

INGENIERIA DEL PLAN DE SEGURIDAD INDUSTRIAL EN UNA CENTRAL NUCLEAR

Fernando MARINAS GARCIA

El presente artículo está orientado a centrales nucleares de agua ligera (PWR, BWR), que sigan la normativa americana para el diseño del Plan de Seguridad Industrial, el cual es necesario realizar para el licenciamiento de la Instalación.

INTRODUCCION

El objetivo de la Seguridad Física o Industrial («Security») es evitar el robo o dispersión de materiales nucleares y los actos de sabotaje que produzcan emisiones radiactivas, las cuales pongan en peligro la salud pública y las instalaciones.

Por consiguiente, la seguridad nuclear («Safety») y la seguridad física («security») tienen aspectos comunes en cuanto a sus objetivos y, por tanto, tienen interfases en el diseño y operación de la Planta.

Como conclusiones de este artículo podríamos adelantar que se proponen las siguientes:

- El Plan de Seguridad Física («Security») debe integrarse como un sistema más de la Planta, realizándose el proyecto e implementación del mismo simultánea y coordinadamente con el resto de sistemas.
- El Plan de Seguridad, aún siguiendo normas y criterios generales exigibles, debe ser específico de cada central, en base a la diversidad de condicionantes locales posibles.

NORMATIVA

Los riesgos que comportan las instalaciones nucleares ante una amenaza de tipo intencionado, robo o sabotaje, que pudieran ocasionar fugas radiactivas o dispersión del material nuclear, poniendo en peligro la salud pública y la propia instalación, hacen que la responsabilidad de tales riesgos no sea exclusiva de las propiedades, sino también de las autoridades civiles y militares.

Por consiguiente, para las centrales nucleares se exige el cumplimiento de una normativa o requisitos específicos en relación con las medidas de Seguridad Física que han de ser implementadas, las cuales, hacen licenciable a la Central por los organismos oficiales competentes en esta materia.

Desde el año 1977 en que aparece en USA la norma 10CFR73.55 se está exigiendo, en los reactores de origen americano, el cumplimiento de la misma para su licenciamiento en cuanto al sistema de Seguridad Física. Anteriormente a esta norma, el diseño de medidas de seguridad se inspiraba en las normas ANSI N18.17 (1973) y Regulatory Guide 1.17 (1973), menos restrictivas que la 10CFR73.55.

Actualmente, la observancia de esta normativa 10CFR73.55 se ha hecho general, utilizando además otras guías re-

guladoras y documentos que orientan el diseño de detalle del Plan de Seguridad en una Central Nuclear.

Entre los documentos y guías que se utilizan como referencia para las distintas fases del diseño, podemos mencionar los siguientes:

- * **REGULATORY GUIDES: RG 1.17; RG5.7; RG5.44**
- * **NUREG: 0178, 0207, 0219, 0220, y 0908**
- * **REVIEW GUIDELINES: NO.4; NO.10**
- * **OTROS DOCUMENTOS: MANUALES DE LABORATORIOS SANDIA ANSI-N18.17 I.A.E.A. INF/CIRC.225 GSA-WA-00450B**
- * **GUIAS DE SEGURIDAD NUCLEAR: GSN-07/78; GSN-06/78**

En este punto conviene hacer unas consideraciones respecto a la normativa aplicable:

● La normativa está condicionada de alguna forma por el espectro de amenazas que se postulen.

● Las amenazas previsibles dependen de muchas variables (políticas, sociales, idiosincrasia de los individuos, entorno, etc.).

● La normativa americana tiende a enfatizar la amenaza del «insider»; la postura europea es de prestar más atención a los individuos y grupos ajenos a la instalación.

Este enfrentamiento entre las premisas europeas y las americanas se constató en el «II Workshop sobre Planes de Seguridad en Centrales Nucleares» celebrado el año 1983 en Savannah, Georgia (USA).

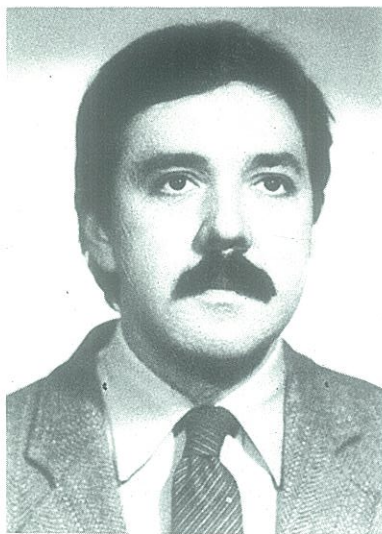
La normativa americana que se aplica establece, entre otros considerandos:

- * Áreas vitales tipo I y II.
- * Separación y compartimentación de las áreas tipo I y II.
- * Regla de los dos hombres.
- * Mayores controles en interior de edificios.
- * Selección y vigilancia del personal de la Planta.

Estos criterios de diseño conducen a:

- Unos costes mayores de equipos.
- Unos costes mayores en horas/hombre de personal de operación y mantenimiento.
- Una penalización en la operatividad de la Planta.

No obstante, el grado de seguridad que se consigue y la protección de los



Fernando MARINAS GARCIA es Ingeniero Industrial por la Escuela de Madrid. Desde el año 1973 trabaja en Ingeniería de Centrales Nucleares en el área de control, orientando su actividad hacia el área de seguridad industrial a partir del año 1978. Ha participado, entre otros, en planes de seguridad de la C. N. Ascó y de la C. N. Vandellós II, actuando en esta última como Director de Proyecto y Gerente Adjunto de la Unión Temporal INITEC-SEPISA. Asistió al «Workshop sobre Planes de Seguridad en Centrales Nucleares» en USA en el año 1983.

objetivos que son susceptibles de amenaza son excelentes.

● Los organismos oficiales que tengan competencia en el licenciamiento de plantas nucleares deberían reflexionar en cuanto al alcance de las medidas de seguridad física que hay que exigir en una planta nuclear, considerando por un lado las amenazas razonables a postular, y por consiguiente, la normativa o guías que serían adecuadas exigir en el país en que se trate en orden a no penalizar innecesariamente los costes y operatividad de la Planta debidos al Plan de Seguridad Industrial.

En este sentido sería muy útil disponer de documentos anexos o guías reguladoras que complementarían la GSN-07/78 de la JEN y se dispusiera de normativa nacional propia para la implementación de medidas de seguridad física en centrales nucleares.

FILOSOFIA DE LA SEGURIDAD

El punto de partida para establecer la filosofía de seguridad lo constituye el «Análisis de Vulnerabilidad» donde se postulan todas las amenazas estableciendo una matriz de agresores/sucesos.

