TNO-rapport
FEL-98-A248

JWID'98: een impressie

TNO Fysisch en Elektronisch Laboratorium

Oude Waalsdorperweg 63
Postbus 96864
2509 JG 's-Gravenhage

Telefoon 070 374 00 00
Fax 070 328 09 61

Datum
december 1998

Auteur(s)
Ir. P.H. Zwaard

Opdrachtgever	Min. van Defensie/Defensiestaf
Projectbegeleider	Lkol F.W.J. van Weverwijk
Onderdeel	CIS
Rubricering	
Vastgesteld door	Lkol F.W.J. van Weverwijk
Vastgesteld d.d.	30 november 1998
Titel	Ongerubriceerd
Managementuittreksel	Ongerubriceerd
Samenvatting	Ongerubriceerd
Rapporttekst	Ongerubriceerd
Bijlage	Ongerubriceerd
Exemplaarnr.	23
Oplage	54
Aantal pagina's	100 (incl. bijlage, excl. RDP & distributielijst)
Aantal bijlagen	1

Alle rechten voorbehouden. Niets uit dit rapport mag worden vermenigvuldigd en/of openbaar gemaakt door middel van druk, fotokopie, microfilm of op welke andere wijze dan ook, zonder voorafgaande schriftelijke toestemming van TNO.

Indien dit rapport in opdracht van het ministerie van Defensie werd uitgebracht, wordt voor de rechten en verplichtingen van de opdrachtgever en opdrachtnemer verwezen naar de 'Modelvoorwaarden voor Onderzoeks- en Ontwikkelings-opdrachten' (MVDT 1997) tussen de minister van Defensie en TNO indien deze op de opdracht van toepassing zijn verklaard dan wel de betreffende terzake tussen partijen gesloten overeenkomst.

© 1998 TNO

19990420 031

DISTRIBUTION STATEMENT A
Approved for Public Release
Distribution Unlimited

DTIC QUALITY INSPECTED 4

AQF 99-07- 1321

TNO Fysisch en Elektronisch Laboratorium is onderdeel van TNO Defensieonderzoek waartoe verder behoren:

TNO Prins Maurits Laboratorium
TNO Technische Menskunde

Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek TNO

Managementuittreksel

Titel	:	JWID'98: een impressie
Auteur(s)	:	Ir. P.H. Zwaard
Datum	:	december 1998
Opdrachtnr.	:	A98D755
IWP-nr.	:	761
Rapportnr.	:	FEL-98-A248

Doelstelling
Het doel van het project 'Deelname JWID '98' is om de krijgsmacht inzicht te verschaffen in de ontwikkelingen op het gebied van C2 systemen zoals die op JWID (Joint Warrior Interoperability Demonstration) zijn gedemonstreerd.

Omschrijving van de werkzaamheden
De werkzaamheden bestaat uit het vergaren van informatie over de C2 systemen die zijn gedemonstreerd op JWID '98. Hiervoor is een bezoek gebracht aan SHAPE in Mons (België) waar de NATO locatie van JWID '98 is gevestigd.
Een impressie van de gedemonstreerde C2 systemen is weergegeven in dit verslag.

Conclusies en aanbevelingen
JWID '98 heeft 'aangetoond' dat het mogelijk is met functionaliteit van het World Wide Web en Internet technologie commercieel beschikbare systemen te combineren met militaire systemen tot een C4I netwerk ('a system of systems') waarin NATO partners C2 informatie kunnen delen. Deze technologieën maken het mogelijk met een standaard commerciële PC toegang te krijgen tot het digitale gevechtsveld. JWID '98 heeft verder aangetoond dat de uitwisseling van informatie vaak nog moeizaam is door verschillen in berichtenstandaarden en datamodellen. In de praktijk zal nog aangetoond moeten worden of militaire netwerken voldoende bandbreedte beschikbaar hebben voor de ondersteuning van een dergelijk C4I netwerk. Vraagtekens blijven bestaan bij de robuustheid en beveiliging van de getoonde produkten.

Voor Nederland is het van belang aan toekomstige JWID demonstraties deel te nemen met eigen C2 systemen. Door deelname wordt waardevolle praktijkervaring opgedaan over de interoperabiliteit van deze C2 systemen met die van andere NATO partners. Deze ervaring kan worden gebruikt in de ontwikkel- en aanschafprocessen van deze systemen en kan bijdragen aan de functionaliteit en de interoperabiliteit van huidige en toekomstige C2 systemen welke voldoen aan de wensen van de krijgsmacht.

Samenvatting

Het doel van JWID '98 is om technologische oplossingen te demonstreren welke bijdragen aan de interoperabiliteit van C2 systemen van multinationale eenheden. JWID '98 is een demonstratie waarin bestaande militaire systemen, commercieel verkrijgbare systemen en nieuwe systemen samengevoegd zijn tot een samenwerkend C4I netwerk ('a system of systems').

JWID '98 heeft 'aangetoond' dat het mogelijk is met Web functionaliteit en Internet technologie commercieel beschikbare systemen te combineren met militaire systemen tot een C4I netwerk waardoor het mogelijk wordt met een standaard commerciële PC toegang te krijgen tot het digitale gevechtsveld van verschillende NATO partners.
De uitwisseling van informatie tussen de C2 systemen is echter vaak nog moeizaam door verschillen in berichtenstandaarden en datamodellen. In de praktijk zal tevens nog aangetoond moeten worden of militaire netwerken voldoende bandbreedte beschikbaar hebben voor het extra dataverkeer. Vraagtekens blijven bestaan bij de robuustheid en beveiliging van de getoonde produkten.

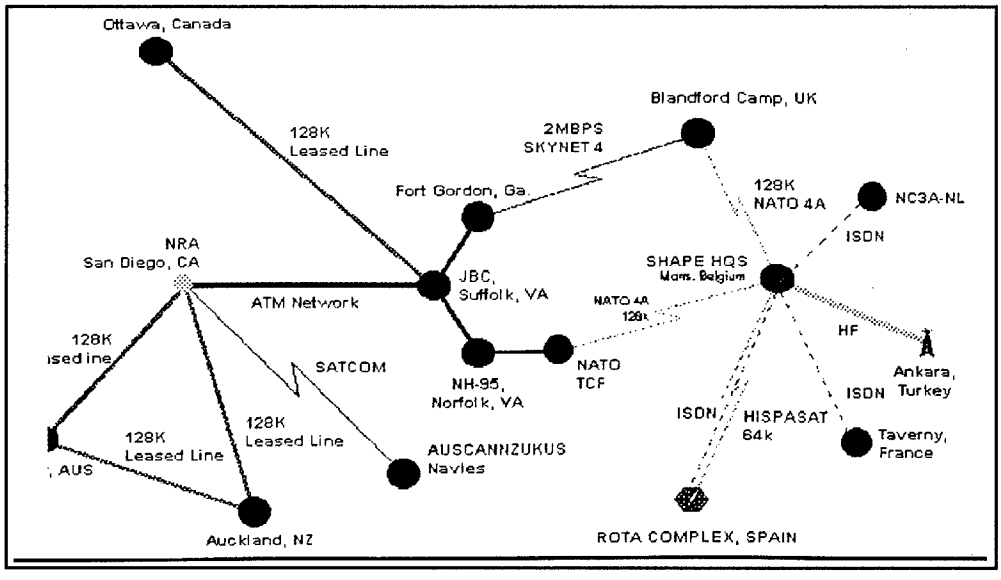
Voor Nederland is het van belang aan toekomstige JWID demonstraties deel te nemen. Door deelname wordt waardevolle praktijkervaring opgedaan die kan worden gebruikt in de ontwikkel- en aanschafprocessen van deze systemen en kan bijdragen aan de functionaliteit en de interoperabiliteit van C2 systemen welke voldoen aan de wensen van de krijgsmacht.

Inhoud

1. Inleiding

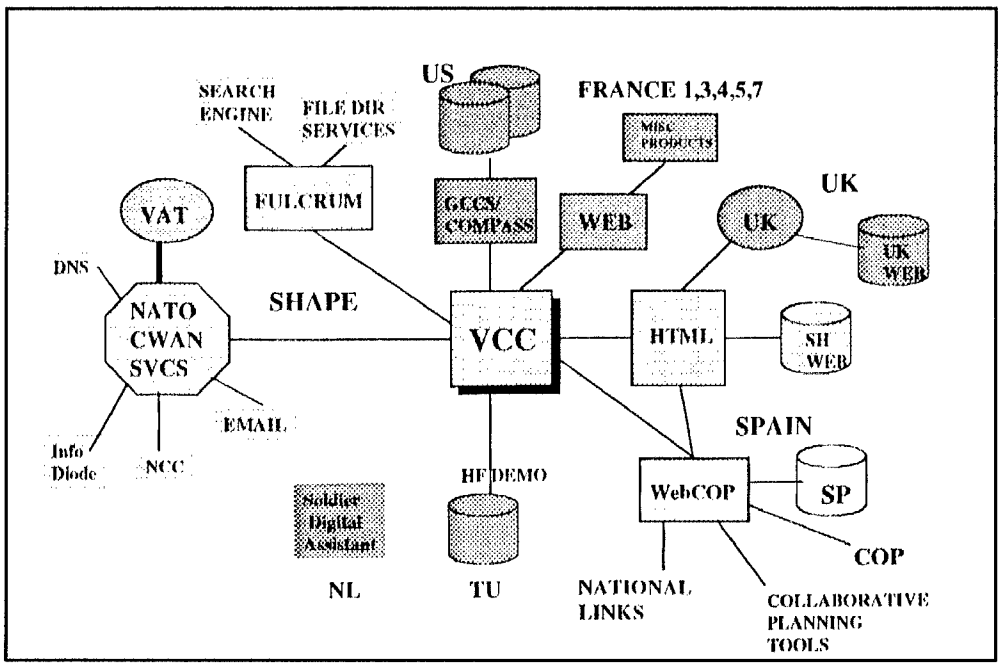
JWID '98 is een vervolg op eerdere initiatieven van de Verenigde Staten om de bruikbaarheid van verschillende technologieën voor de interoperabiliteit van de commandovoering te demonstreren. Het is in 1989 begonnen met de 'Integrated Tactical-Strategical Data Networking' demonstratie en is sindsdien een regelmatig terugkerend fenomeen.

Het doel van JWID '98 is om technologische oplossingen te demonstreren welke bijdragen aan de interoperabiliteit van C2 systemen van multinationale eenheden. JWID '98 is een gezamenlijke demonstratie waarin bestaande militaire systemen, commercieel verkrijgbare systemen en nieuwe systemen samengevoegd zijn tot een samenwerkend C4I netwerk ('a system of systems'). Een belangrijk onderdeel van JWID '98 vormt de beproeving van dit C4I netwerk door middel van de uitvoering van een gesimuleerde militaire operatie van multinationale eenheden.



Figuur 1.1: JWID Coalition Wide Area Network

JWID '98 maakt gebruik van een 'Coalition Wide Area Network' (CWAN) zoals getoond in Figuur 1.1. Het CWAN is een TCP/IP netwerk over beveiligde verbindingen. Dit CWAN wordt gebruikt als backbone netwerk voor de koppeling van de diverse C2 systemen (Figuur 1.2).
Deelnemende landen en instanties aan JWID '98 te SHAPE zijn Frankrijk, Spanje, Turkije, Nederland, NACOSA, SHAPE, NC3A. Verder nemen ook Canada, het Verenigd Koninkrijk en de Verenigde Staten deel aan JWID '98 vanuit nationale opstellingen.



Figuur 1.2: C2 systemen in JWID '98

In het volgende hoofdstuk worden de verschillende demonstraties, zoals die te zien waren bij SHAPE in Mons, kort toegelicht.

2. Demonstraties

De demonstraties die zijn getoond bij SHAPE te Mons (België) zijn onder te verdelen in Message Handling Systemen, Command & Control Systemen en Ondersteunende Gereedschappen.

2.1 Message Handling Systemen

2.1.1 MESREG

Uitvoerder:
Sagem, Frankrijk

Toepassing:
Frankrijk demonstreerde een Military Message Handling systeem genaamd MESREG. MESREG maakt het mogelijk berichten te versturen vanuit mobiele posten naar Command Centres. Mogelijke berichten zijn SITREPs en andere berichten over de voortgang van een missie. De eigen positie kan met een GPS ontvanger automatisch worden bepaald en in het SITREP bericht worden opgenomen. De berichten kunnen veelal automatisch in C2 computer systemen worden ingevoerd.
MESREG is door het Franse leger toegepast in Joegoslavië.

Technische beschrijving:
MESREG maakt de uitwisseling van berichten mogelijk in verschillende formaten waaronder ADatP-3, SMTP (Internet email) en X.400. MESREG kan verschillende communicatiemiddelen gebruiken voor de uitwisseling van deze berichten. Tijdens JWID is MESREG gebruikt in combinatie met een Ethernet TCP/IP netwerk, FM9000 combat net radio en GSM mobiele telefoon. Andere mogelijkheden zijn satellietverbindingen en telefoonverbindingen. De berichten kunnen worden vercijferd voordat ze over het communicatiemedium worden verzonden. Verder is het mogelijk digitale handtekeningen aan het bericht te verbinden om een authenticatie van de afzender uit te voeren.
MESREG is een applicatie die draait op een DOS of WINDOWS NT computer. De getoonde demonstratie maakte gebruik van COTS laptop computers welke in een metalen attachékoffer is gemonteerd.

Referenties:
- bijgevoegde brochure (zie appendix A);
- http://www.sagem.com.

2.1.2 OTEMAS

Uitvoerder:
Turkije

Toepassing:
OTEMAS is vergelijkbaar met de MESREG demonstratie van Frankrijk. OTEMAS maakt het mogelijk elektronische berichten uit te wisselen tussen (mobiele) posten. Naast berichtenuitwisseling biedt het OTEMAS systeem ook mogelijkheden voor spraakcommunicatie, echter alleen voor HF, VHF en UHF communicatiemiddelen.

Technische Beschrijving:
OTEMAS wisselt berichten uit op basis van de X.400 standaard voor berichtenverkeer en het Internet SMTP protocol. OTEMAS kan verschillende communicatiemiddelen gebruiken voor de uitwisseling van deze berichten. Tijdens JWID is OTEMAS gebruikt om berichten uit te wisselen tussen SHAPE en Turkije via een HF netwerk. Andere mogelijkheden zijn VHF, UHF, GSM, satellietverbindingen, WAN/LAN verbindingen en telefoonverbindingen. De berichten worden vercijferd voordat ze over het communicatiemedium worden verzonden. Verder is het mogelijk digitale handtekeningen aan het bericht te verbinden om de authenticiteit van de afzender te bewijzen.
OTEMAS is een applicatie die draait op een PC. Voor toepassing van OTEMAS over HF, VHF en UHF communicatiemiddelen is een aparte Radio Control Unit (RCU) benodigd. Deze RCU verzorgt de controle van diverse radiosystemen. De RCU biedt ook de secure digital voice mogelijkheden van OTEMAS.

Referenties:
- bijgevoegde brochure (zie appendix A).

2.2 Command & Control systemen

2.2.1 ACOM & SIR

Uitvoerder:
Franse defensie en Matra Frankrijk

Toepassing:
Deze Franse demonstratie omvat twee systemen. ACOM is het C2 informatiesysteem dat in gebruik is bij de Franse marine. Momenteel zijn meer dan 50 Franse marine schepen uitgerust met ACOM. ACOM maakt het mogelijk waargenomen objecten uit te wisselen zodat op alle schepen hetzelfde beeld van het gevechtsveld aanwezig is.
SIR is het C2 informatiesysteem voor de Franse landmacht. Het is vergelijkbaar met het toekomstige Nederlandse BMS (Battlefield Management Systeem). Ook in het SIR systeem worden waarnemingen automatisch uitgewisseld om te komen tot een gezamenlijk beeld van het gevechtsveld.
Voor JWID is een koppeling gemaakt tussen SIR en ACOM zodat ACOM het totale overzicht van het gevechtsveld (landstrijdkrachten en marine) kon leveren. Verder is een koppeling gemaakt tussen ACOM en de volgende systemen: GCCS van Amerika, JMCIS van de Multi-National Task Group, WEBCOP van Spanje en het Virtual Command Centre (VCC) van SHAPE. SIR is gekoppeld met het WEBCOP systeem van Spanje en een systeem in Engeland.

Technische Beschrijving:
Voor beide systemen geldt dat updates op de informatie automatisch worden verzonden naar de andere aanwezige platformen. SIR verzendt zijn updates in het ADatP-3 berichtenformaat. ACOM verzendt updates in het OTH-GOLD berichtenformaat. Voor ACOM geldt dat het web-enabled is. Dit wil zeggen dat het ACOM systeem het beeld van het gevechtsveld kan presenteren in de vorm van HTML-pagina's. Deze HTML pagina's kunnen met COTS PC's en webbrowsers (Netscape, Internet Explorer) worden bekeken.
Voor JWID is gebruik gemaakt van IP verbindingen. Onder operationele omstandigheden kunnen SIR en ACOM werken over Link 11, tactische VHF radio netwerken, tactische wide area netwerken, HF radio netwerken en satellietverbindingen.

Referenties:
- JWID handout (zie appendix A).

2.2.2 SIPAC-NT

Uitvoerder:
Franse defensie en Alcatel ISR Frankrijk

Toepassing:
SIPAC-NT is een C2 systeem voor gebruik in commandoposten. SIPAC-NT biedt een aantal functionaliteiten zoals een digitaal beeld van het gevechtsveld met status informatie van de eenheden (zoals positie, snelheid en richting van verplaatsen), beheer van documenten, workflow management (bijv. routering van documenten langs de juiste functionele organen) en informatieuitwisseling met andere commandoposten en eenheden te velden op basis van X.400 Military Message Handling. Het systeem bestaat uit een aantal client workstations waaraan de gebruikers werken. De informatie is beschikbaar op een aantal servers.

