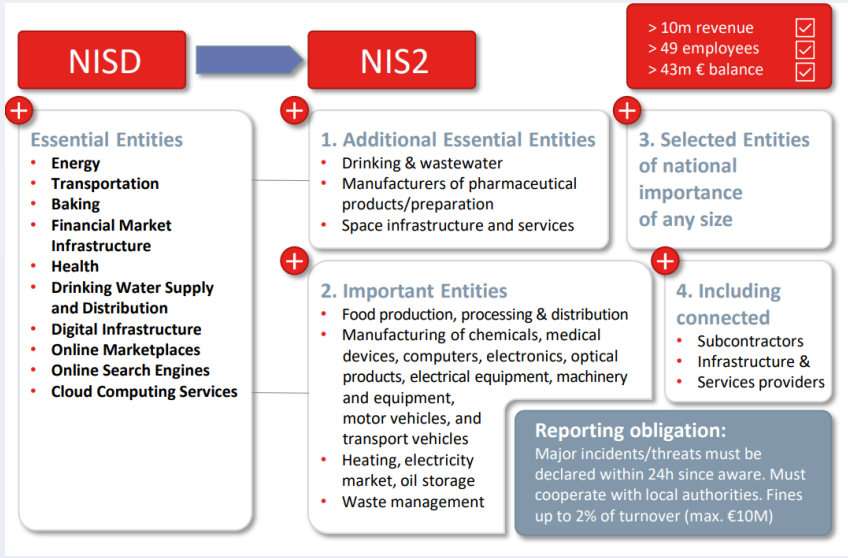
- Accessible to professionals with no prior cybersecurity experience, particularly those from the rail industry.TS-50701 links cybersecurity concepts with familiar aspects of rail safety and operations (e.g., Section 2 on safety)
- Helps students relate existing knowledge of rail networks to new cybersecurity requirements
- More effective than starting with IEC 62443, which can be too technical and complex for newcomers
- Templates (e.g. zoning) bridge the gap between existing knowledge and new cybersecurity concepts.



waterfall

# Regulatory Alignment and Future Relevance

- Addresses concerns about regulation, specifically NIS 2
- Aligns with Article 25, which requires European standards where possible
- Though not yet a standard, TS-50701 aligns with upcoming compliance requirements
- Students felt empowered by learning a standard that will be essential for future compliance with NIS 2
- Provides a master plan for building a cybersecurity strategy that meets regulatory demands




waterfall

waterfall

# TS-50701 Takeaways

## Negative – or better - Opportunities

# Challenges with Risk Assessment Templates

- Risk assessment templates in TS-50701 were not as useful compared to other templates (e.g., zoning and segmentation)
- Students often created their own risk assessment templates based on IEC 62443, leading to inconsistency
- Confusing guidance: TS-50701 didn't provide clear instructions on how to connect risk assessments with zoning and conduits
- Likelihood-based assessments were problematic, as different professionals had varying interpretations of likelihood
- Recommendation: Future versions of TS-50701 should provide stricter, more consistent templates for risk assessments
- Shift towards consequence-based assessments: Suggest moving from likelihood to consequence-based risk assessments, which are easier to align with zoning and criticality.