El espectro previsible de amenazas es único para cada central y depende de diversos factores locales (políticos, sociales, idiosincrasia del pueblo, ambientales, etc.).

Del análisis de este cuadro se establecen las amenazas más probables o nominales, las cuales han de servir para definir el Plan de Seguridad y que dicho Plan evite los efectos de las amenazas nominales postuladas.

Conviene recordar que un Plan de Seguridad Física en una instalación nuclear no está diseñado para protegerse de:

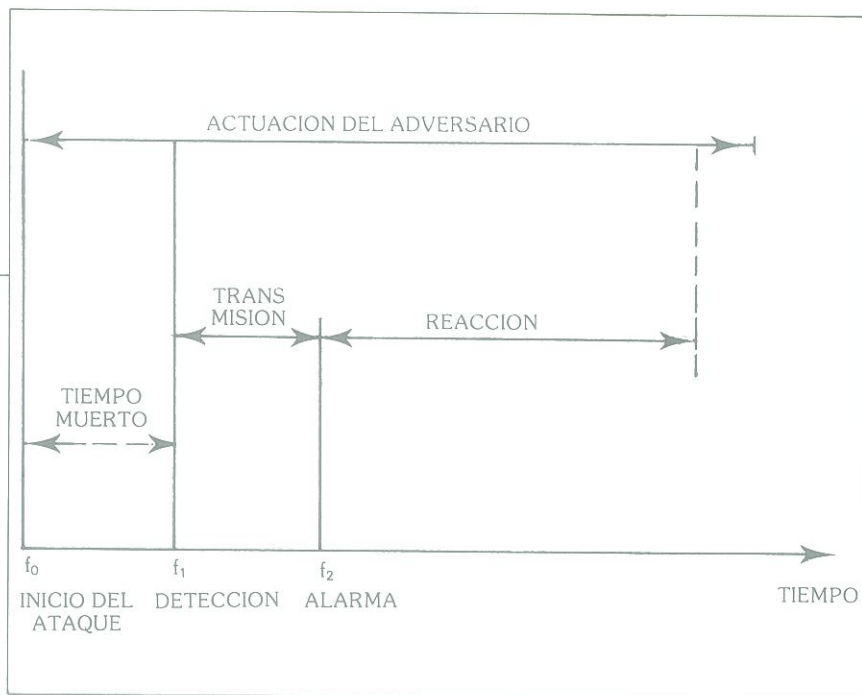
- Grupos con armamento pesado o paramilitares.
- Catástrofes naturales

Las medidas de seguridad física en una planta nuclear tienen un primer objetivo que es la **disuasión**.

Como segundo objetivo, en caso de producirse una amenaza, es el de contestar, y abortar dicha amenaza antes de que ésta se consuma (ver figura 1).

Para que el sistema de protección física sea, por tanto, efectivo han de estar sincronizadas y actuar adecuadamente las siguientes funciones:

Detección de intentos de intrusión no autorizada por individuos o de actos



FI Disposiciones de una planta

malintencionados realizados por personal interno o externo.

Comunicación de las señales detectadas y evaluadas en los sensores, hasta los centros de control donde se toman las decisiones de respuesta.

Retardo o impedimento de las intrusiones efectuadas en el área protegida para aumentar el tiempo de acceso a las áreas vitales.

Respuesta adecuada, efectuada por las fuerzas de la Organización de Seguridad con los guardas y equipo necesario para neutralizar la agresión que se produzca.

El «Análisis de Vulnerabilidad» define cuáles son los objetivos o blancos susceptibles de ataque o sabotaje; para lo cual hay que establecer un estudio de **Áreas Vitales**, definiendo, en primer lugar, los equipos y sistemas que se consideran vitales y posteriormente definir, según su situación, las Áreas Vitales a proteger. Para este procesose pueden

utilizar como herramienta de trabajo los «Árboles de Fallos» y «Diagramas Lógicos».

Las Áreas Vitales pueden dividirse en dos categorías o tipos I y II, según contengan o no en su interior sistemas o equipos redundantes y, por consiguiente, se precise de una sola acción o más acciones para conseguir un sabotaje con éxito.

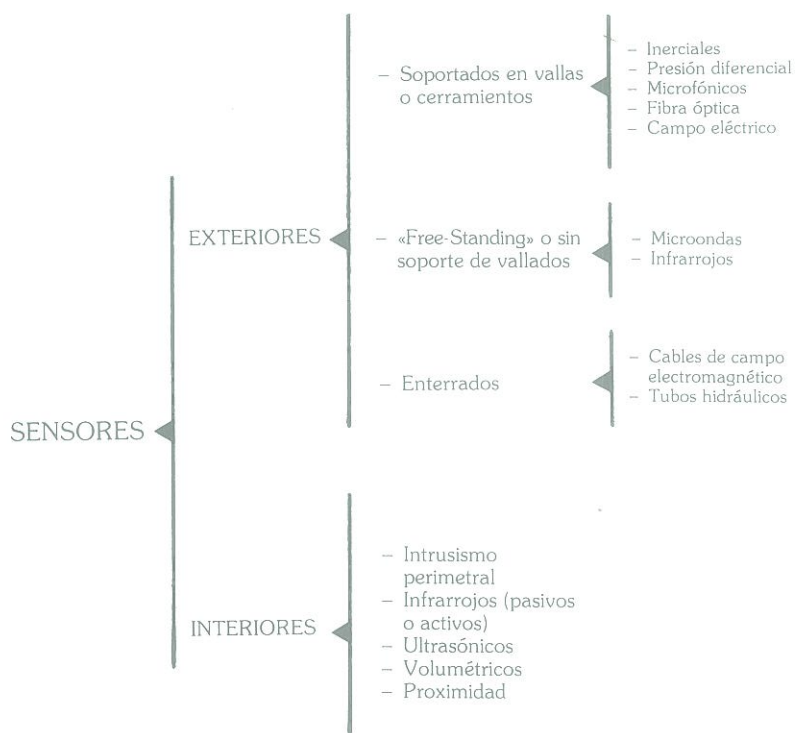
De las tres preguntas que se plantea un especialista en Seguridad Física a la hora de proteger una instalación: **¿Qué** hay que proteger?, **¿Contra quién** hay que proteger? **¿Cómo** hay que proteger?, con el «Estudio de Amenazas» y «Análisis de Áreas Vitales» que conforman el **Análisis de Vulnerabilidad**, se contestan las dos primeras.

Para contestar al **¿Cómo?** hay que definir las medidas de Seguridad Física, las cuales para un Plan de Seguridad de una central nuclear, las dividiremos en subsistemas y proceder a su definición e interfaces de unos con otros (ver tabla 1).