Technische Beschrijving:
SIPAC-NT is ontwikkeld voor een Windows NT omgeving. Op de Windows-NT client workstations is MS-Office beschikbaar voor het aanmaken van documenten (Word, Excel, Powerpoint, etc.). Voor de uitwisseling en beheer van documenten binnen een commandopost wordt gebruik gemaakt van Lotus Notes. Verder is een Windows-NT server beschikbaar met een Oracle database. Deze database bevat het digitale beeld van het gevechtsveld. Deze database wordt gevoed met informatie van eenheden te velde welke binnenkomt als X.400 versie 1988 MHS berichten. Uitwisseling van informatie met andere commandoposten vindt eveneens plaats met X.400-88 MHS berichten.

Referenties (zie appendix A):
- bijgevoegde brochure SIPAC-NT;
- JWID handout.

2.2.3 JACIS

Uitvoerder:
Thomson-CSF Frankrijk

Toepassing:
JACIS is een C2 systeem dat een digitaal beeld van het gevechtsveld kan tonen en status informatie van de aanwezige eenheden. Toepassing zal voornamelijk in commandoposten zijn, hoewel de architectuur toepassing in voertuigen ook mogelijk maakt.

Technische Beschrijving:
JACIS is voor een groot deel gebaseerd op Web technologie. Het systeem bestaat uit een JACIS webserver. Deze Web server is gekoppeld met een database welke is opgezet volgens het ATCCIS datamodel. Thin client computers kunnen met standaard webbrowsers (Netscape, Internet Explorer) contact maken met de JACIS webserver. De JACIS webserver stuurt vervolgens een JAVA applicatie naar de browser. Deze JAVA applicatie verzorgt vervolgens de interactieve presentatie van het digitale gevechtsveld. De JAVA applicatie maakt het mogelijk om veranderingen in de gegevens direct op het scherm van de client zichtbaar te maken (push technologie). Voordeel is dat de client volledig kan bestaan uit COTS apparatuur.
De ATCCIS databases kunnen onderling worden gekoppeld volgens de ATCCIS architectuur. Hierdoor is het eenvoudig een gezamenlijk digitaal beeld van het gevechtsveld op te bouwen met andere eenheden uit eigen troepen of multinationaal.
Voor de communicatie is een IP-gebaseerd netwerk nodig. In de praktijk moet de bruikbaarheid nog worden aangetoond met name met betrekking tot de beschikbaarheid van voldoende bandbreedte in militaire netwerken.

Referenties:
- JWID handout (zie appendix A).

2.2.4 WEBCOP

Uitvoerder:
Spaanse Marine en ISDEFE Spanje

Toepassing:
WEBCOP is, net als het Franse JACIS, een C2 systeem dat een digitaal beeld van het gevechtsveld kan tonen en status informatie van de aanwezige eenheden. Toepassing zal voornamelijk in commandoposten zijn, welke zich zowel aan land of op een schip kunnen bevinden.

Technische Beschrijving:
WEBCOP maakt verregaand gebruik van Internet technologie. De architectuur bestaat uit database servers die onderling de gegevens up to date en consistent houden door middel van replicatie mechanismen. Informatie, zoals het digitale beeld van het gevechtsveld, GIS informatie en status informatie van eenheden kan worden verkregen door met standaard PCs en standaard webbrowsers contact te maken met deze servers. Het systeem biedt verder groupware en workflow management functies om documenten te beheren en naar de juiste functionele organen te routeren.
Gegevens worden geautomatiseerd uitgewisseld door middel van berichten volgens het OTH-G formaat. Voor de gegevensuitwisseling is een IP netwerk nodig. Naast wide area netwerken en tactische netwerken zijn ook IP radio en satelliet verbindingen mogelijk met het WEBCOP systeem. Verder heeft het systeem de mogelijkheid real time data van Link 11 of Link 14 bronnen in de database op te nemen.

Referenties:
- JWID handout (zie appendix A).

2.2.5 JFACC-AOC

Uitvoerder:
Franse Luchtmacht, DGA Frankrijk, Thomson CSF Frankrijk.

Toepassing:
JFACC-AOC is een systeem voor geautomatiseerde planning en bewaking van lucht campagnes. Gebaseerd op de ontvangen Joint Target List biedt JFACC-AOC ondersteunende gereedschappen om gedetailleerde plannen te maken voor de toewijzing van vliegtuigen aan doelen, planning voor de bewapening van vliegtuigen en de planning van de sorties. Modules van JFACC-AOC kunnen direct worden gekoppeld met Datalink 1, 11, 11B and 16 waardoor real-time bewaking van de luchtcampagne mogelijk is.

Technische Beschrijving:
JFACC-AOC bestaat uit een aantal losse modules. Elke module draait op een UNIX werkstation onder de X-Windows omgeving. Onduidelijk is of en hoe de systemen onderling gekoppeld zijn. Volgens de brochure is een koppeling met de buitenwereld mogelijk op basis van military message handling voor de uitwisseling van informatie over de situatie op het gevechtsveld (SITREPS etc.).

Referenties (zie appendix A):
- JWID handout,
- brochure SICOA,
- kopieën van slides.

2.2.6 VCC

Uitvoerder:
SHAPE

Toepassing:
Het Virtual Command Centre (VCC) vormt het hart van de JWID demonstraties in SHAPE lokatie. Het is volledig gebaseerd op Internet technologie. Op de webserver van het VCC is informatie en resultaten te vinden van overige JWID demonstraties. Voor zover deze demonstraties web-enabled zijn kunnen de demonstraties via het VCC worden benaderd. Verder beschikt het VCC over faciliteiten voor videovergaderen. Het VCC bevat een video en sound server waarmee radio en televisiestations beschikbaar worden gemaakt op de VCC server. Tenslotte is een koppeling gemaakt met het publieke Internet om de informatie aldaar (gedeeltelijk) beschikbaar te maken.

Technische Beschrijving:
Zoals gezegd is het VCC volledig gebaseerd op Internet technologie en met name de WWW technologie. Het hart wordt gevormd door de VCC server. Deze VCC server bevat een groot aantal webpagina's met informatie over de diverse systemen die deelnemen aan JWID. De diverse deelnemers kunnen zelf resultaten en andere informatie toevoegen middels een publikatiesysteem. Voor demonstraties die web-enabled zijn, zoals JACIS en WEBCOP, zijn hyperlinks in het VCC beschikbaar om contact te maken met deze demo's.
Op de VCC server zijn ook een select aantal pagina's beschikbaar van het publieke Internet. Via een 'Info diode' worden deze pagina's regelmatig ververst. De Info diode bestaat uit een tweetal PC's. De eerste is gekoppeld met het publieke Internet, de tweede kan alleen informatie ontvangen van het publieke Internet (het versturen is fysiek onmogelijk gemaakt) en is tevens gekoppeld met het geclassificeerde JWID netwerk. De eerste PC doet regelmatig (en automatisch) aanvragen voor bepaalde webpagina's op het publieke Internet, maar geeft als retour adres het IP adres van de tweede PC. De tweede PC zal derhalve de aangevraagde pagina's ontvangen en sluist deze door naar de VCC server. Vergeleken met een directe koppeling met het Internet of een koppeling middels een firewall is zo op een veiliger wijze een selecte hoeveelheid informatie van het publieke Internet beschikbaar gemaakt.
Op soortgelijke wijze is een selectie van TV en radio stations van de publieke omroep als streaming video en audio beschikbaar gemaakt.
Voordeel van de opzet gebaseerd op WWW technologie is dat met standaard PCs uitgerust met standaard browsers vanaf iedere willekeurige plek in het JWID netwerk deze informatie kan worden benaderd.

Naast de webpagina's biedt het VCC ook faciliteiten voor videovergaderen. Hiervoor is het commerciële product van Proshare geïnstalleerd op een aantal werkstations. Dit systeem is niet vanaf iedere willekeurige werkplek te gebruiken.

Referenties:
- JWID handout (zie appendix A).

2.2.7 SDA

Uitvoerder:
TNO-FEL Nederland

Toepassing:
De Soldier Digital Assistent (SDA) is een compact informatie en communicatiesysteem bedoeld voor de individuele gevechtssoldaat. De SDA zal worden toegepast binnen groepen van soldaten zoals een groep van infanteristen te voet of een groep van mariniers. De SDA bevindt zich nu in de prototype fase. De operationele versie moet het mogelijk maken de gevechtssoldaat te koppelen met C2 systemen van hogere echelons zoals het Nederlandse BMS en ISIS. De SDA biedt de soldaat drie basisfuncties:
- positiebepaling en uitwisseling waarbij de posities van de groep op het scherm in een (nog te implementeren) elektronische kaart worden weergegeven;
- spraakfunctie waardoor de soldaten in de groep onderling kunnen communiceren zoals met een portofoon;
- tekenfunctie waardoor de soldaten onderling aanvullende informatie, zoals missie planning en waarnemingen, aan elkaar kunnen doorgeven.

Technische Beschrijving:
De SDA demonstratie was een stand-alone demonstratie en maakte geen deel uit van het geïntegreerde JWID netwerk. In de toekomst kan koppeling met C2 systemen zoals op JWID getoond tot de mogelijkheid behoren.
De SDA prototype is geïmplementeerd gebruik makend van COTS producten. De SDA bestaat uit een enigszins ruggedized draagbare PC uitgerust met Windows 95. Daaraan is een (militaire) GPS ontvanger gekoppeld voor positiebepaling. De PC heeft een pen-interface waarmee tekeningen op het scherm kunnen worden gemaakt. De pen fungeert ook als 'muis' voor de bediening van het systeem. De spraakfunctie is gerealiseerd door middel van Internet telefonie (voice over IP) software. De SDA communiceren onderling middels een wireless LAN netwerk gebruikmakend van het TCP/IP protocol. TNO-FEL heeft de software ontwikkeld om deze modules te integreren en de besturing van de SDA en de presentatie van de informatie zo gebruikersvriendelijk mogelijk te maken.

Referenties (zie appendix A):
- SDA leaflet;
- JWID handout.

2.3 Ondersteunende gereedschappen

2.3.1 NACOSA VAT

Uitvoerder:
NACOSA

Toepassing:
VAT staat voor het 'Vulnerability Analysis Team'. Dit team analyseert de beveiliging van het de informatiesystemen die op het JWID netwerk zijn aangesloten. Op basis van een beveiligingsplan, bekende dreigingen en bekende of onbekende zwaktes van computersystemen neemt het VAT het totale netwerk van informatiesystemen onder de loep.
Verder bewaakt het VAT het verkeer op het netwerk en is in staat bepaalde aanvallen op netwerk en informatiesystemen te herkennen en te stoppen.
Deze toepassing past in de activiteiten van de NATO op het gebied van 'Information Operations'.

Technische Beschrijving:
Het VAT heeft een tweetal tools gedemonstreerd waarmee de beveiliging wordt geanalyseerd, beide toegespitst op Internet technologie. De eerste tool is de Internet Security Scanner. Deze tool is in staat de aangesloten computersystemen automatisch te analyseren op zwaktes in de beveiliging. De tool doet dit aan de hand van bekende zwaktes in verschillende operating systemen. Voor ieder bekeken computer systeem geeft de tool een lijst van gevonden zwaktes (gemarkeerd naar de ernst van de zwakte) en geeft ook mogelijke tegenmaatregelen. Deze tool draait op een PC onder Windows NT.

Een andere getoonde tool is een network analyser. Deze analyser brengt in kaart welke computers onderling verbinding maken. Verder kunnen datapakketjes van het netwerk worden opgevangen voor verdere analyse. Op deze wijze kunnen verdachte verbindingen worden opgespoord en geanalyseerd. Ook deze tool draait op een PC onder Windows NT.

Referenties:
- JWID handout (zie appendix A).

2.3.2 JDIIC-D

Uitvoerder:
NACOSA

Toepassing:
JDIIC-D is een netwerk management systeem gebruikt voor het beheer van het JWID netwerk. Het JWID netwerk is verdeeld in drie segmenten. Ieder segment heeft een netwerk controle centrum met een JDIIC-D systeem. Ieder netwerk control centrum beheert zijn eigen segment. De JDIIC-D systemen zijn onderling gekoppeld om overall beheer van het netwerk mogelijk te maken.

Technische Beschrijving:
JDIIC-D is gebaseerd op commercieel verkrijgbare producten. Het hart wordt gevormd door HP Openview geïnstalleerd op een krachtige Sun Sparc-20 computer. HP Openview zorgt voor de (grafische) presentatie van de netwerkstatus naar de gebruiker en automatische bewaking van netwerkelementen (bijv. Routers) via management software behorende bij het betreffende netwerk element. Verder is HP Openview gekoppeld met een Remedy en Trouble Ticketing systeem (gebaseerd op een Oracle database) voor de registratie van netwerkproblemen en de bewaking van het proces om deze problemen op te lossen. Communicatie tussen JDIIC-D en netwerkelementen en andere JDIIC-D systemen gebeurt hoofdzakelijk middels het Simple Network Management Protocol (SNMP), het management protocol uit de Internet suite.

Referenties:
- JWID handout (zie appendix A).

3. Conclusies en Aanbevelingen

In JWID '98 is de functionaliteit van C2 systemen van verschillende NATO partners en de onderlinge interoperabiliteit van deze systemen onderzocht. Een belangrijk onderdeel van JWID is het uitvoeren van een gesimuleerde militaire operatie waardoor veel praktijk ervaring wordt opgedaan met de functionaliteit en de interoperabiliteit van de C2 systemen van verschillende NATO partners.

Het eerste resultaat is dat JWID '98 heeft 'aangetoond' dat het mogelijk is commercieel beschikbare systemen te combineren met militaire systemen tot een C4I netwerk ('a system of systems') waarin NATO partners C2 informatie kunnen delen. Functionaliteit van het World Wide Web en Internet technologie spelen bij JWID '98 een belangrijke rol. Deze technologieën maken het mogelijk met een standaard commerciële PC uitgerust met standaard commerciële Web-browser (Netscape, MS Internet Explorer) gebruik te maken van de C2 applicaties van verschillende NATO partners en toegang te krijgen tot het digitale gevechtsveld vanaf elke plek in het netwerk. Hierdoor wordt de gebruiker ontkoppeld van de technologie die is gebruikt om de C2 applicatie te implementeren. Het resultaat is dat met relatief lage kosten een dergelijk C2 systeem beschikbaar kan worden gemaakt voor een groot aantal gebruikers. Vraagtekens blijven bestaan bij de robuustheid en beveiliging van de getoonde produkten. Voor JWID zijn dit minder belangrijke criteria aangezien het hier gaat om de praktische bruikbaarheid van nieuwe technologieën.

De verschillende C2 systemen zijn veelal in staat informatie uit te wisselen op basis van een militair berichten formaat (bijv. ADatP-3 of OTH-G). Een tweede resultaat van JWID '98 is dat de uitwisseling van deze informatie tussen C2 systemen van verschillende NATO partners vaak nog moeizaam is. Enerzijds omdat er veel implementatie-varianten zijn van dezelfde berichtenstandaard, anderzijds omdat de verschillende C2 systemen afwijkende datamodellen gebruiken. Verder zal in de praktijk nog aangetoond moeten worden of militaire netwerken voldoende bandbreedte beschikbaar hebben om de gedemonstreerde technologiën te ondersteunen. In de komende jaren zullen daarvoor oplossingen moeten worden gevonden om te komen tot een echt geïntegreerd C4I netwerk.

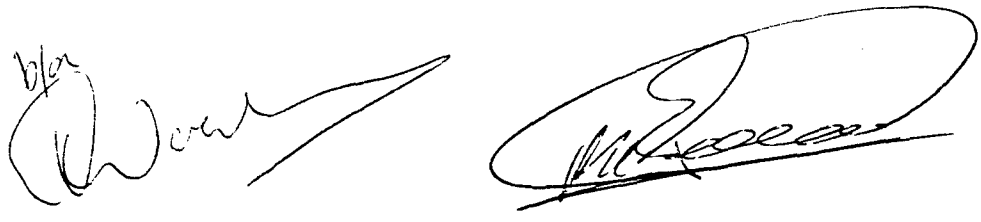
Binnen Nederland zijn C2 systemen in ontwikkeling of in verwervingsvoorbereiding die vergelijkbaar zijn met de systemen gedemonstreerd op JWID '98. Voorbeelden zijn ISIS, BMS en SDA van de Koninklijke Landmacht en het C2P systeem van de Koninklijke Marine. Omdat JWID '98 heeft aangetoond dat met name de interoperabiliteit van C2 systemen van verschillende NATO partners nog beperkt is, ondanks toepassing van berichtenstandaarden, wordt aanbevolen om met Nederlandse C2 systemen deel te nemen aan toekomstige JWID demonstraties. Door deelname wordt waardevolle praktijkervaring opgedaan die kan worden gebruikt in de ontwikkel- en aanschafprocessen van deze systemen

en kan bijdragen aan de functionaliteit en de interoperabiliteit van huidige en toekomstige systemen welke voldoen aan de wensen van de krijgsmacht.

4. Afkortingen

BMS	Battlefield Management System
C2	Command & Control
C4I	Command, Control, Computers, Communication & Information
COTS	Commercial Of The Shelf
CWAN	Coalition Wide Area Network
GPS	Global Positioning System
HP	Hewlett Packard
HTML	HyperText Markup Language
IP	Internet Protocol
JWID	Joint Warfare Interoperability Demonstrator
MHS	Military Message Handling
NC3A	NATO Command Control & Communication Agency (voorheen SHAPE Technical Centre)
PC	Personal Computer
RCU	Radio Control Unit
SDA	Soldier Digital Assistant
SHAPE	Supreme Headquarters Allied Powers Europe
SITREP	Situation Report
SMTP	Simple Message Transfer Protocol
SNMP	Simple Network Management Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TNO-FEL	Nederlandse organisatie voor Toegepast Natuurwetenschappelijk Onderzoek - Fysisch en Elektronisch Laboratorium
VAT	Vulnerability Assessment Team
VCC	Virtual Command Centre
WWW	World Wide Web

5. Ondertekening



D.W. Fikkert
Groepsleider

Ir. P.H. Zwaard
Auteur

Bijlage A Brochures van JWID '98

Inhoud

A.1 Handout JWID '98

NORTH ATLANTIC TREATY ORGANISATION
JOINT WARRIOR INTEROPERABILITY DEMONSTRATION (JWID 98)

HANDBOOK

This handbook was prepared by the Supreme Headquarters Allied Powers Europe (SHAPE) as a synopsis of NATO's participation in the Joint Warrior Interoperability Demonstration 1998 (JWID 98). This handbook is intended to increase the visitor's awareness of the C4I technology being demonstrated during JWID 98, and to highlight NATO's and United States' Objectives.