waterfall

| N° | ELEMENTO | LISTADO DE EVENTOS CON RIESGO (01/12/2023) | DEFINICIÓN DE LOS RIESGOS POTENCIALES (01/12/2023) | ZONA (01/12/2023) | ZONA SEGUN NORMA (02/12/2023) | ZONA REAL (02/12/2023) | Confidencialidad | Integridad | Disponibiliad |
|---|---|---|---|---|---|---|---|---|---|
| 1 | Unidad de Control Principal | - Intrusión en la controlita si esta se encuentra en red.<br>- Fallo de conectividad con otros elementos/equipos del tren.<br>- Fallo de alimentación. | Acceso No Autorizado: Riesgo de que personas no autorizadas obtengan acceso al sistema, lo que podría llevar a manipulación de datos o interrupción del servicio.<br><br>Ataques de Ingeniería Social: Posibilidad de que los usuarios sean engañados para revelar información confidencial o credenciales de acceso<br><br>Error de Configuración: Realización de tareas para la puesta en funcionamiento<br><br>Interrupciones en el Suministro de Energía y conexiones : La falta de suministro eléctrico podría afectar el funcionamiento del sistema | Operacional | ZC-L5 | | Medio | Bajo | Bajo |
| 2 | Sistema de Aire Acondicionado | - Fallo en regulación de temperatura.<br>- Funcionamiento intempestivo.<br>- Manipulación del equipo por parte de otro sistema | Interrupciones en el Suministro de Energía: La falta de suministro eléctrico podría afectar el funcionamiento del sistema de aire acondicionado, lo que podría impactar negativamente en la comodidad de los pasajeros.<br><br>Fallos Técnicos No Detectados: Riesgo de que los fallos en el sistema no sean identificados a tiempo, lo que podría resultar en la falta de refrigeración en áreas críticas. | Operacional | ZC-L1 | | Medio | Medio | Alto |
| 3 | WC Estándar y PMR | - Entrada del PLC del sensor de "baño ocupado".<br>- Intrusión en el funcionamiento de los elementos del baño (WC, secador, etc.) | Fallos Técnicos o Bloqueos: Riesgo de mal funcionamiento de los sistemas de WC, lo que podría causar molestias a los pasajeros o interrupciones en el servicio.<br><br>Vandalismo: Posibilidad de daño deliberado a los sistemas de WC, lo que podría afectar su funcionamiento y requerir reparaciones costosas. | Operacional | ZC-L2 | | No aplica | No aplica | No aplica |
| 4 | Sistema de Video Vigilancia CCTV | - Fallo de configuración.<br>- Fallo del equipo por intrusión.<br>- Fallo debido a manipulación externa.<br>- Fallo en la emision de datos al exterior por confidencialidad e integridad. | Acceso No Autorizado a las Imágenes: Riesgo de que personas no autorizadas obtengan acceso a las imágenes de CCTV, comprometiendo la privacidad y seguridad.<br><br>Sabotaje: Posibilidad de que los dispositivos de CCTV sean dañados intencionalmente, dejando áreas sin supervisión | Integridad, disponibilidad y confidencialidad | ZC-L3 | | Alto | Alto | Medio |
| 5 | Sistema de Información al Pasajero | - Intercepción por acceso a la red interna del tren.<br>- Fallo de la configuración por mala instalación. | Manipulación de Información: Riesgo de que se introduzca información falsa en los sistemas de información, lo que podría causar confusión y afectar la confianza de los pasajeros.<br><br>Interrupciones del Servicio: Posibilidad de que el sistema experimente interrupciones, lo que podría dejar a los pasajeros sin información actualizada. | Integridad, disponibilidad y confidencialidad | ZC-L3 | | Medio | Alto | Medio |
| 6 | Registrador de Eventos | - Posible manipulación de datos en entre la captación y el ordenador principal.<br>- Fallo en la cronología de los eventos. | Pérdida de Datos Críticos: Riesgo de que se pierdan datos importantes debido a fallos en el sistema, lo que podría afectar la capacidad de investigar incidentes.<br><br>Manipulación de Registros: Posibilidad de que los registros sean manipulados para ocultar eventos no deseados. | Integridad, disponibilidad y confidencialidad | ZC-L5 | | Alto | Alto | Muy Alto |
| 7 | Sistema de Comunicación GSM-R | - Fallo de comunicación y envío de datos.<br>- Intrusión en la frecuencia de funcionmiento. | Intercepción de Comunicaciones: Riesgo de que las comunicaciones sean interceptadas, comprometiendo la confidencialidad de la información transmitida.<br><br>Fallos en la Red: Posibilidad de que la red experimente fallos, lo que podría afectar la comunicación crítica entre trenes y estaciones. | Operacional<br>o<br>Integridad, disponibilidad y confidencialidad | ZC-L5 | | Alto | Alto | Alto |

| | | | LIKEHOOD | | | | |
|---|---|---|---|---|---|---|---|
| | | | EXP | VUL | L | THREAD RISK | ASSET ZONE |
| Unidad de Control Principal | Parar el tren | C | 1 | 2 | 2 | Low | ZC-RS 5 |
| | No poder parar el tren | A | | | | Significant | |
| | No se pueda detectar un fuego | A | | | | Significant | |
| | No se pueda detectar sobretemperatura de rodadura | A | | | | Significant | |
| | Bloquear DMI u otras pantallas en cabina | C | | | | Low | |
| | Corte de sistema eléctrico de servicio del tren (pantógrafo, disyuntor, …) | C | | | | Low | |
| Sistema de Aire Acondicionado | Que no funcione el aire ac | C | 2 | 2 | 3 | Medium | ZC-RS 4 |
| WC Estándar y PMR | Inutilizar los servicios WC | D | 2 | 2 | 3 | Low | ZC-RS 3 |
| Sistema de Video Vigilancia CCTV | Acceso a las imágenes CCTV | B | 2 | 2 | 3 | Significant | ZC-RS 3 |
| Sistema de Información al Pasajero | Exhibición de imágenes/audios inapropiados en sist. Info. al viajero | D | 2 | 2 | 3 | Low | ZC-RS 3 |
| | No permitir la exhibición de imágenes/audios | D | | | | Low | |
| Registrador de Eventos | Alterar datos del JRU / event recorder | D | 1 | 2 | 2 | Low | ZC-RS 5 |
| Sistema de Comunicación GSM-R | Que no pueda comunicarse datos con centro de control (CRC, RBC) | B | 1 | 2 | 2 | Medium | ZC-RS 5 |
| | Que no pueda comunicarse voz con centro de control (CRC) | D | | | | Low | |
| Sistema de Detección de Incendios | No se pueda detectar un fuego | A | 2 | 2 | 3 | High | ZC-RS 4 |
| Conexión WiFi | Robo de datos de pasajeros | B | 3 | 2 | 4 | High | ZC-RS 1 |
| Sistema Contador de Pasajeros | Manipulación del conteo automático de pasajeros | D | 2 | 2 | 3 | Low | ZC-RS 3 |