TI

SUBSISTEMA	FUNCIONES				
	Disuasión	Detección	Retardo	Comunicación	Respuesta
a) Vallado perimetral y cerramientos	X		X		
b) Detección intrusismo	X	X		X	
c) CCTV	X	X		X	
d) Control de Accesos	X	X	X	X	
e) Gestión de datos y control central				X	X
f) Alimentación Eléctrica		X (1)		X (1)	
g) Iluminación	X	X (1)			X (1)
h) Comunicaciones	X			X	X
i) Inspección	X	X	X		
j) Cables y conducciones		X (1)		X (1)	
k) Miscelaneos	X				X
l) Interfaces					

(1) Como subsistemas auxiliares a ciertas funciones.



Los subsistemas que conforman el sistema de seguridad de una central nuclear han de proporcionar en su conjunto las características fundamentales que debe tener el Plan de Seguridad:

- Defensas en profundidad.
- Impacto mínimo de un fallo de componente.
- Protección equilibrada.
- Seguimiento del adversario.

SUBSISTEMAS

A continuación se describen de forma muy sucinta los diferentes subsistemas en que podemos dividir el sistema de seguridad, los cuales actúan de forma integrada para que la información y actuación que proporcionan sea lo más eficaz posible en orden a tomar las acciones de respuesta más adecuadas y rápidas.

VALLADO PERIMETRAL Y CERRAMIENTOS

El vallado perimetral limita y conforma el «Área Protegida» de la Planta.

Puede estar formado este cerramiento por una o, mejor, dos vallas de tela metálica soportada a unos postes separados entre ellos (ver figura 2).

Las vallas estarán separadas entre sí una distancia de 6 m. aproximadamente. Esta zona de seguridad entre vallas no tendrá obstáculos superiores a 15 cm. sobre el suelo y carecerá de vegetación, para un buen funcionamiento de los equipos de Detección Perimetral y CC.TV.

A ambos lados de los dos vallados se dejarán unas «zonas de aislamiento» de unos 6 m. libres de obstáculos, edificaciones y/o vegetación para una mejor función de inspección y supervisión de la zona perimetral.

DETECCION DE INTRUSISMO

Lo componen fundamentalmente los sensores utilizados en áreas exteriores, y más concretamente los asociados al vallado perimetral y a las barreras físicas de las «Áreas Vitales Exteriores».

Los sensores pueden dividirse según la tabla 2).

La elección de un detector o sensor perimetral de exterior suele ser bastante compleja en función de las variables exteriores y que pueden ser las siguientes:

Topográficos

Declives, barrancos, acequias, ríos, montículos, etc.

Vegetación

Arboles, arbustos, hierbas, etc.

Vida animal

Topos, madrigueras, pájaros, insectos, etcétera.

Ruido de fondo

Tráfico, viento, tren, interferencias electromagnéticas, etc.

Meteorológicos

Viento, temperatura, lluvia, nieve, niebla, granizo, tormentas, corrosión aérea, etc.

Terreno

Humedad, composición química, etc. Para los enterrados.

Las características más importantes de los detectores de intrusismo son: Probabilidad de Detección, Vulnerabilidad del Sensor y Rango de Falsas Alarmas.

En algunos diseños puede ser aconsejable la disposición de dos sistemas de detección asociados a la barrera perimetral para minimizar el problema de las falsas alarmas y mejorarla probabilidad de detección. En estos casos existirán dos categorías de señales de alerta y alarma según actúe un sistema o los dos sistemas de detección.

CCTV

La función del sistema es de vigilancia de ciertas zonas sin necesidad de guardias en puestos locales para realizar tal misión. Además es un sistema de apoyo del de Detección Perimetral, así cuando actúa una alarma de una zona del perímetro, se conmuta automáticamente a un monitor de alarma la imagen de la cámara de televisión asociada a dicha zona.

Mediante el sistema CCTV y con sus cámaras motorizadas se puede seguir una hipotética intrusión en el Área Protegida.

Con cámaras de televisión interiores o exteriores, se controla e identifica a los individuos que acceden o pasan por determinadas dependencias o zonas vitales o de seguridad.

Es un subsistema de vigilancia que facilita a los guardias las funciones de control e identificación dando una información de primera mano que permite la toma de decisiones rápidas ante una amenaza de intrusismo o sabotaje.

Este subsistema permite, asimismo, reducir el número de guardas al eliminar ciertas funciones locales y realizarlas a distancia.

Las **Cámaras fijas perimetrales** se sitúan junto al vallado perimetral en la parte interior del Área Protegida, estas cámaras suelen tener un campo de visión de unos 80 a 100 m. de alcance. Suelen estar asociadas cada cámara a una «zona» cubierta por un detector perimetral.

Por estar a la intemperie estas cámaras, llevan una carcasa de protección. Todo el conjunto se instala sobre un soporte o torreta adecuada.

La ubicación de las cámaras se realiza de tal forma que cualquier cámara es vigilada u observada por otra cámara perimetral o por una motorizada.

Las **Cámaras motorizadas** se suelen situar también en exteriores en puntos adecuados que permitan entre otras las siguientes funciones:

- Respaldo de cámaras fijas perimetrales.
- Seguimiento por el Area Protegida de una intrusión.
- Vigilancia de áreas determinadas del Area Protegida o Areas Vitales.

Estas cámaras llevan unos accionamientos motorizados que les permiten moverse en sentido horizontal («pan») los 360° y en sentido vertical («Tilt») los 90°. Asimismo, para acoplar la imagen a vigilar disponen de zoom motorizado. Todos estos dispositivos tienen mando a distancia desde los Centros de Control.

El sistema de circuito cerrado de televisión envía las imágenes tomadas a los centros de control CAS y SAS del sistema de seguridad.

En consecuencia, los equipos que integran este subsistema, además de las cámaras, son:

- Monitores de recepción de imagen.
- Conmutadores / secuenciadores de imagen.
- Mandos equipos auxiliares de las cámaras.
- Grabadores de vídeo.
- Amplificadores/ecualizadores.
- Cables de video coaxiales.