TABLE OF CONTENTS

Background of JWID 98

The Joint Warrior Interoperability Demonstration (JWID) 98 is a continuation of previous United States efforts beginning with the Integrated Tactical-Strategic Data Networking demonstration started in 1989 and later called Secure Tactical Data Network demonstrations in 1991, which supported the US Joint Staff Command, Control, Communications, Computers, and Intelligence (C4I) for the Warrior initiatives. This year's demonstrations provide a showcase for technology, networking and interoperability within the environment of a Coalition Task Force. Of prime importance is the "value to the warfighter" and specifically the support to a Coalition Task Force Commander's C4I requirements.

The US Navy is the lead service for JWID-98. The US Atlantic Command (ACOM) is the lead Commander in Chief (CINC) for JWID-98. While JWID-97 was a theme year, JWID-98 is an exploitation year, focusing further exploitation of JWID-97 technology as well as new technology.

JWID-98 will demonstrate technological solutions to Joint C4I problems within a Navy-led Coalition Task Force. It will be a joint demonstration of existing, off-the-shelf, new and evolving technologies that solve Joint C4I interoperability shortfalls while providing seamless information exchange for the joint warfighter. Conducted in the July 1998 timeframe, JWID-98 will address interoperability problems of today, while maintaining a focus on the future joint warfighting environment, thereby providing the opportunity to use technology to shape the battlefield of the future.

While JWID-97 was led from Joint Battle Centre, Washington DC, JWID-98 will be led from Blandford Camp in UK. The UK JWID-98 Project will host the facilities. The JWID-98 Demonstration Control Group will be established at Blandford Camp. Also the Coalition Wide Area Network (CWAN) will be managed from Blandford Camp as well as the Coalition Vulnerability Assessment Team (CVAT).

The US Global Command and Control System (GCCS) will be deployed on the CWAN to different Allied sites. The GCCS will be the principal system for managing the Common Operational Picture (COP) executed by Joint Battle Center in Washington DC.

NATO's initial participation was in JWID-94. In JWID-96, NATO conducted 12 demonstrations between the SHAPE bunker and the NATO C3 Agency (NC3A), Den Haag. In JWID-97 participation evolved into sixteen demonstrations. In JWID-98 NATO will conduct 12 demonstrations which include active participation from SHAPE, NC3A, Spain, France, Turkey and The Netherlands. The demonstrations continue to focus on interoperability issues between US, NATO and other allied systems as well as developing web solutions to address NATO's C3I future requirements. NATO will showcase this year's demonstrations at its primary demonstration site in the SHAPE bunker in Mons, Belgium and other secondary sites in Rota, Spain. There will also be connections into Ankara, Turkey and Taverny, France. However, these will not be visitor sites. The Roving Command Vehicle (RCV) from NC3A will be placed at Blandford Camp, UK with links back to SHAPE.

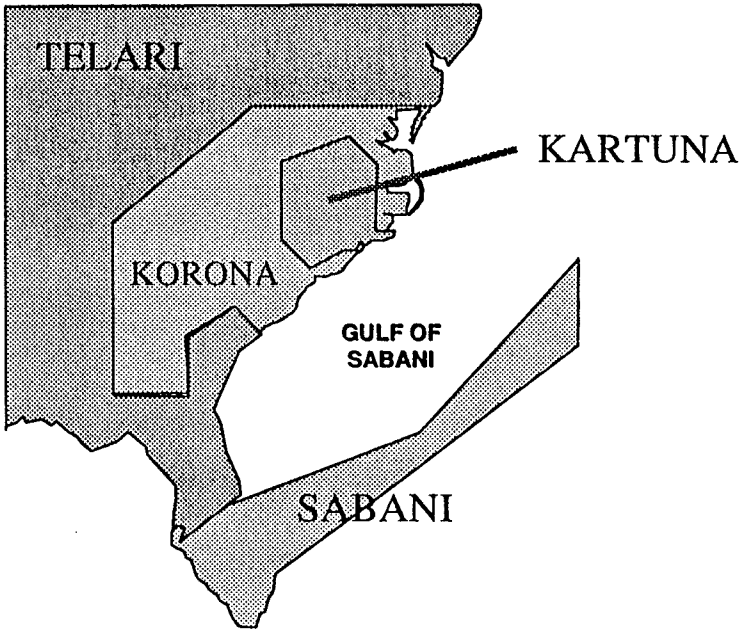
Operational Environment

The operational environment is developed within a scenario that encompasses two countries in the CINCUSACOM AOR: Korona and Kartuna. Two other countries in the region, Sabani and Telari, are not directly involved in the conflict.

The JWID scenario uses a real map of the southeastern United States encompassing Virginia, North Carolina, South Carolina, Georgia, and Florida. The place names are notional but the geographic locations are accurate in relationship to the southeastern United States. Figure 2 depicts the JWID-98 boundary lines.

The demonstration scenario covers eight phases: pre-deployment, deployment, presence, hostilities, forcible entry, build up, decisive combat and re-deployment. Only the phases; presence, hostilities, forcible entry, build up and decisive combat will be played during four scenario days. In all phases, Coalition forces will face a terrorism threat. The force structure consists of combined ground, air, and maritime components, to include carrier battle groups and amphibious task forces. These forces will conduct combined operations that include amphibious and airborne assaults, and split-based operations.

Scenario Boundaries



JWID-98 US Joint Staff Objectives (As of 1997, and the basis for the exploitation year 1998):

1. Demonstrate real-time and seamless information exchange between multiple levels of security at the CTF and component level, particularly for the purposes of command and control (C2) and collaborative planning.

2. Demonstrate innovative telecommunications and information management technology that enhances data delivery to and from Joint Warriors at the unit level, particularly common operational picture and imagery.

3. Demonstrate tailorable Dominant Battlespace Awareness (including 3D) in a CTF setting, highlighting multimodal data fusion, common operational picture track correlation and management.

4. Demonstrate sensor-to-sensor and sensor-to-shooter technologies to enhance combat identification and theater missile defense in a Coalition environment, and to provide targeting information for stand-off and precision guided munitions utilizing selected portions of the Joint Requirements Oversight council (JROC) approved precision strike C4I architecture.

5. Demonstrate technologies that enhance information superiority through the use of Information Operations/Information Warfare (IO/IW). These technologies should provide assurance of coalition access, use, and integrity of command, control, communications, computer, intelligence, surveillance and reconnaissance (C4ISR) systems while preventing unauthorized use of the same.

6. Demonstrate the ability of commercial off-the-shelf/government off-the-shelf (COTS/GOTS) technology to provide constant data exchange with in-garrison, in-transit, and deployed elements of the CTF.

7. Demonstrate enhancements to the Defense Information Infra-structure (DII) that improve its utility and interoperability to the CTF.

8. Demonstrate an integrated, near real-time focused logistics system with a planning and decision support capability. The system should track all classes of supply, pre-positioned war reserve assets, and personnel to and from the sustaining base and wholesale depots.

9. Demonstrate the ability to provide an integrated solution for all tactical and non-tactical applications on a single PC.

10. Demonstrate the ability of Information Technology to identify and solve millennial problems in order to operate beyond the year 2000.

NATO JWID-98 Objectives

The following are the NATO JWID-98 objectives. These are the basis for the selection of the NATO demonstration to JWID-98.

- NATO Common Operational Picture (COP) Development and links to US Global Command and Control System (GCCS)
- Integration of NATO and US systems to Virtual Command Centre (VCC)
- Integration of Email and formatted messages
- Multi Level Security systems and data labeling (database and HTML)
- Joining LANs to CWAN with different classification levels
- Joining National Systems to CRONOS and the VCC
- Exploitation of NT Operating System
- Automatic file translation to HTML
- Collaborative Planning Tools and Web Front Ends

NATO will conduct twelve demonstrations as identified below to address the following areas of interest to NATO:

a) Interoperability between NATO Systems (WebCOP, VCC, SIPAC, and others).

b) Interoperability between the US Global Command and Control System (GCCS) and NATO systems such as: WebCOP from Spain, SIPAC and MESREG from France, and OTEMAS from Turkey.

c) Maximize the use of COTS and GOTS for data exchange.

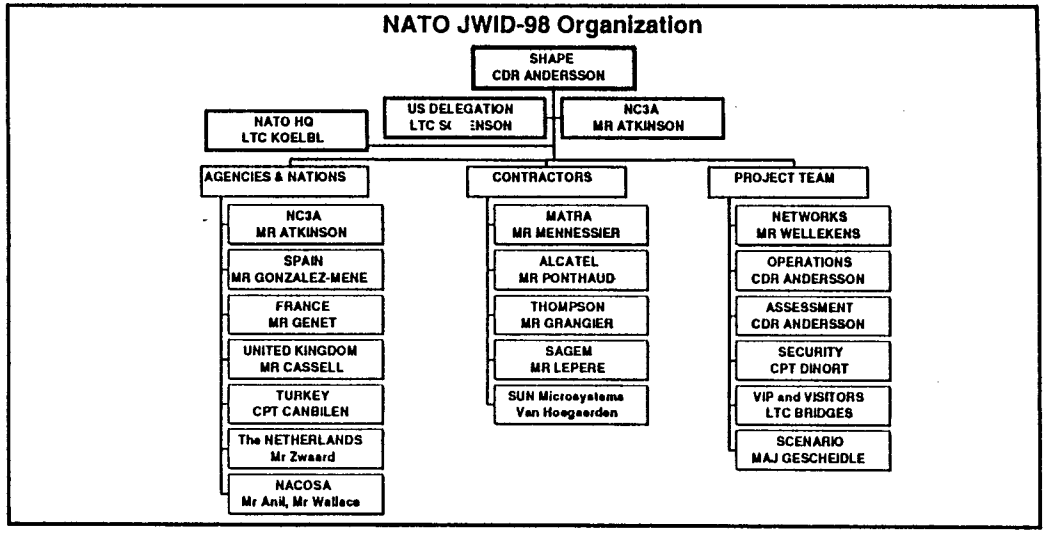
d) Integration of command functions into a Virtual Command Center utilizing Web Technology.

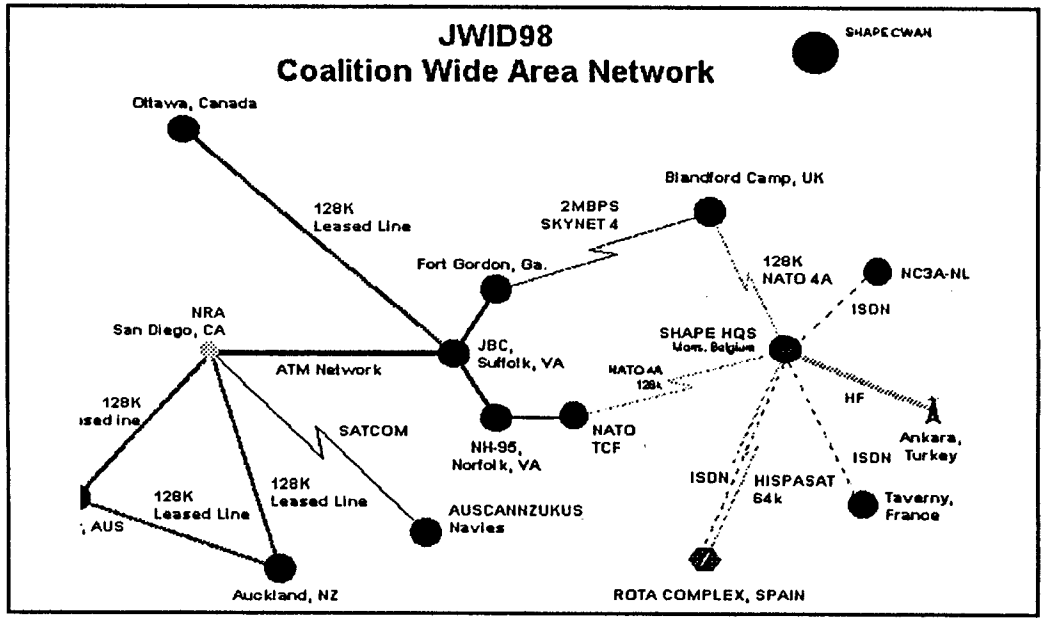
e) Provision of integrated solutions on a single PC.

f) Exploit the Virtual Command Center with security solutions using NT

NATO JWID-98 Organization

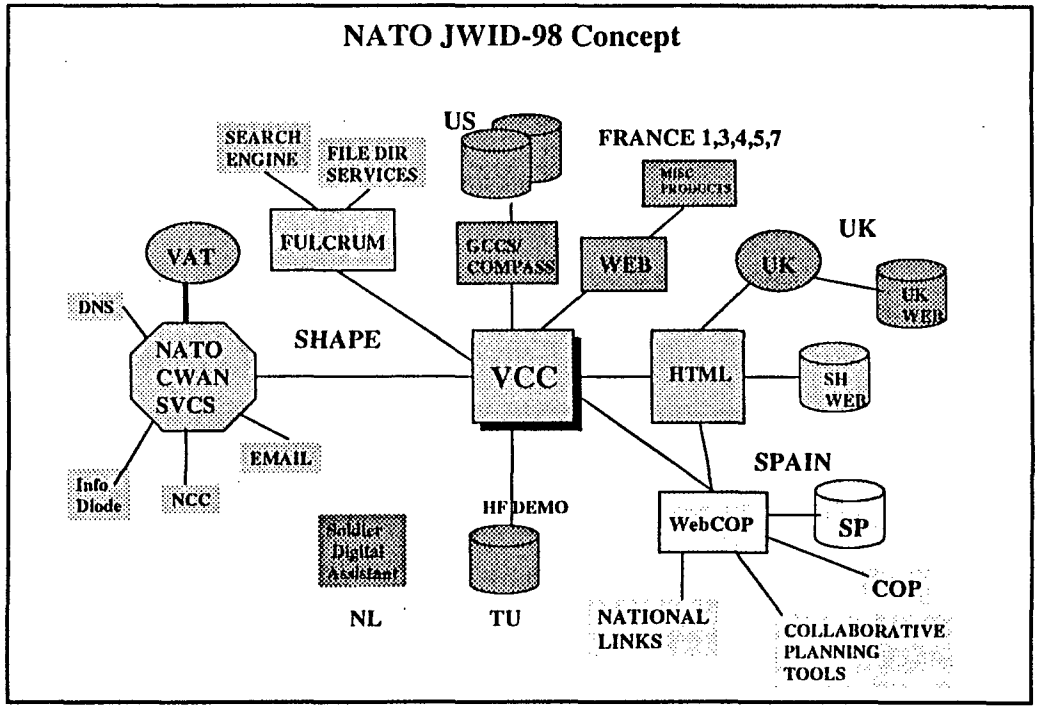
The NATO JWID-98 organization is reflected in figure 3. The Senior Management Group (SMG) is the highest level in the NATO JWID-98 organization. The SMG consists of; Mr. B. Atkinson NC3A – The Hague, LTC B. Sorenson US Del NATO, LTC J. Koebl NATO HQ and CDR T. Andersson SHAPE.





NATO'S Participation Overview

NATO will establish a Virtual Command Center (VCC) that integrates all command functions into a single PC and utilizes web technology to simplify operational procedures while becoming platform independent. The figure below provides a general concept of this VCC and how it integrates into JWID-98.



The use of the VCC and the JWID-98 Coalition Network, will allow NATO to play the scenario from the SHAPE bunker representing the NATO Contingent Deployed HQs'. The products of the various NATO demonstrations can be displayed at all JWID sites by using web technology and a standard PC with a browser.

The SHAPE bunker in Mons, Belgium, will serve as the entry node into the JWID-98 Coalition Network. This hub will provide connectivity to all the NATO demonstration sites including SHAPE (BE), Spain, France, Turkey and NC3A. The NATO JWID-98 network extends the Coalition WAN (CWAN) using a mixture of satellite links, landline and Internet links connecting all the NATO demonstration sites. The secured network operates at a security level up to NATO Secret Releasable to the Coalition. The Internet network operates as non-classified. NATO demonstrations linking to US demonstrations provide an excellent opportunity for the exchange of data, procedures and products between NATO and US JWID participants. Included are web tools and technology; Common Operational picture (COP); messages; multi-media applications, protocols and others.