# Freshening Up Controls

- Lack of clarity on control types in TS-50701, especially regarding physical vs. software controls (e.g., firewalls, gateways, data diodes)
- IEC 62443-3-3 (2013): Controls are somewhat outdated; an opportunity exists to refresh controls for rail-specific needs
- Importance of physical controls: Rail systems rely on physical safety mechanisms (e.g., relays) to prevent system damage, not fully accounted for in IEC 62443-3-3
- Confusion among students: Some students struggled to differentiate between physical and software controls, particularly when performing detailed risk assessments



waterfall

# Detailed Risk Assessments

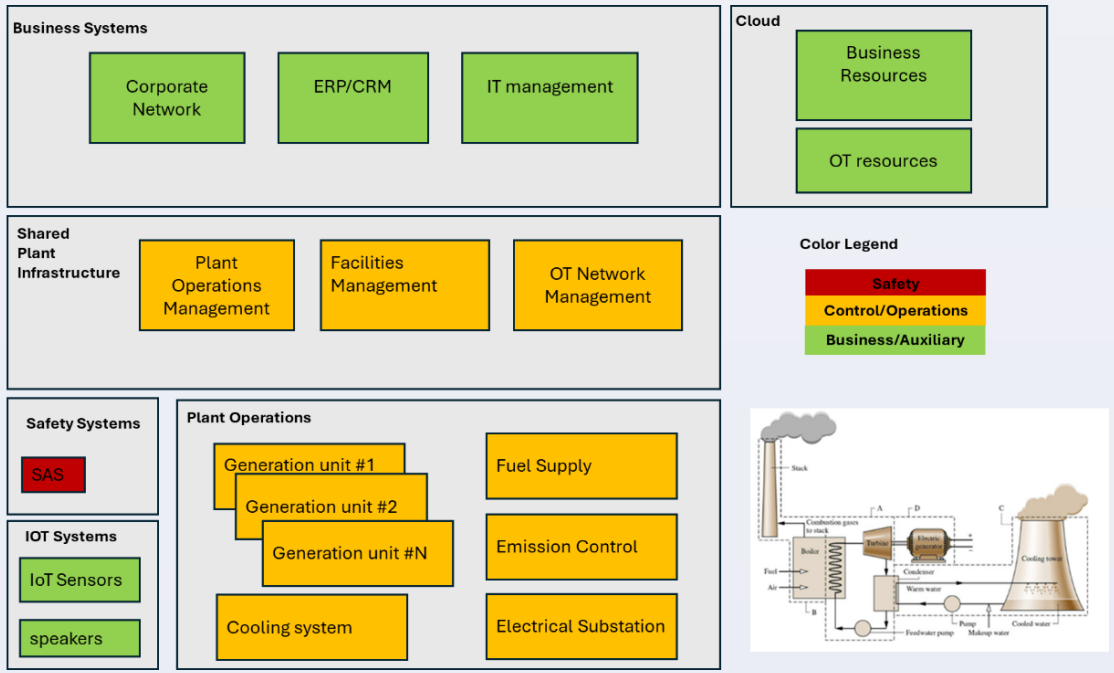
- **Detailed risk assessments: Section 7 in TS-50701 briefly touches on risk assessment vectors (e.g., SL vectors), but students found it confusing**
- **Opportunity to provide practical examples on how to perform detailed risk assessments, particularly for rail systems**
- **Adding an appendix for detailed risk assessment methods, similar to how conduits are discussed, would be beneficial for students and professionals alike**

waterfall

# Final Thoughts: Other Industries

# Maybe More than Rail?

- **TS-50701 can inspire other industries**
- **I will discuss this in the upcoming S4 conference in Tampa**









waterfall