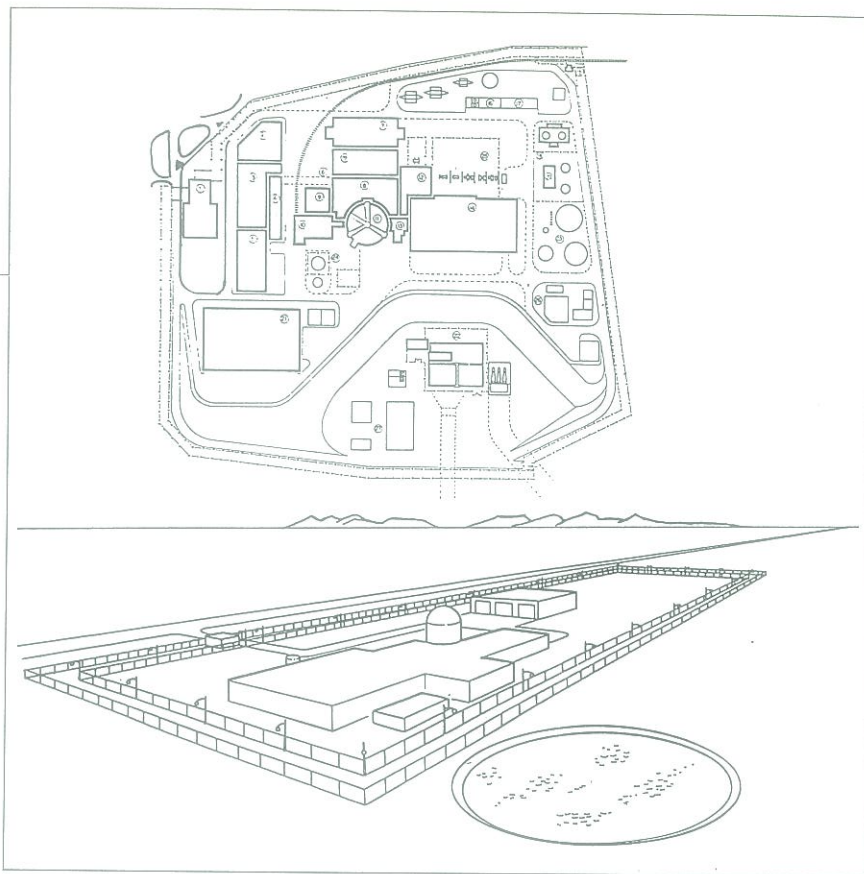
CONTROL DE ACCESOS

Entre sus funciones podemos enumerar las siguientes:

- Control e identificación de las personas y vehículos que acceden al Area Protegida.
- Establecer niveles de acceso a ciertas áreas.
- Control e identificación de las personas que acceden a zonas de seguridad.
- Tiempo de permanencia en cada área de las personas que accedieran.
- Alarmas en caso de acceso no autorizados a ciertas dependencias.

Después del análisis de Areas Vitales y Areas de Seguridad se definirá un equipamiento para las puertas que controlarán los accesos a las áreas mencionadas. Este equipamiento puede variar según la zona controlada y pueden considerarse los siguientes elementos:

- Lectora de entrada.
- Lectora de salida.
- Lectora de entrada con teclado.
- Botón pulsador de salida.
- Cerradura eléctrica.
- Contacto de balance magnético (BMS).
- Cerradura de seguridad con llave.
- Caja de control de puerta.



F II Control principal de accesos

Lectoras

Son el elemento fundamental del Control de Accesos que permite leer el código de la tarjeta magnética codificada que se introduce en ella. La información que «lee» la lectora es enviada vía Multiplexor al Ordenador del Sistema de Seguridad y según el Programa previsto se enviará o no una señal de apertura de la puerta.

Todos los elementos asociados a una puerta de control de acceso están cableados a una Caja de Control situada en el interior de la zona protegida y próxima a la puerta. Desde esta Caja de Control se envían las señales al Multiplexor asociado a la puerta correspondiente, el cual se comunica con el Ordenador a través del lazo de señal multiplexado del Subsistema de Gestión de Datos.

Controles de Acceso Principales

Existirá un Control Principal de Acceso para acceder al Area Protegida tanto para personas como para vehículos.

El Control de personas se realiza mediante la identificación de las mismas y proporcionando la tarjeta codificada adecuada o la escolta si fuera necesario.

A continuación se inspecciona al individuo y sus paquetes o bolsas de mano y finalmente se realiza su control de acceso mediante lectora y puerta o torniquete al efecto.

GESTION DE DATOS Y CONTROL CENTRAL

El sistema de seguridad dispone de unos Centros de Control denominados:

CAS

Central Alarm Station, Estación Central de Alarmas.

SAS

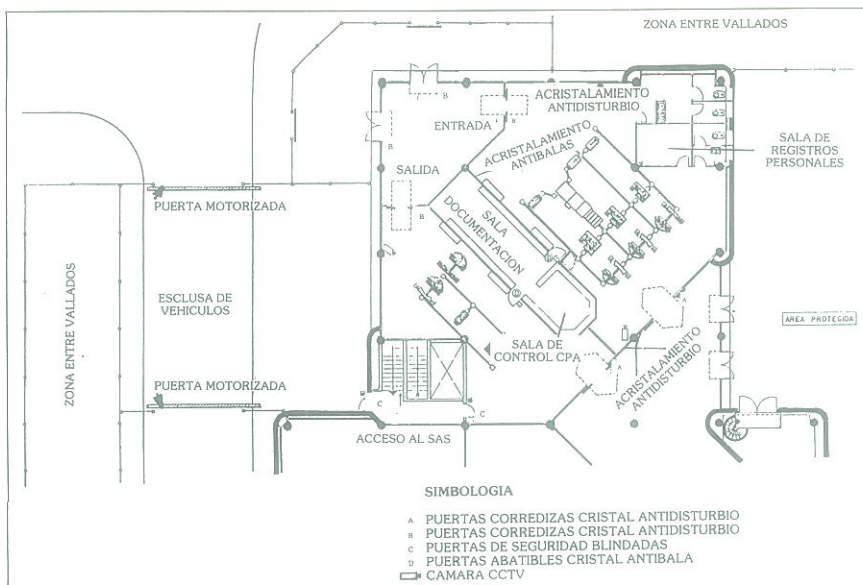
Secondary Alarm Station, Estación Secundaria de Alarmas.

ACB o CPA

Control Principal de Accesos.

El Control Central se realiza desde los Centros CAS y SAS, en los cuales están situados los Paneles de Monitores y las Consolas de Control. Son dos centros similares y redundantes.

La recogida y procesado de toda la información de Seguridad relacionada con la vigilancia, supervisión de líneas, detección, fallos, condiciones de alarmas de tamper, será recogida por un Sistema de Proceso de Datos que consta de dos minicomputadores redundantes trabajando en dual. La configuración recomendada, permite que cada uno de los minicomputadores pueda actuar como órgano principal del Sistema, compartiendo ambos dos unidades de disco. Los dos minicomputadores estarán interconectados por un sistema de transferencia continua (bus de conexión).