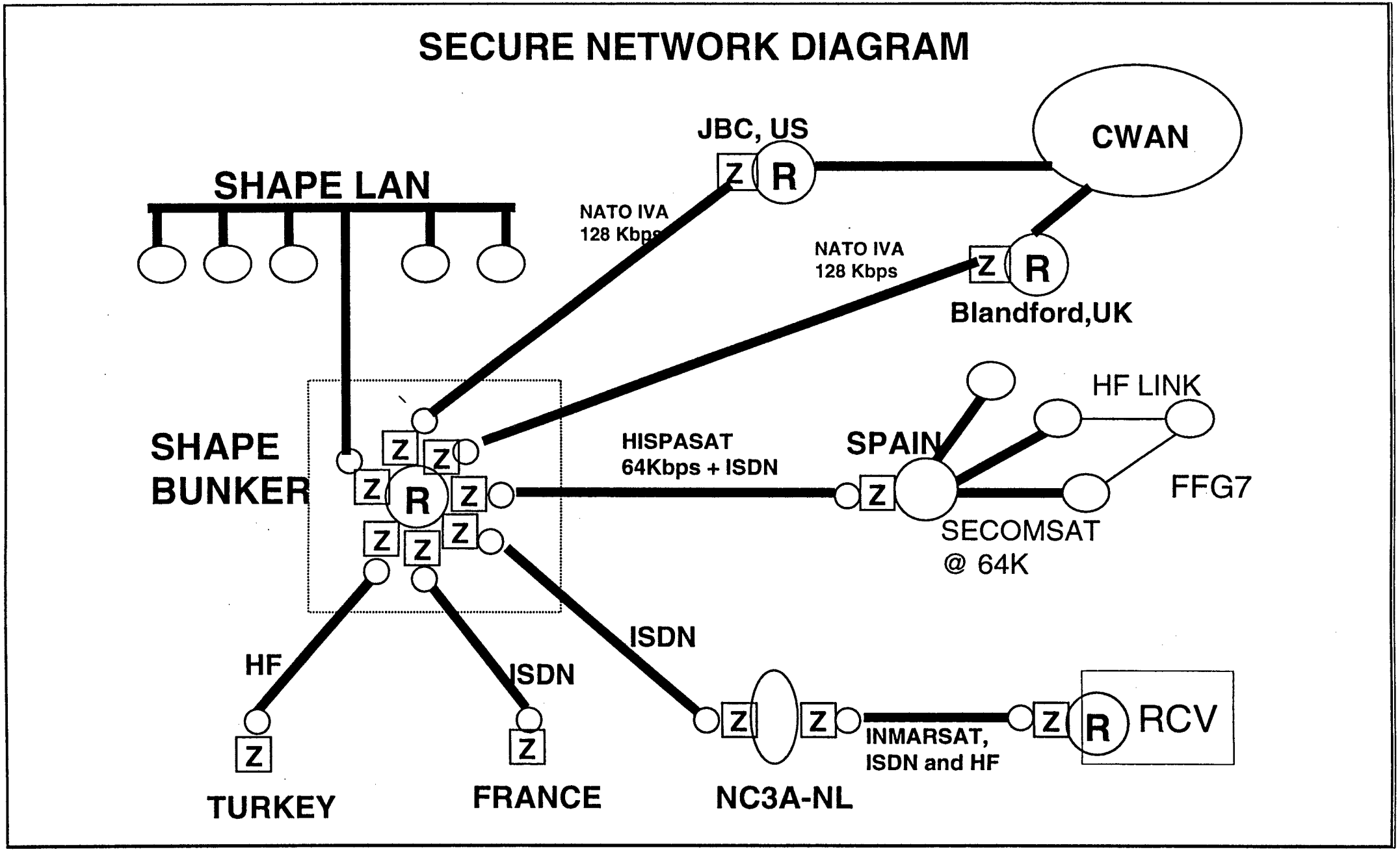
NATO's principal VIP demonstration site is the SHAPE bunker in Belgium. The visitors week from 27 July to 30 July 98, coincides with the UK JWID-98 VIP week. Visitors can also visit the national demonstration site in Rota, Spain.

To publicize NATO's participation in JWID-98 to the widest audience, NATO developed a homepage in the Internet (http://www.nacosa.nato.int) that provides additional information and details on NATO's efforts and the specific objectives of each demonstration.

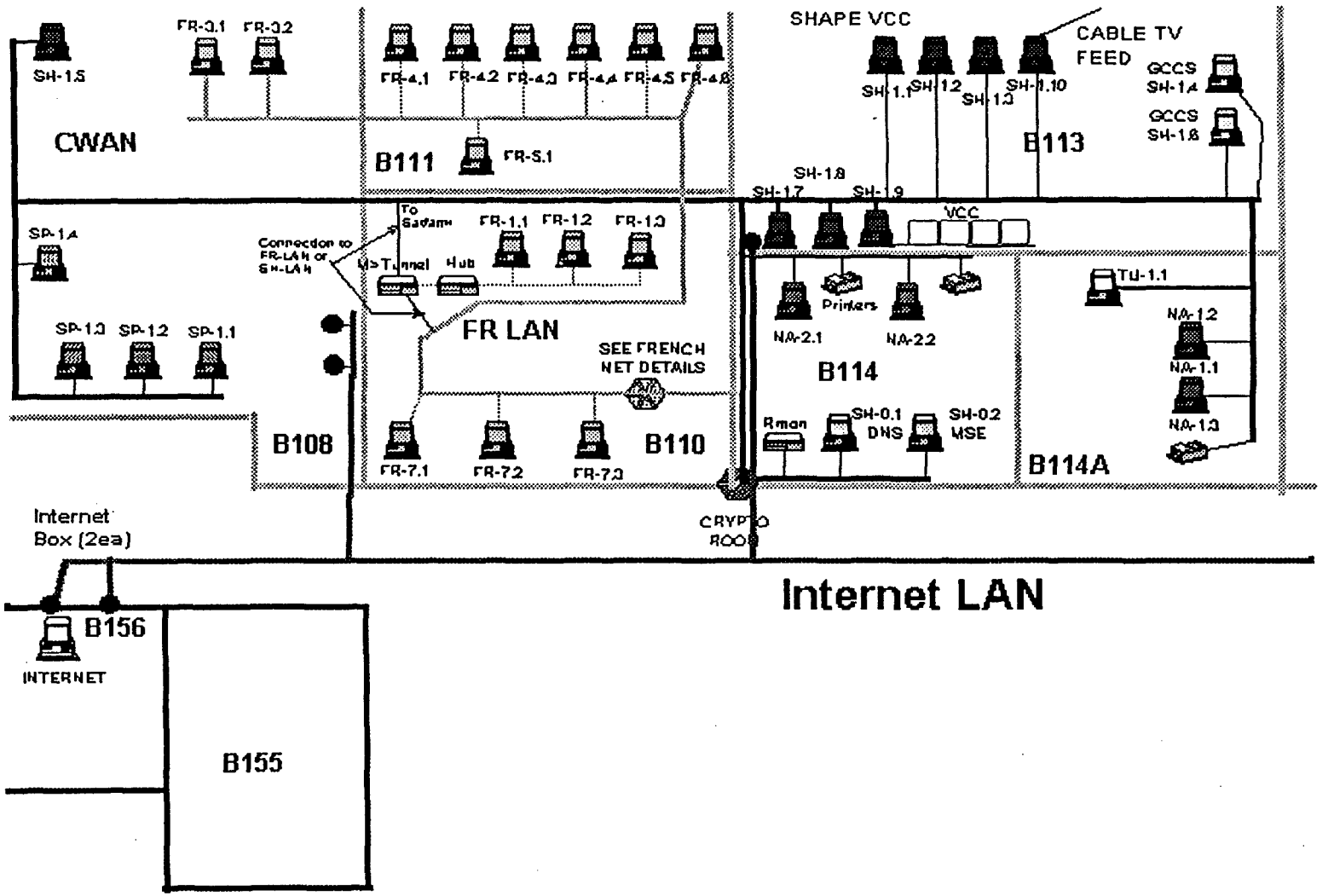
NATO Network Configuration.

The NATO JWID-98 network is a hybrid composed of various networks. The principal network is a TCP/IP backbone extending the CWAN to the SHAPE with extension to Spain, France, Turkey and NC3A. SHAPE connects to the CWAN via two links; to Blandford Camp, UK and to Joint Battle Center Washington DC, US. The SHAPE and Spanish nodes utilize internal LANs to connect the various stations or demonstrations to the principal backbone and to other coalition sites. France connects to the SHAPE LAN from a separate French LAN in the SHAPE Bunker. The Netherlands demonstration is standalone and not linked to the CWAN. The NATO network topology is described on the next page.

The second major NATO network is an extension of the Internet. NATO sites use either single workstations or LANs connected to the Internet to meet local unclassified demonstration requirements and to conduct general administration of the JWID-98.


SECURE NETWORK DIAGRAM
JBC, US
CWAN
SHAPE LAN
NATO IVA
128 Kbps
NATO IVA
128 Kbps
Blandford,UK
HF LINK
SHAPE
BUNKER
HISPASAT
64Kbps + ISDN
SPAIN
FFG7
SECOMSAT
@ 64K
ISDN
HF
ISDN
INMARSAT,
ISDN and HF
RCV
TURKEY
FRANCE
NC3A-NL

Bunker Demonstration Layout



NATO JWID 98 Demonstrations

FRANCE-1 : MULTINATIONAL AMPHIBIOUS OPERATION

FRANCE-3 : SIPAC-NT

FRANCE-4 : JFACC-AOC

FRANCE-5 : TACTICAL INFORMATION SYSTEM WITH GPS, IMAGERY, GSM AND CNR RADIO CAPABILITIES

FRANCE-7 : JACIS

NACOSA-1 : VAT CAPABILITY FOR DEFENSIVE INFORMATION WARFARE

NACOSA-2 : JDIICS-D in the NATO and Coalition Environment

SHAPE-1 : VIRTUAL COMMAND CENTRE (VCC)

SPAIN-1 : C2IS AND MIS WEB SYSTEM-WEBCOP

TURKEY-1 : RADIO-BASE MESSAGE TRANSMISSION SYSTEM (OTEMAS)

NC3A-1 : ROVING COMMAND VEHICLE (RCV)

NETHERLANDS-1 : SOLDIER DIGITAL ASSISTANT (SDA)

THE FOLLOWING PAGES CONTAIN DETAILED DESCRIPTIONS OF EACH DEMONSTRATION. THESE ARE THE DEMONSTRATORS' OWN DESCRIPTIONS.

FRANCE-1

MULTINATIONAL AMPHIBIOUS OPERATION

SPONSORS: FRENCH MOD AND MATRA SYSTÈMES & INFORMATION

Objectives

- Demonstrate the interoperability between the French CIS involved in an amphibious operation(ACOM and SIR)and Alliance's similar systems available for this exercise (GCCS and JMCIS).
- Show the capacity of the French systems to run in and to manage a joint multinational operation.
- Show new Intranet technology (E-mail messages, HTML pages, browser) with the validated use of different interoperability standards (ADatP-3 and OTH-GOLD messages).

Description Overview

The operational frame of the FR-1 scenario is to participate in a multinational amphibious operation, the aim of which is to rescue nationals. The capacities of the French CIS are used in the operational scenario. The coordination of this multinational deployment (see Figure 1) enables multiple and varied exchanges with other participating nations.

ACOM is the French Navy CCIS (similar to JMCIS and MCCIS) currently fitted on more than 50 ships. SIR is the French Army Battlefield Digitalization Program federating all the sensors and the weapons systems of the battlefield. The SIR demonstrator is shown on the « satellite farm » during JWID 98. ACOM and SIR are able to automatically exchange, process and display sets of consistent information. At each command level, these systems build up a common picture. This picture is automatically updated by automated message processing (no man in the loop).

In JWID 98 exercise, the focus is made on the interoperability aspect which represents one of the most challenging issues in all multinational operations

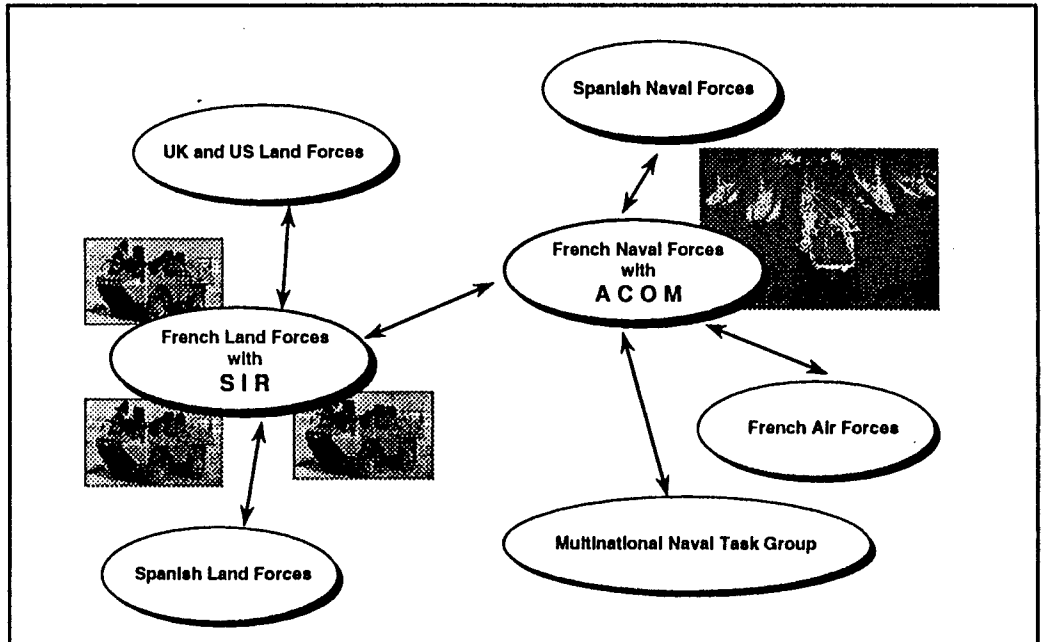


Fig 1 - Multinational Coalition Deployment

(see Figure 2). ACOM and SIR are widely open and enable high-level interoperability with other systems, based on well-known military or commercial standards such as ADatP-3, OTH-GOLD, HTML, Java scripts and SMTP. These large capacities enable to exchange and share data with other similar systems using the same exchange standards.

Our demonstration is distributed between the bunker (workstations) and the satellite farm (SIR Demonstrator fitted in an APC). This vehicle, fitted with all relevant equipment, illustrates the future French Army command vehicle. It was

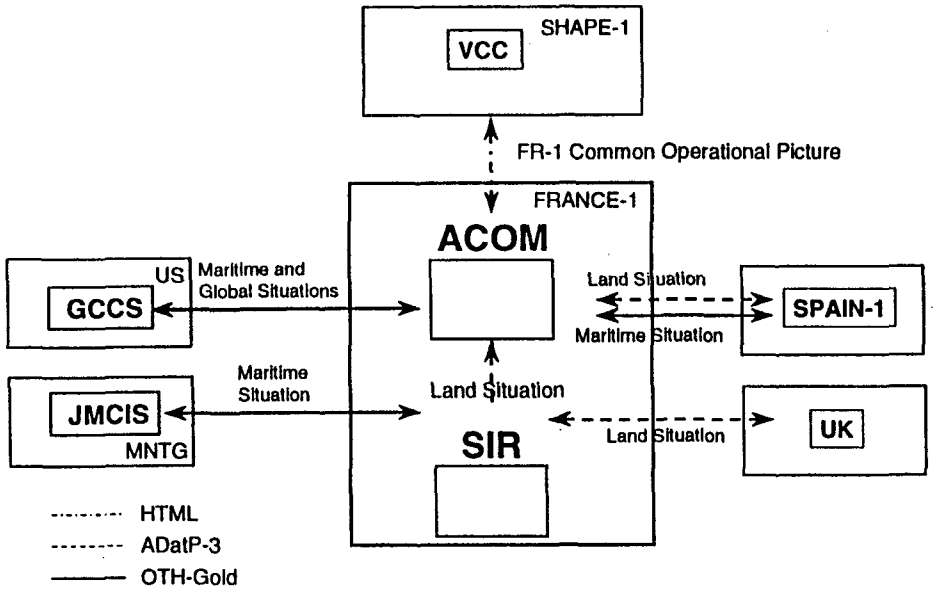


Fig 2 - National & Multinational Interoperability

successfully operated during the BIP (Battlefield Interoperability Program) in November 97 (Munich) with Germany, UK, and US.
For the specific case of JWID configuration, some connections are built up on IP links instead of operational communications (L11, tactical VHF radio or area networks, HF radio network, satellite link) only to make it easier to operate in the SHAPE environment; one IP link is enciphered with the MATRA product M>tunnel (COTS).

Anticipated Results

- ACOM: to demonstrate its capacity to manage a multinational amphibious operation. The system is expected to provide the JWID participants with a Common Operational Picture.
- SIR : to demonstrate the capability to command a multinational task group of land forces and confirm its interoperability scope already tested during the BIP experiments in Germany in November 97.
- Show the high level of interoperability already achieved thanks to the use of complementary solutions based, in one hand, on military standards and proven mechanisms (ADatP-3 and OTH-GOLD messages) and in the other hand, on commercial information technologies (HTML pages and Javascripts).

Collaborating Agencies/Industries

- French MOD : Joint Staff and Procurement (DGA)
- French ARMY
- French NAVY
- MATRAnet
- MATRA Systèmes & Information
- MOSAIC

FRANCE-3

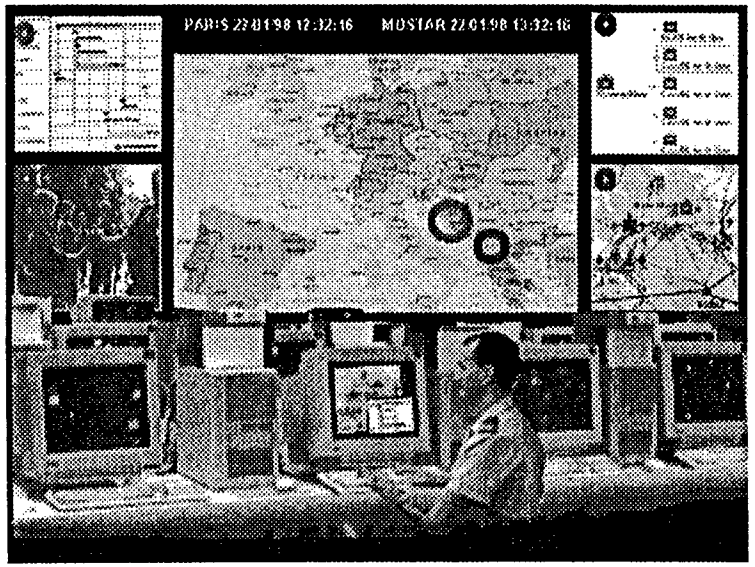
SIPAC-NT

SPONSOR: MOD FRANCE AND ALCATEL ISR

Objectives

SIPAC-NT is a CCIS dedicated to the Joint Forces command and control level. The objectives of the demonstration are two-fold:

- On the operational side, to demonstrate the capability to integrate and to handle into a single database various types of data (army, air, maritime friendly/hostile forces, logistics, humanitarian, etc.) coming from different sources, in order to provide very flexible information management and situation assesment capabilities, adapted to the new operationnal environment dominated by crisis management.
- On the technical side, to demonstrate how the integration and cutomization of standard COTS (Lotus-Notes, MS-Project) enables to deliver easy-to-use, and cost-affordable joint-forces CCIS components.



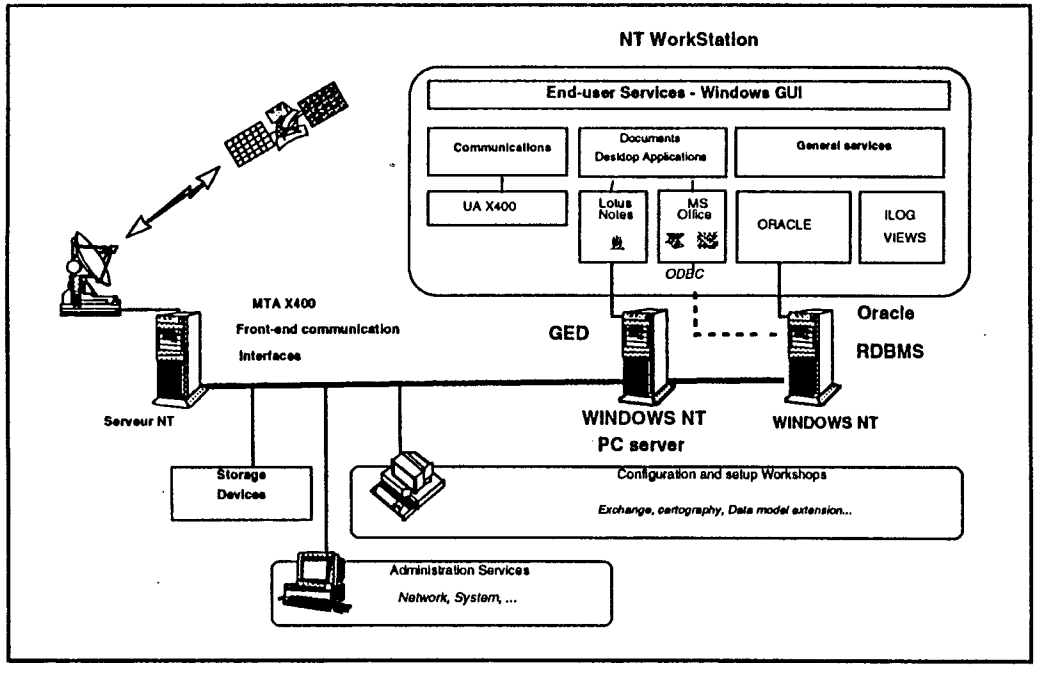
Description Overview

SIPAC-NT has been experimented for the first time during the multi-national « EOLE 98» exercise which took place in the south of France in June 98 and implied France, Italy and Spain. It was installed at the allied joint-forces headquarter.

The demonstration will be based on the data of this exercise and will illustrate major feedbacks and results from this exercise.

The demonstration will illustrate the main features of the SIPAC-NT system:

- The complete integration of all user services on a single PC workstation (MHS, documents management and edition, operationnal data and maps management, situation synthesis production, ...).
- The use of standard COTS (lotus-Notes) for providing a very exhaustive set of integrated services including message handling, workflow management, documents management, Intra-Net information broadcasting.
- A flexible approach for data management based on the concept of data folders, which enable users or system administrators to configure customized access and personnal views to a multi-source data-repository.
- The capability to add new object-types into the system in order to meet unplanned information management requirements.



Details of the Project

SIPAC-NT has been developed within the framework of the French SICA project which is managed by the French MOD/DGA/SPOTI services. The aim of this program is the development of information systems at the joint forces level.

All the user services run on WINDOWS-NT PC workstations, connected to a WINDOWS-NT server supporting Lotus-Notes and Oracle Server. Some tools dedicated only to system administrators (data dictionary administration and maps acquisition workshop) run on a UNIX workstation.

Collaborating Agencies/Industries

- ALCATEL ISR - MASSY - FRANCE
- French MOD DGA/SPOTI/DP SICA - ISSY-LES-MOULINEAUX – FRANCE

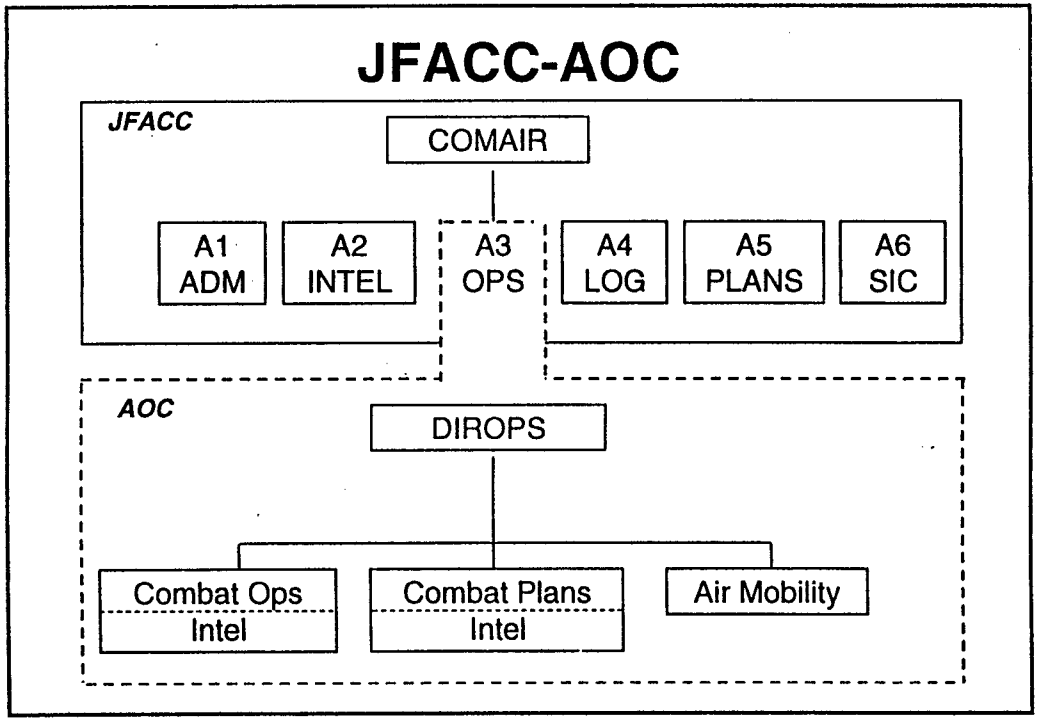
FRANCE-4

JFACC-AOC

SPONSOR: THOMSON-CSF COMMUNICATIONS

Objectives

The aim of the demonstration is to show how the JFACC-AOC functionality are supported by co-operative systems independently developed, which interoperate together and with external systems through communication assets. It sets up on JWID 97 capabilities and advocates the Intelligence support at all decision levels.



Description Overview

The Air Campaign intelligence gathering and fusion is a process that balances between the normal push of data and the requirements pull, taking into account various time frames and forecast needs.

The TRACE system collects and provides information based upon all available Joint intelligence information (SIGINT, IMINT, RADINT, HUMINT, etc.) to support the Joint Air Campaign.

TRACE will demonstrate how the Commanders can be aware of the present and predicted threats that arise from the situations it has gradually built up. It will also demonstrate availability of target status information relevant to the required time frame.

At the beginning of an Air Campaign, the JFACC receives Joint Target Lists, Provides Guidance, Apportionment and Targeting. It develops Concepts of Operations (CONOPS). On a daily basis it plans for D+2 and issues the Air Operations Directives (AOD).

The ASPLAN system addresses the apportionment choices and the initial decision aspects of the COA. It supports the corresponding planning and targeting process and helps determining the overall feasibility. It is interoperable with TRACE (Intel. system), with ASPRO.

ASPLAN will demonstrate how:

- The « CONCEPTION » Application assists the COA definition
- The « PLANIFICATION » Application assists the daily adaptation

The information is shared between the two applications
AT CAOC level, the Combat Plans generates the Master Air Plans (M.A.P), Air Coordination Orders, and Air Tasking Orders (ATO) while Combat Ops control the current operations.

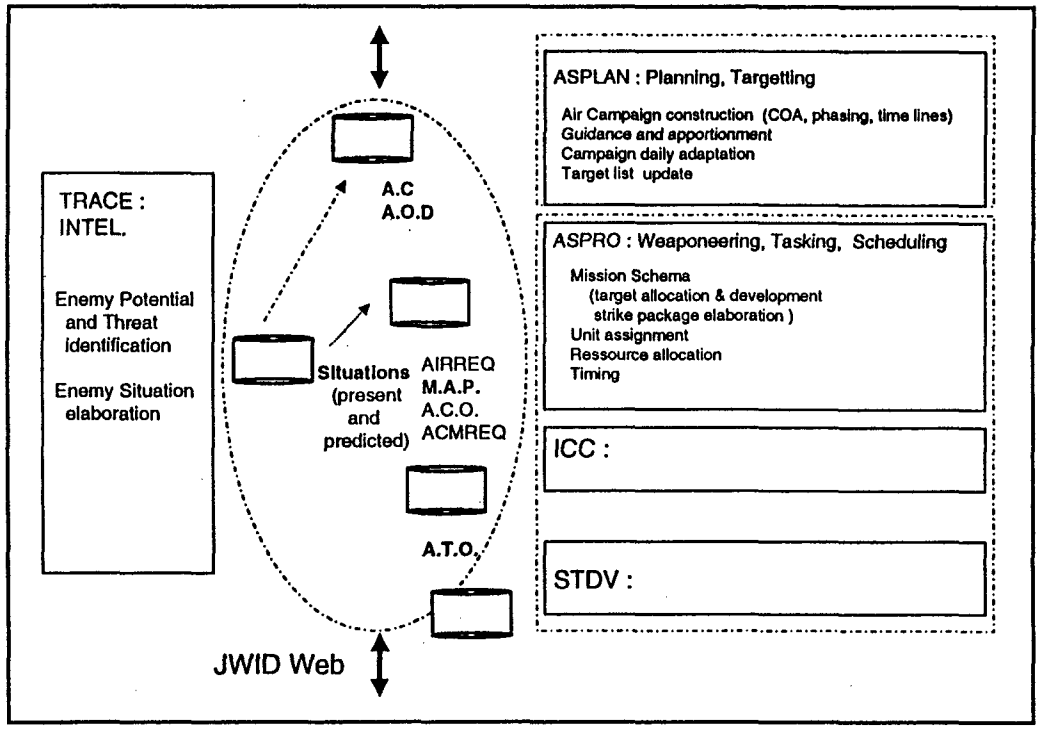
The ASPRO system offers an AOD editor and addressees the mission schema

definition and the weaponeering, tasking and scheduling involved, within the D+1 time frame. It is interoperable with TRACE, with the Joint Level or Army SICF, and with ICC.

It can handle messages about battle field situation (OWNSITREP, ENISITREP, etc.) from the Joint Level . It can receive an AIR REQUEST from the Army Units and answer with an ATM (air task message) in real time. It can exchange with ICC all information needed to set up (ex resources).

ASPRO will demonstrate how:

- It helps to make the important choices for the main missions, optimizing resource use under full control of operators, relying on JIPTL input and up to date target status information, and elaborates the Master Air Plan (MAP),
- It elaborates the ACO, under full control of operators.



Once the MAP process is completed, the ATO development goes on within ICC, considering the MAP as an ATO Shell for Strike, Air Defense, Planning refinement, and using ATO dissemination capabilities to all units. The current operations can then rely on STRADIVARIUS.

JWID Web gives support to a federation concept called BIBOP that aims to enhance interoperability between Intelligence systems, Planning systems (via a common picture based on visual, scripted information or on data exchange) and bring openness to Joint Level Information and Force level Data.

Anticipated Results

Efficient C4I are a must as « the decision process can only be as good as the C4I ». Interoperable C4I such as TRACE, ASPLAN, ASPRO are the next step, setting a trend towards a « seamless application of joint air power » and supporting a iterative process on a multi level basis (Air Campaign & AOD; Mission Schema & MAP, etc.).

Collaborating Agencies/Industries

- FRENCH AIR FORCE
- DGA (FRENCH MOD)
- THOMSON CSF COMMUNICATIONS

FRANCE-5

TACTICAL INFORMATION SYSTEM WITH GPS, IMAGERY, GSM AND CNR RADIO CAPABILITIES

SPONSOR: FRENCH MOD AND SAGEM SA - DEFENSE AND SECURITY DIVISION - FRANCE

Objectives

To illustrate how the Tactical information system MESREG will ease command and control by automating message handling within JWID-98 network. The main objectives supported are:

- To exchange messages, positions and images between MESREG terminals spread over the field of operations by using all available links in the operational context - digital or analog VHF radio nets, switched telephone network, mobile phone network,
- To join National Systems to CRONOS and VCC by pushing the messages, positions and images collected from a mobile terminal in the VCC and CRONOS by using a local net (Ethernet).

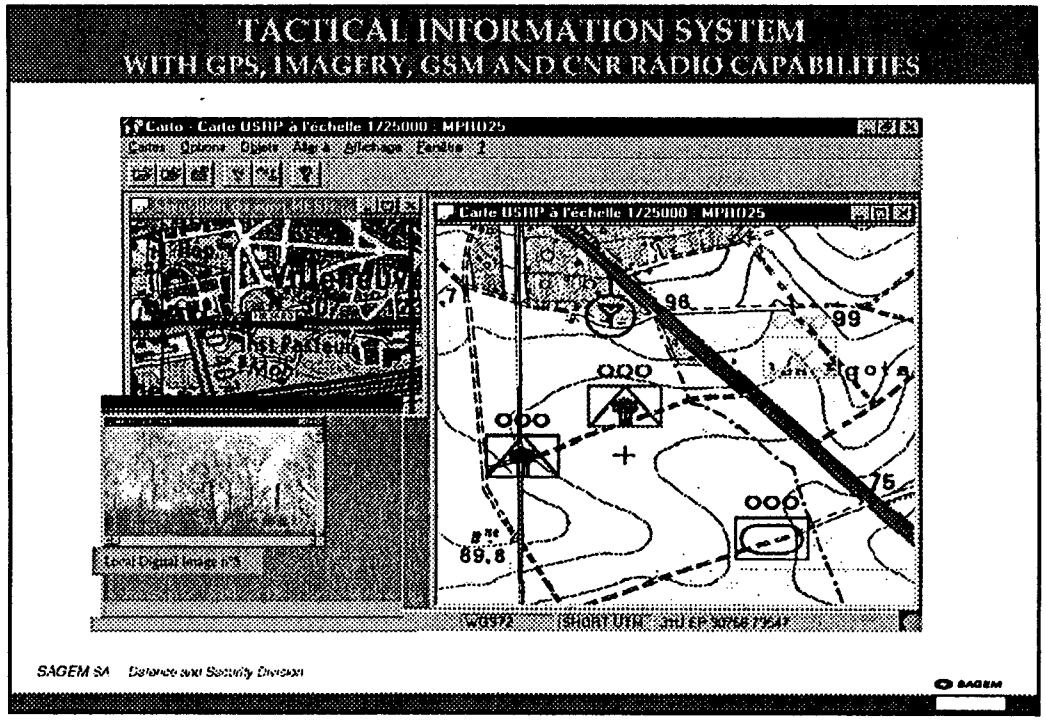
To attend these objectives, the MESREG system integrates:

- Email and messages formatted in ADatP3 formal type,
- A digital camera to add images in the informal messages,
- An integrated digital map coupled with a GPS receiver to localize mobile terminal in real-time.

Description Overview

The demonstration will show how operators on the JWID-98 network could use MESREG system facilities to exchange data between:

- The mobile terminal and the battalion terminal located outside
- The mobile terminal and the terminal located at the HeadQuarter (HQ) in the bunker
- The terminal in the bunker and CRONOS or VCC



Operators communicate together by the MESREG messaging system. All kinds of messages can be exchanged. They can be freehand messages, text or drawings, images, HTML pages, computer files or military messages in AdatP3 formal type. The latter are intended to be processed directly by the headquarter computers which could constantly maintain an up to date picture of the tactical situation.

A PC Card ciphering unit provides security, confidentiality and integrity of the message content. This crypto PC Card is based on a French cryptographic algorithm.

Anticipated Results
At the MESREG HQ terminal, operators will be able to:

- Receive encrypted data from the mobile terminal by a mobile phone network and the public switched network (PSTN),
- Feed the VCC and CRONOS through a web interface by a connection to the CWAN.