F III Diagrama de secuencia del adversario (ASD)

Los minicomputadores estarán conectados con los Periféricos Remotos del Sistema de Seguridad Industrial a través de Unidades Remotas Multiplexoras.

Dichos Multiplexores estarán conectados con las diferentes Zonas de Seguridad de los Subsistemas, recogiendo y transmitiendo los datos al minicomputador en línea para su procesamiento.

La conexión entre los minicomputadores y los Multiplexores será del tipo de anillo, al objeto de crear rutas bidireccionales en prevención de fallos en la línea.

Las Unidades Multiplexoras Remotas están conectadas al Sistema de Tensión Segura o llevan baterías autónomas locales.

Eventualmente los Multiplexores pueden recibir y tratar las señales provenientes del Sistema Contraincendios de la Central para ser procesadas y señalizadas junto con las señales del Sistema de Seguridad.

Asimismo, en algunas centrales se llevan señales o datos del Sistema de Protección Radiológica al Sistema de Seguridad, pues llevando un control de dosis de radiación de los empleados se pueden autorizar o no ciertos accesos a áreas con radiactividad.

ALIMENTACION ELECTRICA

Este subsistema suministra la potencia necesaria con la disponibilidad requerida por la norma para los diferentes subsistemas y equipos del Plan de Seguridad.

Alimentación Normal

Básicamente se dispondrá de una Fuente de Alimentación Normal, en trifásica con neutro 380/220 V 50Hz para una potencia demandada aproximada de 500 Kva.

Alimentación de Emergencia

Se dispone normalmente de una Fuente de Alimentación de Emergencia

compuesta por un Generador Diesel y una Fuente de Tensión Ininterrumpida (UPS).

La Fuente de Tensión Segura (UPS) garantiza la operación de ciertos equipos o subsistemas del SSI sin discontinuidad de funciones, sin pasar por cero de tensión.

El consumo de estas cargas de la UPS puede ser del orden de 30 Kva.

La Alimentación de Emergencia por Generador Diesel entrará a servir las cargas del Sistema de Seguridad por conmutación automática y la vuelta a la Fuente Normal se realizará asimismo de forma automática.

El Generador Diesel debe ser capaz de alimentar a todas las cargas del Plan de Seguridad (SSI) durante un mínimo de veinticuatro horas.

Puesto que todo el Sistema de Seguridad no de clase 1E hay que utilizar un Generador Diesel no clase 1E para realizar la función de la Fuente de Emergencia. Este Generador Diesel puede ser exclusivo para el SSI o compartido con otras cargas no clase 1E de la Planta.

ILUMINACION

Este subsistema tiene como funciones las siguientes:

- Proveer de una iluminación permanente al Vallado Perimetral y al Area Protegida.
- Dar la iluminación mínima requerida para el buen funcionamiento del Subsistema CCTV y para la realización de las funciones de vigilancia e inspección.

Consta el alumbrado del Sistema de Seguridad de las siguientes unidades:

- Alumbrado Perimetral que ilumina la zona de vallado y «zonas de aislamiento».
- Alumbrado de Areas Vitales Exteriores.
- Alumbrado del CAS, SAS, ACB o CPA.

- Se pide un nivel de iluminación mínimo de 5 lux en el Vallado Perimetral.
- Para las Areas Vitales exteriores el nivel es de unos 20 lux de Iluminación Mínima o 50 lux de Iluminación Media.
- Para el Area Protegida se exige un nivel mínimo de 5 lux.
- El tipo de luz normalmente utilizado es a base de lámparas de sodio de alta presión.

COMUNICACIONES

Los sistemas en los que se apoya el SSI en condiciones normales y ante situaciones de emergencia son los siguientes:

- Telefonía Interior y CTNE o Red Nacional.
- Megafonía de la Planta.
- Intercomunicadores Privados.
- Radioteléfonos.

INSPECCION

El edificio de Control Principal de Accesos (ACB o CPA) al Area Protegida, que incluye la esclusa de acceso de vehículos aneja al mismo, canalizará el tráfico de personal de plantilla, visitantes, materiales y vehículos autorizados que pretendan el acceso a la Zona Protegida, realizándose el control e inspección de los mismos según los correspondientes Procedimientos Funcionales, por parte de la Organización de Seguridad.

En dicho edificio se habilitarán varios pasillos o rutas separadas para el tráfico de personas de entrada y otros pasillos independientes para el tráfico de personal de salida (ver figura 3).

Cada uno de los pasillos de entrada estará equipado con un torniquete o puerta controlado por un lector de tarjeta, un Detector de Metales de tipo Arco y un Detector de Explosivos fijo del (tipo «walk through»).

Asimismo, se instalará un equipo para inspección de equipajes de mano y paquetes, por «Rayos X» provisto de cinta transportadora, entre dos de los pasillos de entrada.

En el caso de fallo de los Detectores Fijos, se utilizarán equipos portátiles de detección de metales y explosivos. Los vehículos serán inspeccionados de acuerdo con la NUREG 220.

El control de documentación e inspección, será realizado por guardas de la Organización de Seguridad, escoltándose al vehículo hasta la zona de descarga del interior del Area Protegida y desde aquella hasta la salida.

CABLES Y CONDUCCIONES

Desde los Centros de Control CAS, SAS y ACB o CPA salen unos bancos de conductos que van a parar al Banco de Conductos Perimetral que recorre todo el perímetro por la zona entre vallados preferentemente.

El Banco de Conductos Perimetral es muy útil para la distribución de cables a los equipos asociados al vallado y para los equipos en áreas exteriores.

Este Banco Perimetral puede estar formado por conductos metálicos o de PVC según los condicionantes de señal de los cables, interferencias electromagnéticas e interferencias con instalaciones exteriores.

La sección del Banco Perimetral puede ser variable en función de las zonas y las necesidades de carga.

En el interior de Edificios, las Conducciones del Sistema de Seguridad podrán ser bandejas o conductos de clase no 1E.

Los conductos dentro de Edificios serán metálicos y preferentemente se instalarán en las partes seguras en el caso de los controles de acceso.

Según el tipo de cables se recorrerán por conducciones diferentes (Potencia, Control, Instrumentación).