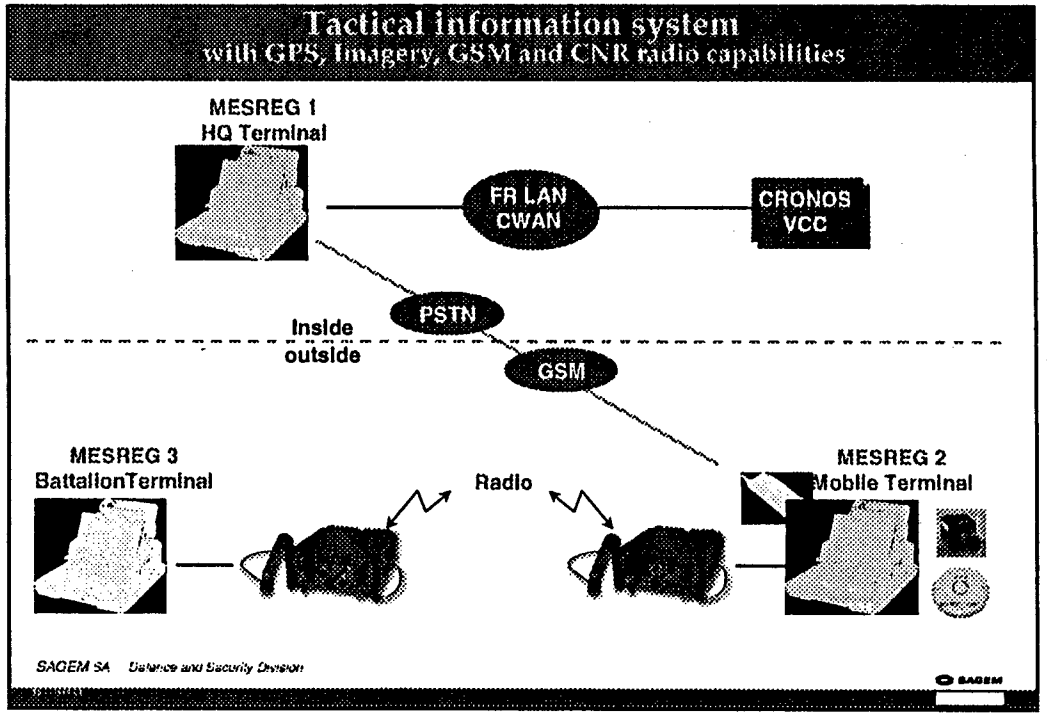
At the MESREG mobile terminal, operators will be able to:

- Capture the local tactical situation with a digital camera and a GPS receiver,
- Send encrypted messages of the tactical situation to the MESREG HQ terminal by a GSM radio link and the PSTN network,
- Send/receive encrypted data to/from the MESREG battalion terminal, by CNR radio.

At the MESREG battalion terminal, operators will be able to:

- Send/receive data to/from the MESREG mobile terminal, by CNR radios.

All MESREG terminals display the position of the mobile terminal on a map as well as images.



Collaborating Agencies/Industries

- SAGEM SA Defense and Security Division Secure System Department PARIS - LA DEFENSE

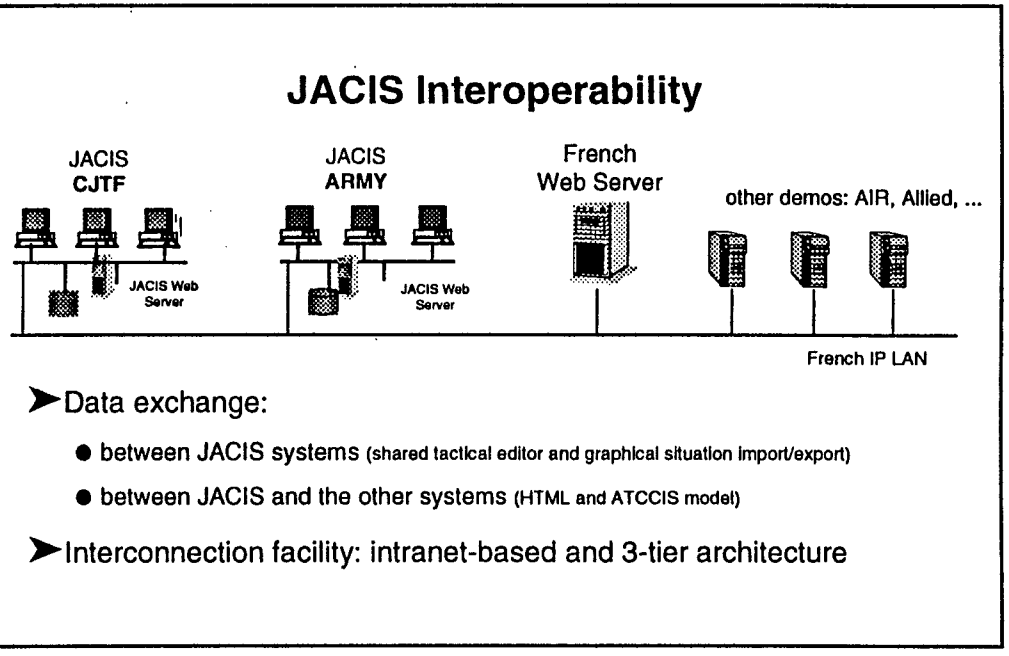
FRANCE-7

JACIS (JAVA-ENABLED AND ATCCIS-BASED CIS)

SPONSOR: THOMSON-CSF COMMUNICATIONS, France

Objectives

This technical demonstrator illustrates how new architectures coming from the Web and applied to CIS can improve their inter-operability and scalability. Being based on the ATCCIS data model, JACIS offers inter-operability at the raw data level. By using Web technology, JACIS enhances the inter-operability and scalability at the MMI level.



Description Overview

The purpose of the demo is to show how operators from different CISs can co-operate to come to an agreement regarding the Operational Picture (OP) their CIS have elaborated separately.

The demonstration will present 2 JACIS systems: one representing the Combined Joined Task Force situation and the other the Army situation. Tactical data from other CISs (by instance, Air CIS) will be read through their generated HTML pages.

JACIS systems can import tactical data from one to the other and inside one JACIS system operators can share the tactical editor for a workgroup session.

JACIS operators can browse through HTML pages generated by the other CISs. Furthermore, each JACIS system can generate the current situation in HTML format.

Being based on the ATCCIS data model, JACIS could potentially inter-operate with other ATCCIS-based CISs through the replication mechanism (which has already been proved).

Details of Project

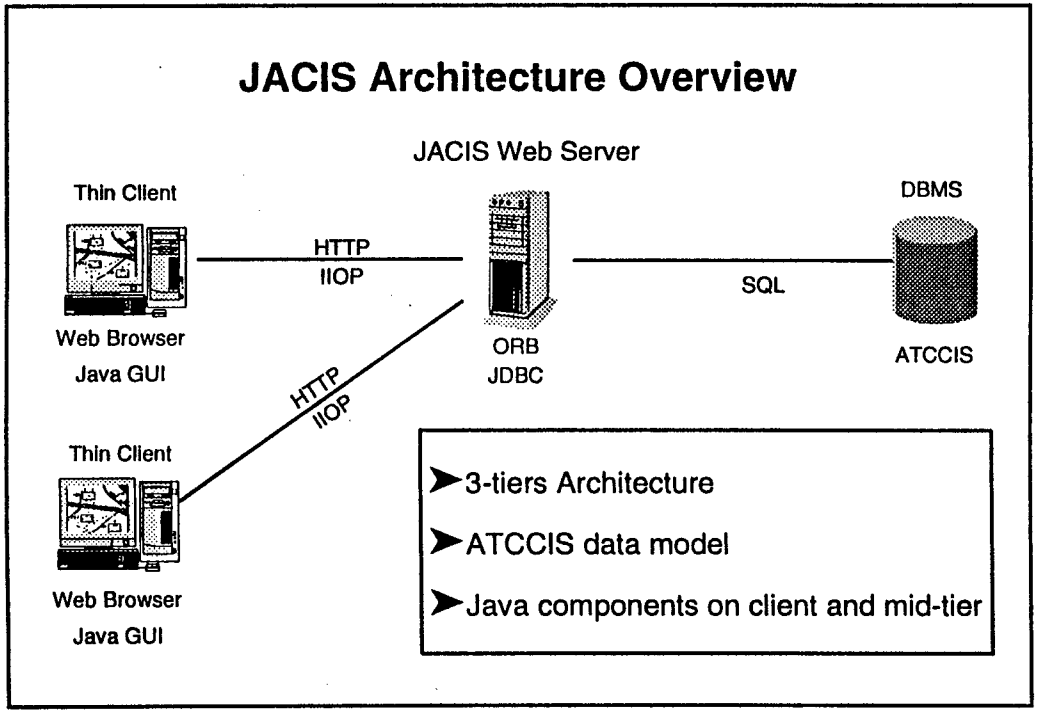
From a technical point of view:

- The architecture of JACIS is based on the 3-tier model: it relies on clients workstations downloading Java components from the Web server (also called mid-tier), where resides the business logic and the business objects extracted from the Situation DB (the basic tier). Object distribution across the tiers is based on the CORBA model concepts.

- A first particular feature of the solution consists in providing the OP together with a tactical (or situation) editor. This editor is entirely written in JAVA and can be downloaded through a Browser from the

Web server into the client operator workstations (which means zero-install of software on the client side). Raw data from the database are encapsulated by Business Objects on the mid-tier and are accessed by the client through HCI driven functions, allowing for consultation, modification, exportation and making it easier to inter-operate. The Data Model is the ATCCIS model.

➳ A second particular feature, called shared tactical editor, is that two operators can enter a cooperative working session to modify synchronously the tactical objects from the OP. Both have downloaded the JACIS tactical editor and as soon as one of them modifies a unit, the modification appears on the other screen as well as in the database. In addition, they can see and hear each other through a video-conferencing mechanism.



Collaborating Agencies/Industries

NACOSA-1

NACOSA VAT (VULNERABILITY ANALYSIS TEAM) CAPABILITY FOR DEFENSIVE INFORMATION WARFARE

SPONSORS: ACE COMSEC / COMPUSEC NACOSA

Objectives

To demonstrate Defensive Information Warfare capabilities in protection of NATO Networks.

Description Overview

Various Security Software Tools will be installed on dedicated hardware for use by a NACOSA INFOSEC Team. The Team will attempt to identify security weaknesses of SHAPE JWID98 assets and introduce countermeasures prior to start of JWID98. During JWID98, the NACOSA INFOSEC Team will monitor, detect and prevent any Offensive Information Warfare attacks which could be demonstrated by other JWID98 VA Teams.

Anticipated Results

NACOSA VAT will coordinate and work, as required, with the other JWID VATs participating in JWID98. When requested by a JWID98 participant, NACOSA VAT demonstrates Offensive Information Warfare on that host's installations for JWID98.

Collaborating Agencies/Industries

- Other NATO JWID-98 participants

NACOSA 2

JDIICS-D IN THE NATO AND COALITION ENVIRONMENT

SPONSOR: NATO CIS OPERATING AND SUPPORT AGENCY (NACOSA)

Objectives

This demonstration entertains one basic assumption:

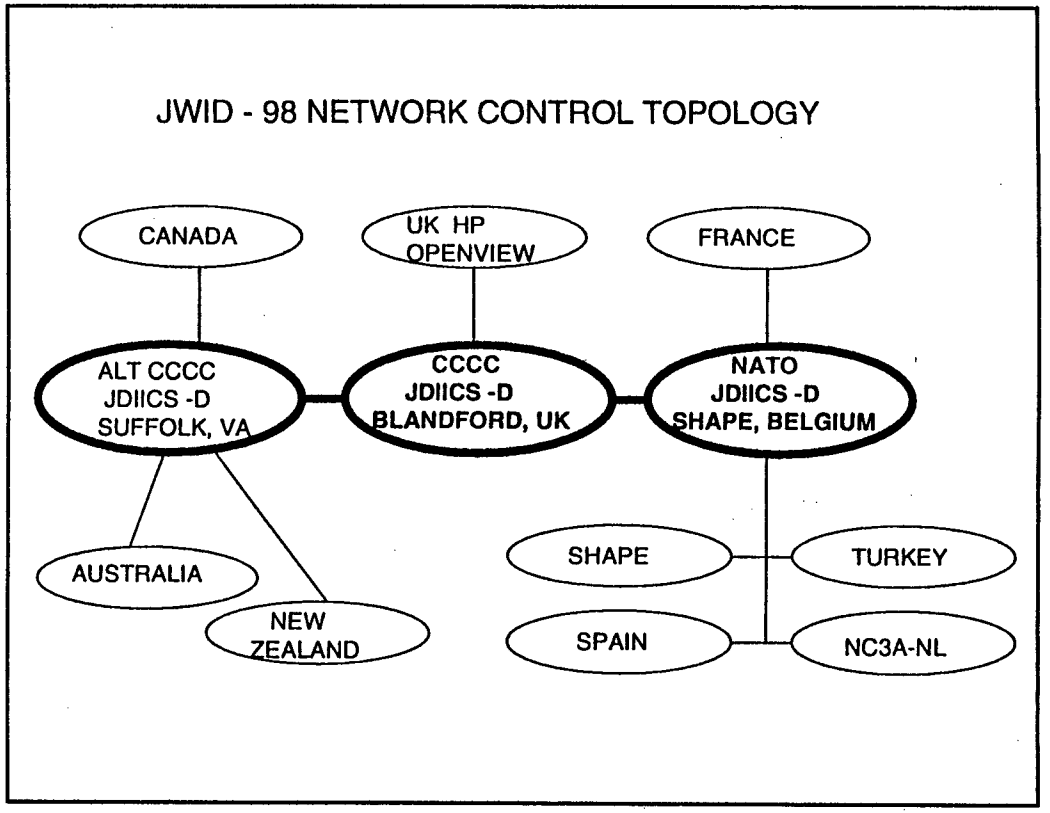
> In a coalition environment, both NATO Military Commanders as well as commanders of coalition partners undeniably require information on the health and welfare of command and control communication systems as an integral ingredient of the decision-making process.

This demonstration seeks to investigate modern tools that allow digital networks to be appropriately managed and controlled, and which provide the coalition commanders with the pulse of the coalition networks dedicated to command and control.

Description Overview

Unlike the other JWID-98 demonstrations, this demonstration is fully functional. In addition to being a JWID-98 demonstration site, the suite of hardware and software used in this demonstration is collaterally used to manage and control the JWID-98 networks. The JWID-98 networks are managed and controlled by three, interconnected and interactive network control centres:

- The Coalition Communications Control Cell (CCCC) located at the Headquarters Joint Task Force, Blandford Camp, UK
- The Alternate CCCC located at the Joint Battle Center (JBC), Suffolk, Virginia, USA
- The SHAPE Command Centre (SCC) located in Casteau, Belgium



The equipment, software, and procedures were put into place to allow the three control centres to each manage their own domains, yet share information regarding the state of those domains to each other in near real time.

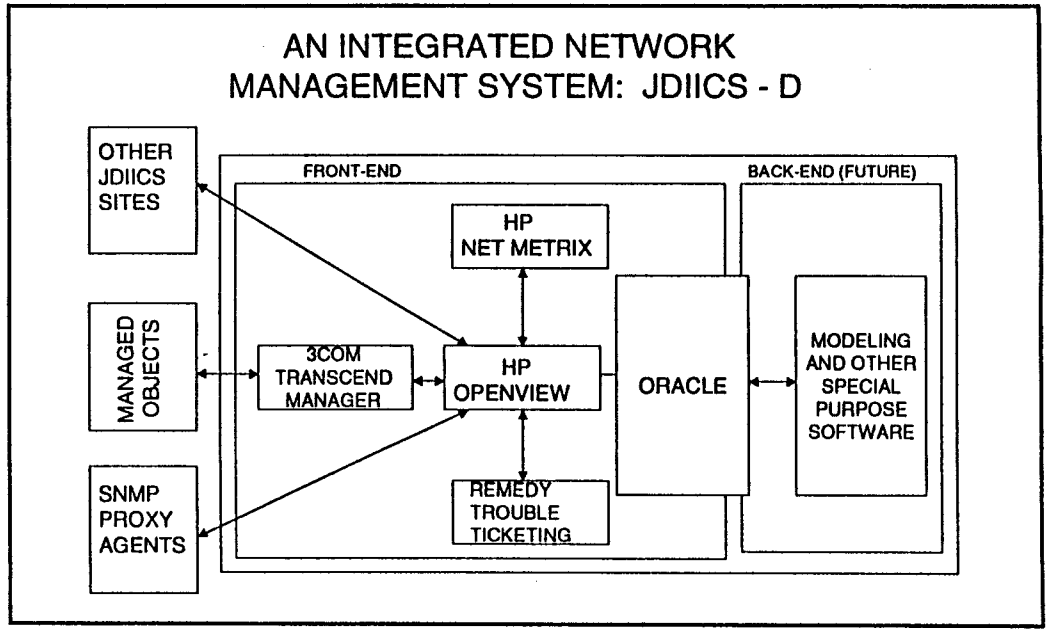
Details of Project

A dedicated and extraordinarily powerful Sun SPARC-20 is loaded with entirely Commercially-Off-The -Shelf (COTS) software. The foundation of the software suite is HP Openview, and specifically, an unmodified Version 5.0; it is configured to report the status of NATO digital networks using essentially Simple Network Management Protocols (SNMP). The HP Openview is further configured to acknowledge a partner or sibling relationship with both the CCCC and the Alternate CCCC. Using software filters, a feature of HP Openview, update to the picture of the current NATO network status also resides at the other two sites.

The ability to react to detected network faults and to have installed a fault management system is provided by both an Oracle Database, and the Remedy Action Request Trouble Ticket system. While all three network control centres manage their respective faults, the Remedy Trouble Ticketing System is configured at all sites to permit a coalition fault management structure to be established. Such a configuration thereby allows a view of the current status of outages, the reason for outages, and the current action being taken to restore service.

Digital networks rely on routers to act as switches and routing devices. The majority of routers in NATO are 3COM. The US, however, uses primarily CISCO Corporation routers. The JDIICS-D suite allows for NATO to use the 3COM Transcend Enterprise Manager as its configuration and management tool, while allowing the US to manage its fleet of CISCO routers with "CISCO Works." Each management tool employs fundamentally SNMP protocols with additional vendor-provided value added tools. Nevertheless, SNMP protocols provide the foundation for router management and control information.

The JDIICS-D suite allows other software suites to be incorporated. The US, for example, also integrates GCCS, TNAPS, and its own satellite management package to form a part of the JDIICS-D suite.