Cables

Existirán diferentes tipos de cables para dar servicio a los distintos equipos y subsistemas del SSI. Básicamente podemos señalar los siguientes:

- Cables de potencia.
- Cables de control.
- Cables de instrumentación.
- Cables coaxiales.
- Cables de comunicaciones

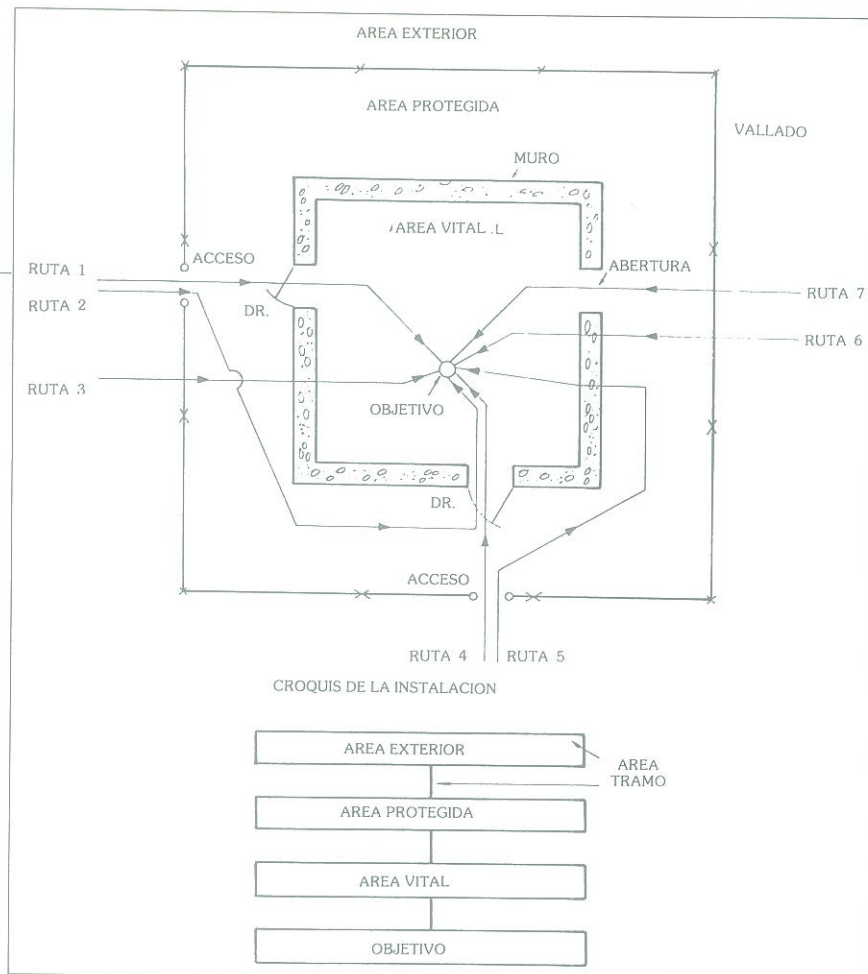
MISCELANEOS

Existen otros equipos o funciones dentro del Sistema de Seguridad, que sin tener entidad de subsistema conviene mencionarlos para tenerlos en cuenta en el diseño y en la operatividad del sistema. Algunos de ellos pueden ser optativos del sistema:

- Pulsadores de emergencia.
- Acristalamientos antibala o antidisturbios.
- Control de llaves mecánicas.
- Controles patrulla en rondas de vigilancia.

INTERFASES

Sin ser propiamente un subsistema de Plan de Seguridad, es conveniente el or-



FIV Esquema de la planta simplificada

denar y estructurar los diferentes criterios y requisitos que la Ingeniería de Seguridad exige o recomienda a otras áreas o disciplinas del proyecto debido a las interfases con ellas.

En este sentido, enunciaremos aquellos aspectos que «Security» tiene interrelacionadas con otros sistemas o equipos del Proyecto General de la Planta:

ARQUITECTURA/OBRA CIVIL

- * Vallados, cerramientos, acristalamientos.
- * Bancos conductos, fundaciones equipos.
- * Disposición CAS, SAS, ACB o CPA.
- * Puertas, cerraduras.
- * Huecos, conductos gran diámetro.
- * Rutas evacuación, dispositivos antipánico.

Ingeniería Mecánica/Nuclear

- * Generadores Diesel.
- * Sistema contraincendios.
- * Aire acondicionado CAS-SAS.
- * Niveles de radiación, Sistemas vitales, Protección Radiológica.

Ingeniería Eléctrica/Control

- * Alimentación normal y emergencia.
- * Fuente Tensión Segura (UPS).
- * Cuadros, paneles, armarios, consolas del Sistema de Seguridad.
- * Iluminación.

- * Cables, conducciones, ruteados, conexiones P. a T.
- * Telefonía, Megafonía

PROCEDIMIENTOS Y ORGANIZACION DE SEGURIDAD

Para que los medios físicos, técnicos y humanos integrados en el Plan de Seguridad sean realmente eficientes, es necesario el desarrollo de unos Procedimientos y/o Reglamentación específica que determine la forma de utilizar los medios materiales y las funciones y responsabilidades concretas del personal asignado a la Organización de Seguridad.

Toda la Reglamentación específica de Seguridad suele integrarse en un «Manual de Procedimientos Administrativos del Sistema» y en el cual se recogen todos los aspectos que a continuación se relacionan, como orientación:

Organización de Seguridad

- Funciones y Responsabilidad del Personal.
- Turnos del Personal de Seguridad.
- Rondas de Vigilancia.
- Interfases del Personal de Seguridad con el Personal de Explotación y Mantenimiento.
- Formación del Personal de Seguridad.

Administración del Sistema de Seguridad

- Accesos de personas al Area Protegida.
- Accesos de vehículos al Area Protegida.
- Vehículos en tránsito interno de la Planta.
- Acceso a las Areas Vitales.
- Fijación de niveles de acceso.
- Identificación del Personal.
- Control de llaves mecánicas.
- Escoltas.

Administración del Sistema de Seguridad en operaciones de recarga y/o mantenimiento pesado.

Administración del Sistema de Seguridad en fase de Pruebas Preoperacionales.

Documentación del Sistema de Seguridad.

Pruebas periódicas del Sistema de Seguridad.

El Plan de Contingencias que forma parte del Plan de Emergencia de la Central es un procedimiento más, que es necesario elaborar para fijar las acciones y responsabilidades, ante las situaciones especiales que en él se cuestionan.

De forma orientativa el «Plan de Contingencias» tiene como alcance típico:

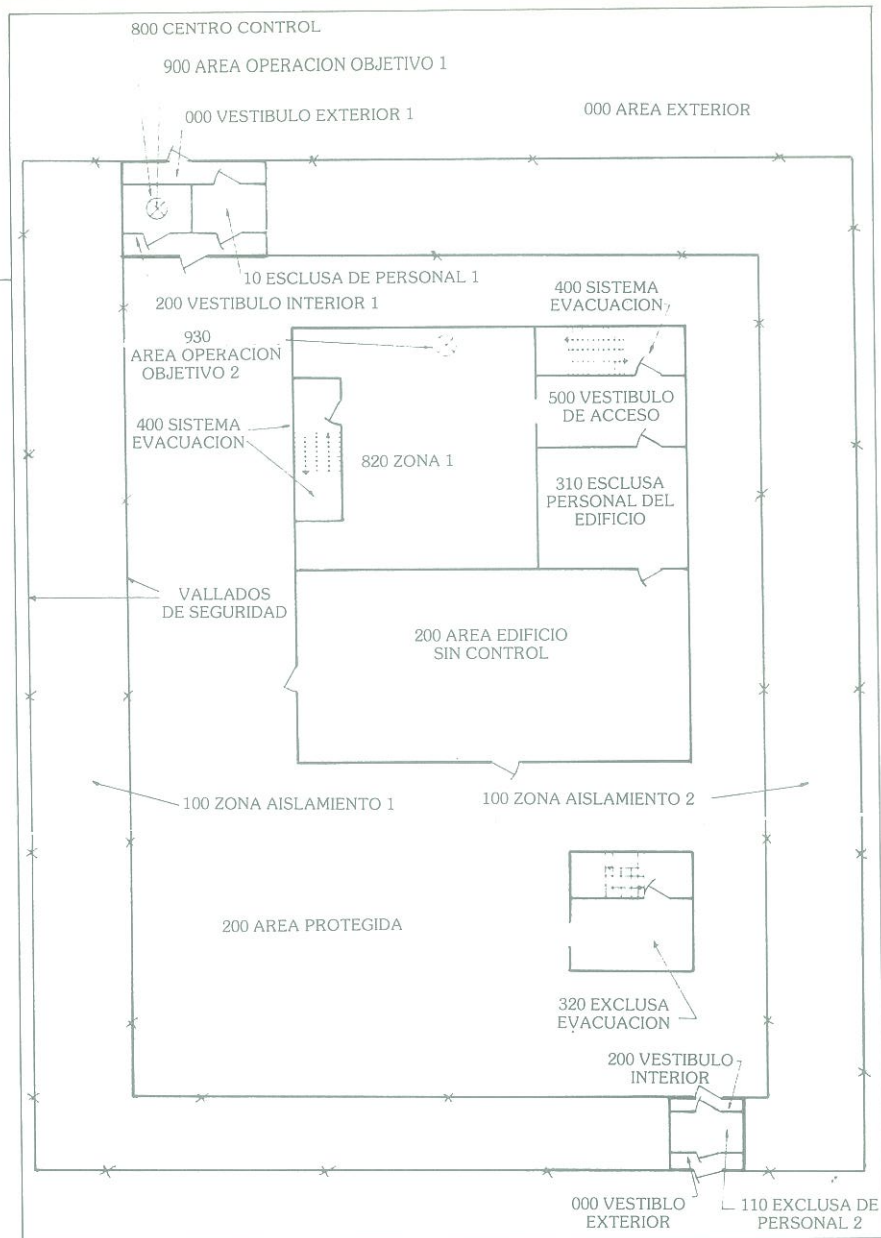
- Definiciones.
- Fuerzas de respuesta exteriores.
- Definición de contingencias (amenaza de bomba; amenaza de ataque; disturbios exteriores a la Central; intrusión al Area Protegida; intrusión en un Area Vital; Pérdidas del Sistema de Comunicaciones, etc.).
- Matriz de responsabilidades y actuaciones.

La Organización de Seguridad suele estar compuesta por personal de la Propiedad y por guardas o vigilantes jurados de empresas privadas.

La responsabilidad de esta organización es administrar el Sistema de Seguridad, haciendo cumplir los procedimientos del Sistema y efectuando las funciones principales cuales son:

- Efecto disuasorio.
- Vigilancia e inspección.
- Rondas de patrullaje.
- Respuesta y neutralización ante amenazas.

La Ingeniería de Seguridad tiene que definir con mucho rigor el número de



FV Esquema de la Planta simplificada

puestos de guardas en la Planta, puesto que por la necesidad de contratar de 4 a 5 guardas por puesto (turnos, corretornos, vacaciones, etc.) este apartado incide muy negativamente en los costes de explotación del Sistema.

La Organización de Seguridad estará coordinada con fuerzas exteriores de respaldo; las cuales actuarían en determinados tipos de amenazas que así lo requieran. Estas fuerzas exteriores pueden ser: Guardia Civil, Policía Nacional o Policía Autonómica, Fuerzas Armadas.

TECNICAS DE EVALUACION DEL SISTEMA DE SEGURIDAD

Una vez que el diseño del Sistema de Seguridad ha sido realizado, es necesario comprobar su efectividad y revisarlo en cuanto que cumple los objetivos propuestos.

La evaluación del sistema persigue lo siguiente:

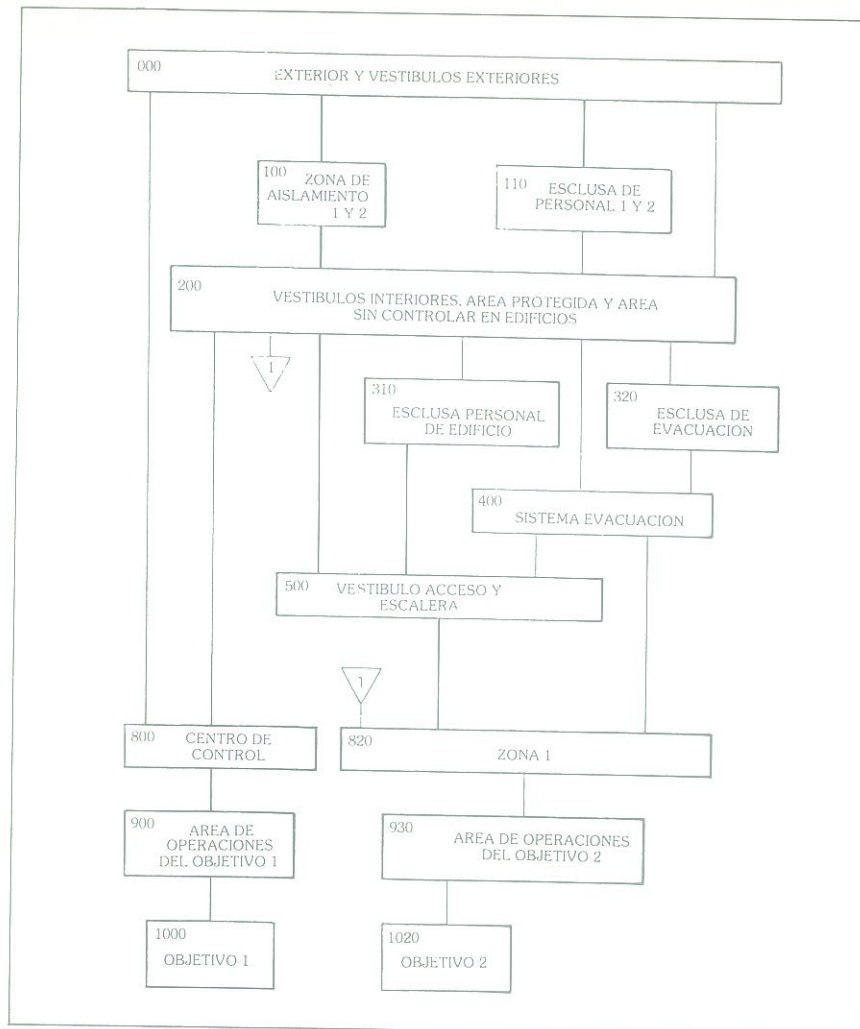
- * Cumplimiento de los requisitos de componentes y subsistemas.
- * No existen puntos débiles.
- * Protección de Seguridad equilibrada o vulnerabilidad uniforme en todo el sistema.
- * Análisis coste/eficacia de los elementos del sistema.