Anticipated Results

Based on exploitation of the US JDIICS-D, NACOSA will:

- Effectively manage JWID-98 NATO digital networks with COTS
- Demonstrate the value of realizing a coalition-wide, near real time picture and status of coalition CIS

Collaborating Agencies/Industries

- NATO C3 Agency - The Hague
- United States Defense C3 Field Office-Brussels
- The United States Defense Information Systems Agency
- The MITRE Organization, Reston, Virginia, USA

SHAPE-1:

VIRTUAL COMMAND CENTER (VCC)

SPONSOR: CIS-ISB, SHAPE & NATO C3 AGENCY, DEN HAAG

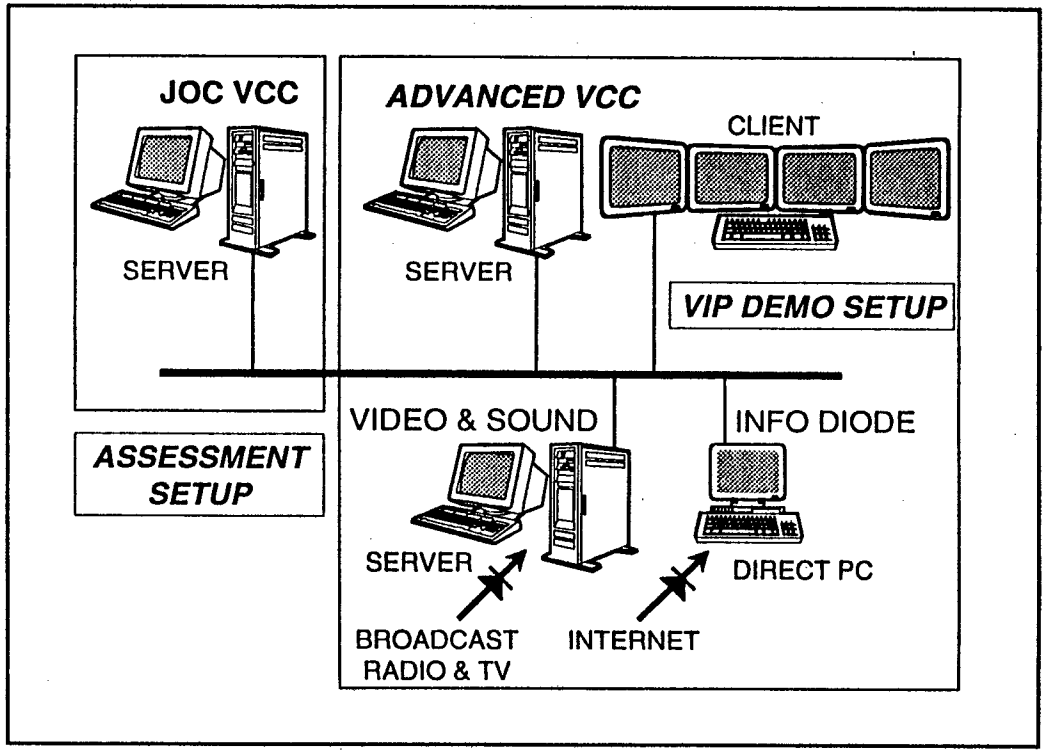
Objectives:
Integration of NATO and Allied Systems.
Exploitation of multi-media products by integrating internal and external demos.
Use of Simple Publication Procedures and Directory Management Services to support Information Access through Web Page Publication.

The Virtual Command Centre (VCC) demonstrations provides a web based Information and Command Center integrated into a single PC, with access to a full range of information sources utilizing a common user interface, supported by user navigation and information access management tools. The use of web technology allows the VCC to simplify user procedures, user training requirements and interoperability between JWID demonstrations and information systems.

The JWID-98 Virtual Command Center (VCC) demonstration incorporates lessons learned in JWID-97 and extends the VCC capabilities to include VTC via the CWAN as part of Collaborative Planning Tools, use of Open Source information from broadcast Radio & TV and the Internet together with extensive use of Web Technology applications. The primary objective of the VCC is to establish an integrated information center that supports command and control functions. Additionally, the VCC exploits the use of web technology to support systems interoperability regardless of hardware platform, operating system or application software.

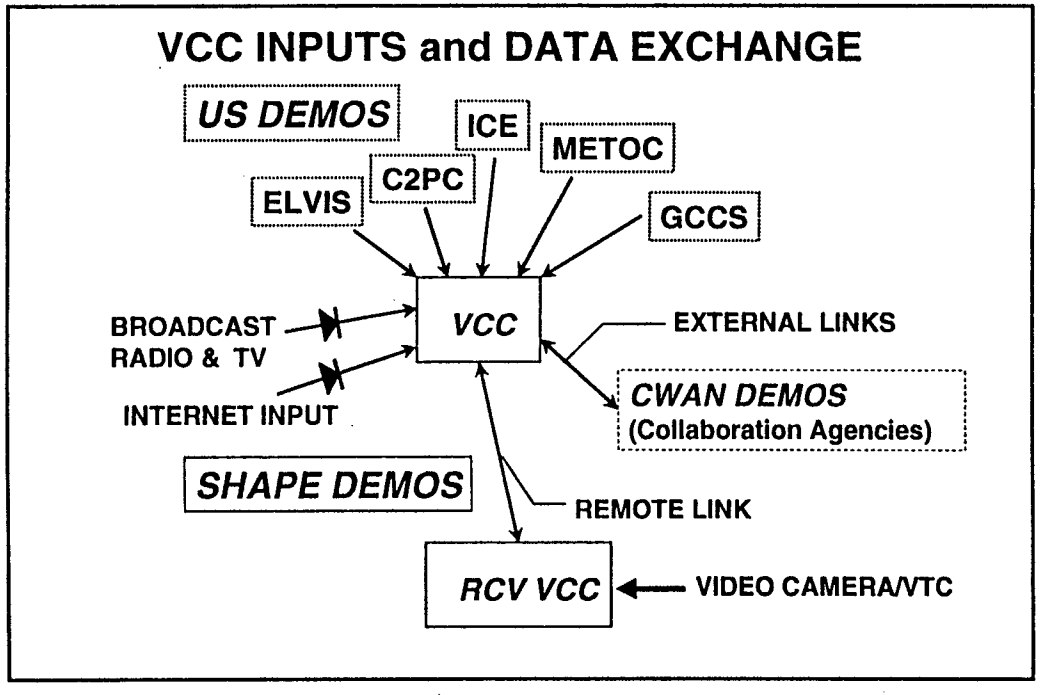
A secondary objective of the VCC is to provide an automated web based publishing tool that supports other demonstrations as part of the NATO infrastructure. In this capacity, the VCC allows all users to use web technology effectively for information collection and dissemination between demonstrations of US, the European partners and NATO organizations.

Description Overview
The VCC demonstration showcases two prototypes. The first called the "JOC VCC" is a copy of the VCC being tested by the SHAPE Joint Operations Center (JOC) as part of the Cronos network. This VCC prototype will be assessed as part of the JWID-98 VCC test plan and the results will be incorporated as part of the JOC VCC trial in the Cronos network. Principally, the "JOC VCC" is a prototype tested under operational conditions at SHAPE JOC.



The second prototype is called the "Advanced VCC" as shown in figure 1. This prototype intends to explore technologies identified as part of the VCC concept but not yet implemented in the "JOC VCC" operational prototype. This version of the VCC will undergo test and assessment to validate future VCC applications contained in the VCC Concept Plan and to provide analytical measurements of performance. The "Advanced VCC" will explore capabilities that include VTC via the CWAN, collaborative tools, broadcast radio & TV and open source inputs to the VCC, Public broadcast and Internet feeds to the VCC and general multimedia and web technology applications.

Finally, since the Roving Command Vehicle (RCV) also contains a VCC on board of a specially equipped mobile platform (Land Rover), JWID-98 will provide the opportunity to connect the two VCC together and exchange data and hold a VTC session via the CWAN connection. The RCV will be located in Blandford



Camp, UK and the base VCC in the SHAPE Bunker, Belgium. Typical data exchanges utilizing the VCC are shown in figure 2.

Anticated Results:
Anticipated results are divided into the following sub-groups:

JOC VCC:

- Performance measurements and validation of the VCC under normal users operational environment
- Validation of operational procedures and training requirements.
- Measurement of bandwidth requirements and security compliance.
- Ease of use and adaptability of the VCC to changing operational scenarios
- Validation of the User Publishing tool and users performance review

Advanced VCC:

- Validation of Technical feasibility for integrating Open Sources, Internet and other sources in the CWAN
- Technical review of the integration between the RCV, the JOC VCC and the Advance VCC
- Exploration of new technology as applied to Command and Control functions
- Measurement of bandwidth requirements to support the new VCC technology
- Security review using the CVAT effort

Roving Command Vehicle (RCV) Interface:

- Technical review of the VTC connections between UK and Shape bunker using the CWAN
- Technical and security review of the data exchange between two VCC (one remote one local)
- Continue technical review of the various VCC configurations (fixed, mobile, others)

Collaborating Agencies

- Communications & Information Systems Division, SHAPE
- NATO C3 AGENCY, Den Haag

SPAIN-1

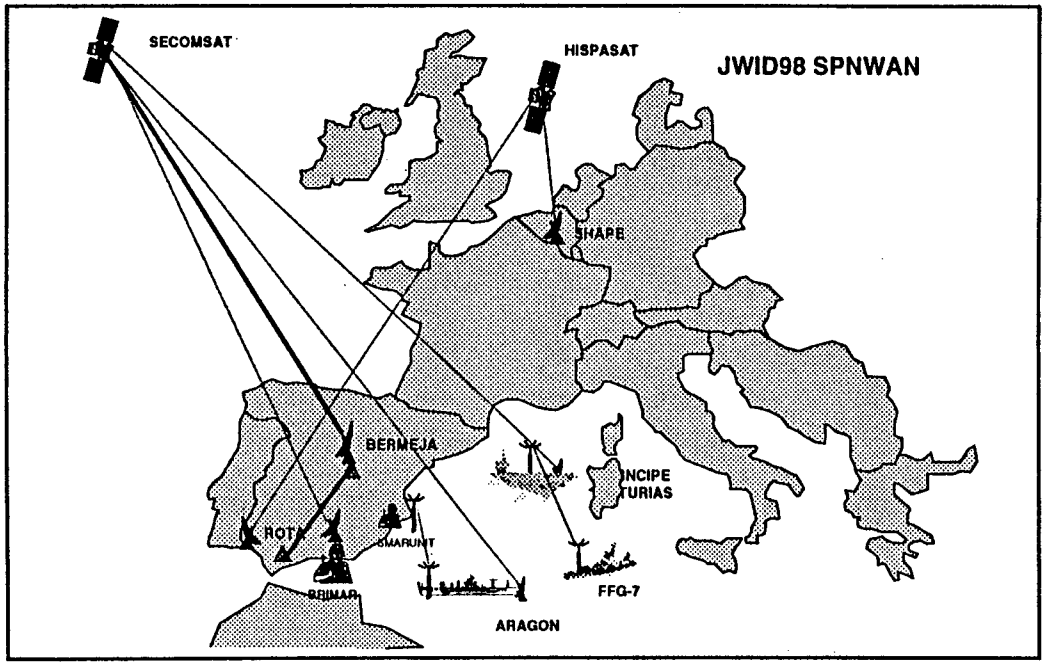
C2IS & MIS WEB SYSTEM - WEBCOP

SPONSOR: SPANISH NAVY AND ISDEFE.

Objectives

WebCOP is a technology concept designed to provide the military commands with all the required C2IS & MIS capability in complex multinational environment by using an Intranet based WAN and Web sole user interface.

Web Architecture supports Common Operational Picture - COP, Geographical Information System -GIS- and Message Handling System -MHS-. By using commercial LAN PCs connected by a secure telecommunication networks to the IP routers, the operational user can deploy and achieve very high performance C4I capability at a fraction of the present cost.



Description Overview

WebCOP System architecture include:

- Automated RDBMS replica.
- JAVA Applets. Functional Interface.
- GroupWare/Workflow.

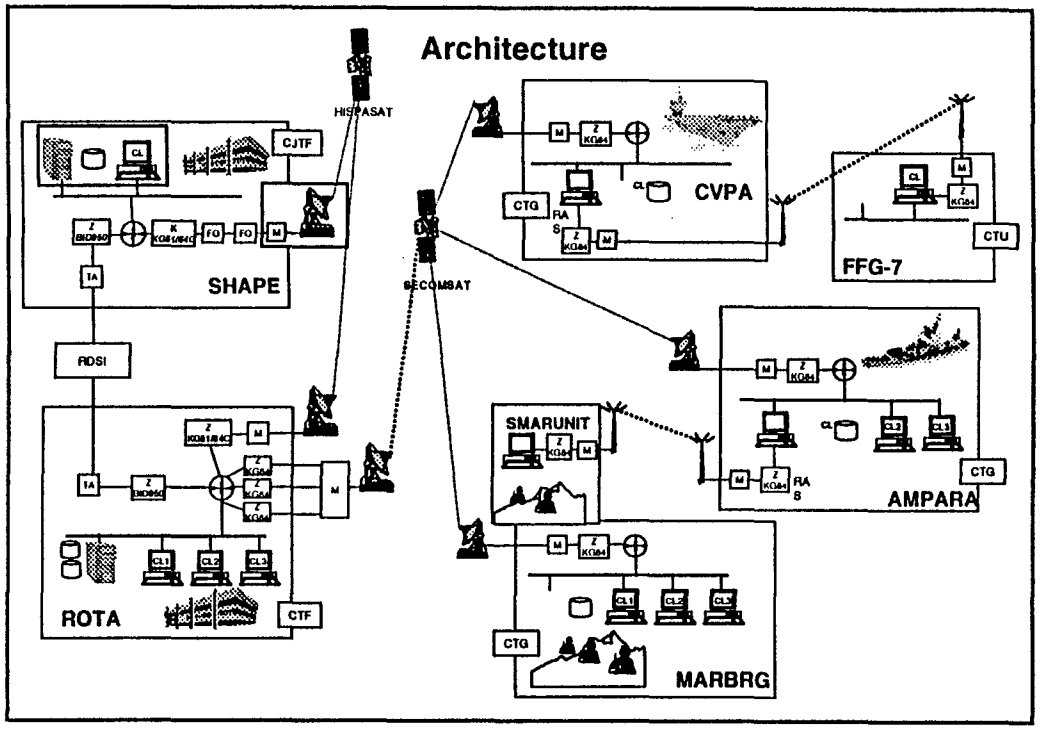
In addition to the global web architecture concept, the technical and operational feasibility of three major elements will be demonstrated:

- TCP/IP radio channels providing WAN connectivity to remote unit Command Post.
- Real time data integration from a Link11/Link14 source.
- Automatic formatted message integration (OTH-G).

Compatibility of all these elements with the Web architecture will extend the application of the WebCOP technology from the NCA strategic level to the C2 requirement of the TU.

WebCOP demonstration is deployed in five major locations: SHAPE Bunker (CJTF), SP Navy Fleet HQ in Rota (CTF), SP Navy Alpha Group Carrier PDA (CTG), SP Navy ARG Flagship - ARAGON (CTF-CATF), SP Navy Marine Brigade Command Post (CTG-CLF). Two radio connections for two CTUs size units will connected a FFG-7 class ship and a Marine Battalion Command Post.

Spanish National JWID WAN will be connected to the CWAN by a secure low cost commercial SATCOM link. System Performance and availability will be demonstrated.



Anticipated Results

JWID98 WebCOP demonstration will show how an actual Amphibious Land Force C2 deployment can be accomplished, with dynamic IP-routing reconfiguration maintaining the system integrity during all the phases of an amphibious assault.

Collaborating Agencies/Industries

- Retevisión
- Oracle
- Digital.

TURKEY-1

RADIO BASED MESSAGE TRANMISSION SYSTEM (OTEMAS)

SPONSOR: TURKISH GENERAL STAFF (TGS)

Oblectives

- Integration of e-mail and formatted messages
- Joining National Systems to CRONOS and the VCC
- Demonstration of e-mail and formatted message exchange over HF links

In this demonstration, the possibility of integration to NATO system over HF communication links will be illustrated. The demonstration will provide rapid connectivity in cases where NATO forces deploy to the field and no static communication infrastructure is available.

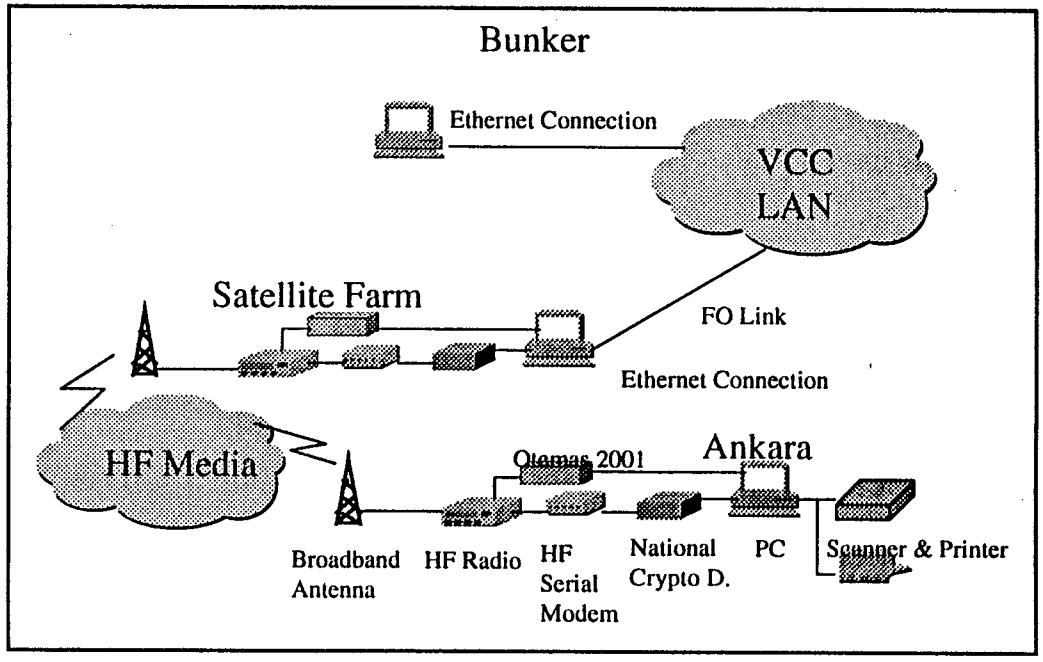
Description Overview

In the demonstration, publishing HTML and MS Office product documents in VCC will be demonstrated.