Esta evaluación puede conducir a la necesidad de rediseñar el sistema y optimizarlo.

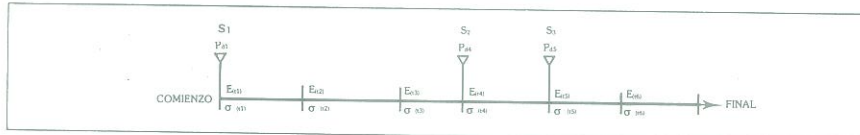
Para realizar la evaluación se recurre a técnicas de modelización del sistema que simulan el comportamiento del mismo en el mundo real.

Las técnicas de modelización parten de las siguientes premisas:

- Caracterización de la instalación.
- Identificación de objetivos.
- Definición de amenazas.

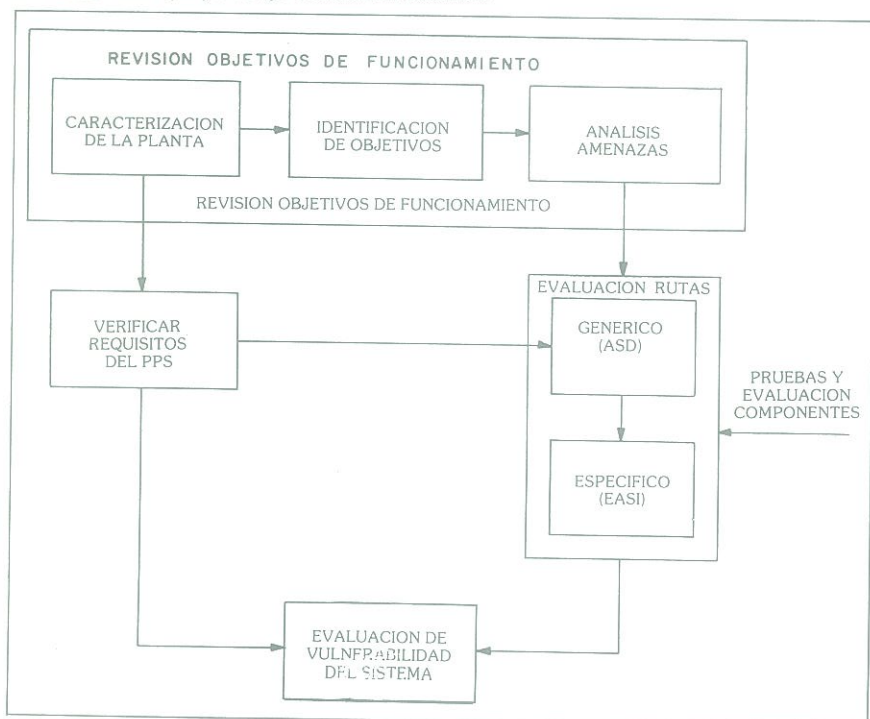


F VI Diagrama de adyacencias significativas



F VII Proceso de análisis/diseño

F VIII Ruta específica tiempo-secuencia del adversario



A continuación se acomete el análisis de rutas que el adversario con unos medios determinados puede realizar para llegar a sus objetivos.

El análisis de rutas puede tener dos niveles, el nivel genérico y el nivel específico.

Una técnica de evaluación de modelo genérico es el modelo ASD (Adversary Sequence Diagram).

Una técnica de evaluación de modelo específico es el modelo EASI (Estimate of Adversary Sequence Interruption).

– Con el modelo **ASD** se analizan todos los posibles caminos o rutas que puede seguir un adversario y se consigue:

- Verificar la existencia de medidas positivas del Sistema de Protección Física.
- Seleccionar las rutas críticas para ser evaluadas posteriormente por otro modelo específico.

El modelo **ASD** está basado en una representación gráfica de la Planta que muestra todas las adyacencias entre áreas y se resuelve con los datos de probabilidades de detección de los diferentes sensores y tiempos de retardo de las barreras asociadas a cada ruta entre diferentes áreas.

Este modelo permite identificar los segmentos de rutas de menor efectividad de detección y menor resistencia de las barreras (ver figuras 4, 5 y 6).

– El modelo **EASI** proporciona un método fácil y útil para evaluar el funcionamiento del sistema de Seguridad para rutas determinadas.

El método efectúa un análisis probabilístico de las interacciones de las funciones del Sistema con el tiempo de respuesta de los guardas.

Por la facilidad del método pueden utilizarse máquinas programadoras portátiles para obtener resultados.

Los datos necesarios para utilizar este método son:

- * Probabilidades de detección y comunicación de los sensores –Pd–.
- * Tiempos medios y desviaciones típicas de los retardos y respuestas –E(t) o (t).

El resultado de este método es la probabilidad de interrupción de la amenaza postulada (robo o sabotaje) en una ruta específica, por la fuerza de la respuesta.

Este método es susceptible de realizar análisis de sensibilidad de forma que modificando probabilidades de detección (Pd) o tiempos de retardo E(t) o (t), se optimice la vulnerabilidad de la ruta analizada (ver figura 7).

– Como regla general las técnicas de evaluación comienzan con métodos de nivel genérico y se procede posteriormente al análisis por métodos de nivel específico.

En la figura 8 se muestra el proceso de optimización análisis/diseño de un Plan de Seguridad Física para una Planta Nuclear.