In addition, the possibility of publishing e-mail messages with attachments to VCC will be shown. The demo also includes inter-operability tests with other demos.

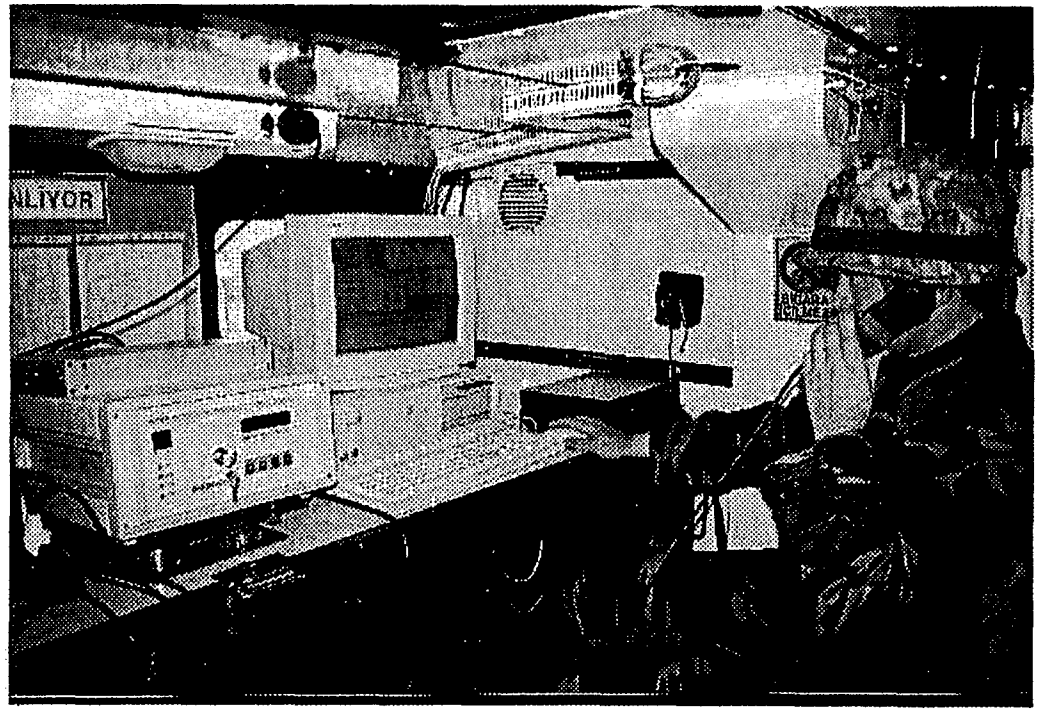
Regarding the communication, the difficulties involved in HF Radio communication and HF Radio communication device operations are addressed, and the ability to establish automatic link between HF terminals without user intervention is demonstrated.

About the topology, the OTEMAS terminal in Ankara is linked to VCC through a HF Radio and controlling terminal situated in the SATFARM. The connection to VCC is enabled by a V.35 router located in the bunker.



Since publishing in VCC can be done in several ways, the demonstration also shows the ability of OTEMAS to handle e-mail and remote file operation capability which is necessary for seamless integration to the VCC.

The OTEMAS ability to act as a transparent link between terminals having HF links for the commercially of the shelf products will also be illustrated. In other words, any POP3 and SMTP compatible client such as Microsoft Mail or Netscape Messenger can be used to exchange e-mail messages with attachments using the transparent link provided by OTEMAS.



Anticipated Results

The important outcome expected from the demo is the recognition of seamless integration to VCC via OTEMAS HF links. Another important issue covered is interoperation of commercially off-the-shelf messaging products with OTEMAS.

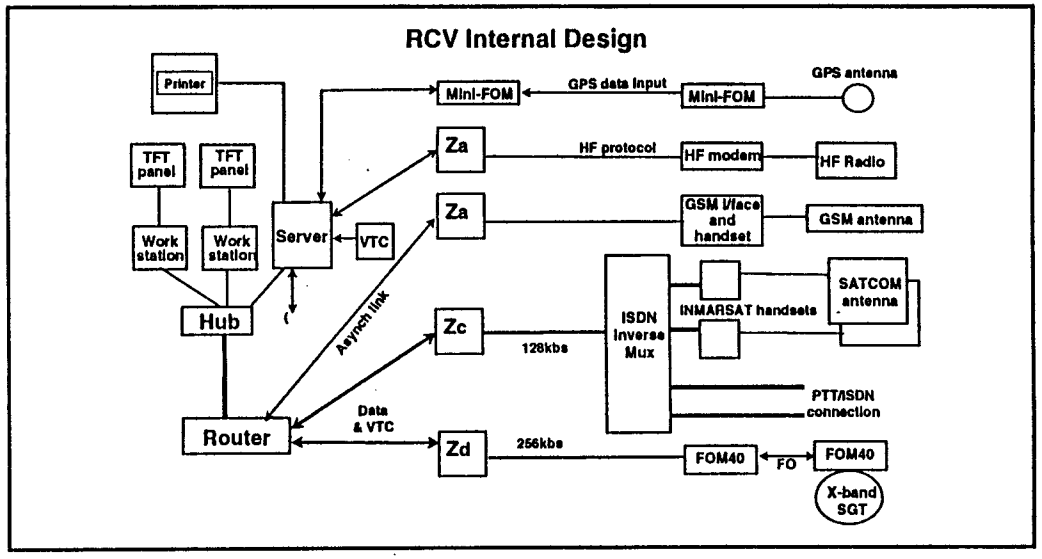
Collaborating Agencies/Industries

- TGS
- INTER
- French, Spanish and UK demonstrations

NC3A-1
THE ROVING COMMAND VEHICLE
SPONSOR: NC3A, DEN HAGUE

Objectives
To illustrate a revised implementation of the concept of a high-mobility vehicle providing CIS facilities to serve the needs of NATO commanders.

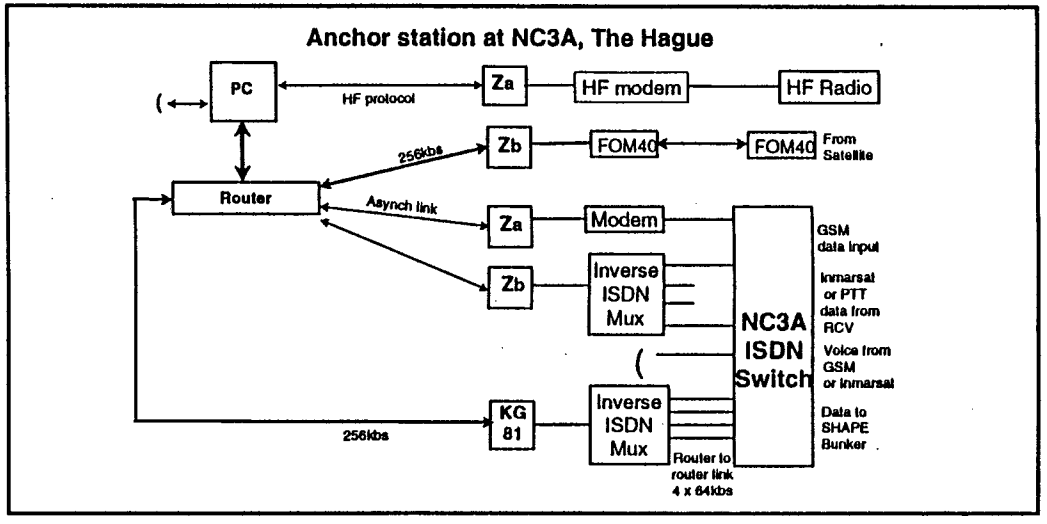
Demonstration Overview
This exhibit demonstrates one possible implementation of a Roving Command Vehicle (RCV). The RCV provides facilities to such commanders to maintain effective command when working remote from their principal headquarters, and therefore detached from the bulk of their staff. The normal channels of communication for information and data updates can be extended forwards to the point at which the commander is working in roving mode.



The RCV also provides facilities for use as a highly effective information-gathering capability, and for relaying such information back to its parent headquarters (or any other location, if so required) in real-time. This capability will provide the commander or the command group with an on-the-spot picture of events as they are unfolding.

The demonstration consists of an "off-the-shelf" commercial high-mobility vehicle fitted with CIS assets, consisting of information systems, encryption devices and multiple communications systems to provide the maximum possible bandwidth under different operating conditions.

The present equipment fit and the facilities provided have been refined from the initial implementation shown at JWID-97 as a result of feedback from visitors, as well as the demonstration team's own experiences. Two major developments of the 1998 version when compared to the 1997 version are the significantly improved layout of the user facilities within the vehicle, and the use of an Anchor Station to terminate all communications links, thus eliminating the need for local engineering to host the RCV.



Details of Project

1. Vehicle.

The vehicle is a standard commercial Land Rover with the addition of a high roof and roof rack (both standard catalogue items) and the provision of an auxiliary alternator and control system, another Commercial-off-the-Shelf (COTS) item. The alternator provides a 220V ac supply using the main engine as a power source, for use if the vehicle is in motion, or if it is not possible to pick up a power source from a site facility when stationary.

The stripping of the original internal fittings of the vehicle, and the installation of new fittings, were carried out in the workshops of the NATO C3 Agency in The Hague. Swiveling chairs provide both a working and a travelling position for two people. Access to the working position is through the back door; the side rear doors are blocked off for personnel, but provide access to the racks and equipment.

2. IS facilities

- The facilities provided are fourfold: data system, video teleconferencing, voice, and public media.

- The data system consists of two workstations and a server, mounted in a desk fitted centrally across the middle of the vehicle, together with a printer for low-volume output. The systems are connected by a LAN within the vehicle, and from that LAN, via a router and the communications assets, to the Anchor Station at NC3A in The Netherlands. The facilities provided at the workstations are similar to those provided for the Virtual Command Centre in the SHAPE bunker. The server and workstations run Windows NT4 operating system, with a range of standard COTS products to provide the main functionality. Most of the data made available at the workstations comes through the medium of a web browser, but e-mail is also available. The use of a web browser maximizes the number of other JWID sites that can be accessed for information. The whole data system is secured by encryption on the communications links.

- Video teleconferencing capability is provided for use in stationary locations where sufficient bandwidth can be made available. This too is a secure facility.

- Several alternative voice circuits are provided, including secure voice through VTC system. When stationary, access to the worldwide PTT system (insecure) is available through Inmarsat. The GSM system provides for PTT access (insecure) when in range of a cell of the local GSM service provider, both static and on the move.

- Public media information services include the reception of broadcast radio and a satellite receiver for video channels

3. Encryption facilities.

The RCV is designed to use miniature KIV-7 units to provide encryption of all data leaving the vehicle. An insecure voice capability is also provided, as described below.

4. Communications capabilities.

Four different communications means are provided for the RCV:

1) A satellite communication capability making use of NATO X-band satellite capacity to provide a bandwidth of 256 KBPS.

2) A satellite communication capability making use of commercial Inmarsat satellite capacity, using two channels to provide a bandwidth of 128 KBPS. This link also provides insecure voice capabilities.

3) A low-speed data circuit over cellular radio, using commercial GSM equipment; this channel can also provide an insecure voice capability.

4) Very low-speed file transfer and e-mail over a HF radio link. This link also provides insecure voice capabilities.

Collaborating Agencies/Industries

- Other NATO JWID 98 Demonstrations
- SHAPE Virtual Command Center

NL-1

SOLDIER DIGITAL ASSISTANT (SDA)

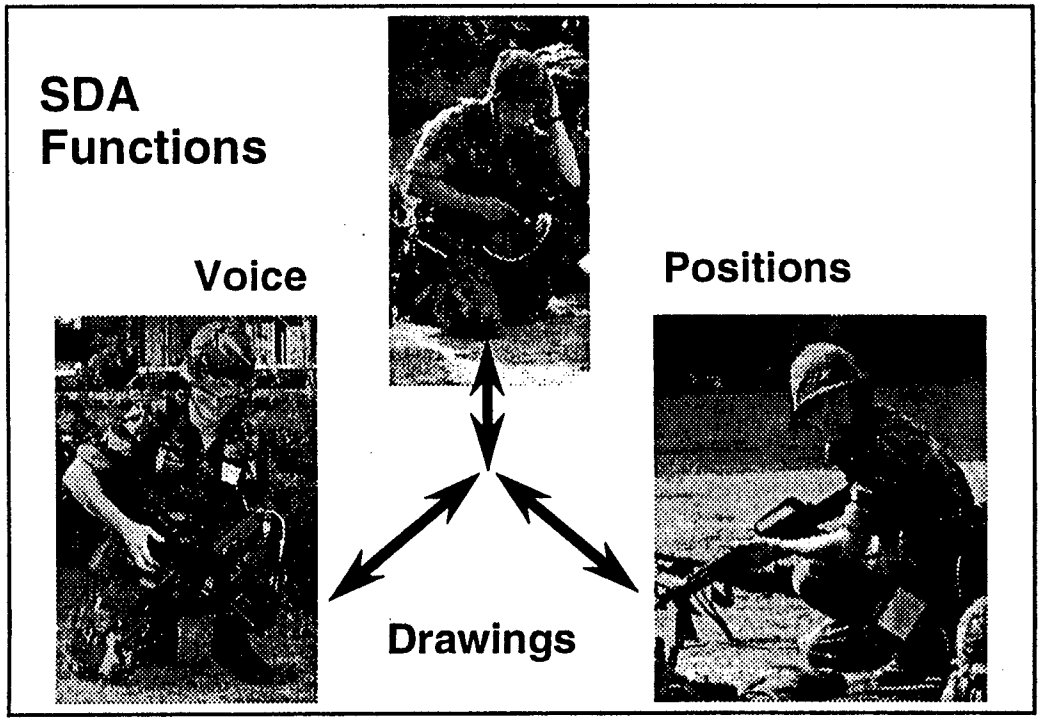
SPONSOR: TNO - PHYSICS AND ELECTRONICS LABORATORY, THE HAGUE

Objectives

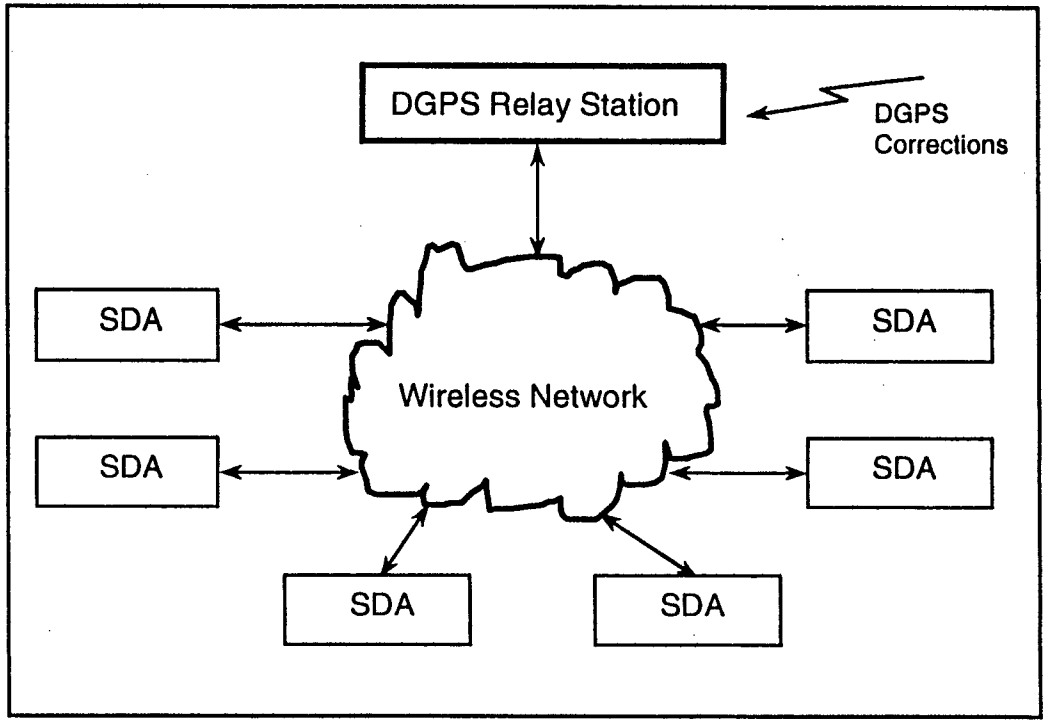
Demonstration of a portable C2 system for the Combat Soldier. The SDA will result in improved C2 capabilities of the soldier and provide him with a better situational awareness.

Description Overview

The SDA provide the combat soldiers with the ability to exchange positions, drawings and speech which results in a rich flavor of communication capabilities (figure below).



The SDA is implemented using COTS products. The figure below provides an architecture overview of the SDA system.



Anticipated Results

For JWID '98 no specific results are anticipated. The SDA is presented in JWID '98 as a stand-alone system. It is a demonstration of new developments on the soldier level. In future demonstrations the SDA is a candidate to become part of the integrated JWID demonstration.

A.2 Brochure van 'MESREG'

MESREG

Regimental message handling system

SAGEM

The right way to handle your message

MESREG est un système de messagerie militaire de niveau régiment. Il facilite l'exercice du commandement en automatisant l'échange de messages au sein des forces projetées.

Cette messagerie est capable d'utiliser tous les moyens de communications disponibles en opérations :
- réseau local (ethernet)
- réseau radio HF et VHF numérique et analogique
- liaisons satellitaires
- réseaux téléphoniques commutés
- reseau GSM.

La combinaison de liaisons à courte et longue portées offre une grande souplesse de déploiement.

La sécurité est assurée par la carte DCS 4000, module de chiffrement extractible au standard PC Card. Les services offerts sont la confidentialité et l'intégrité du contenu des messages.

Une fonction cartographique couplée à un récepteur GPS permet de localiser la station en temps-reel.

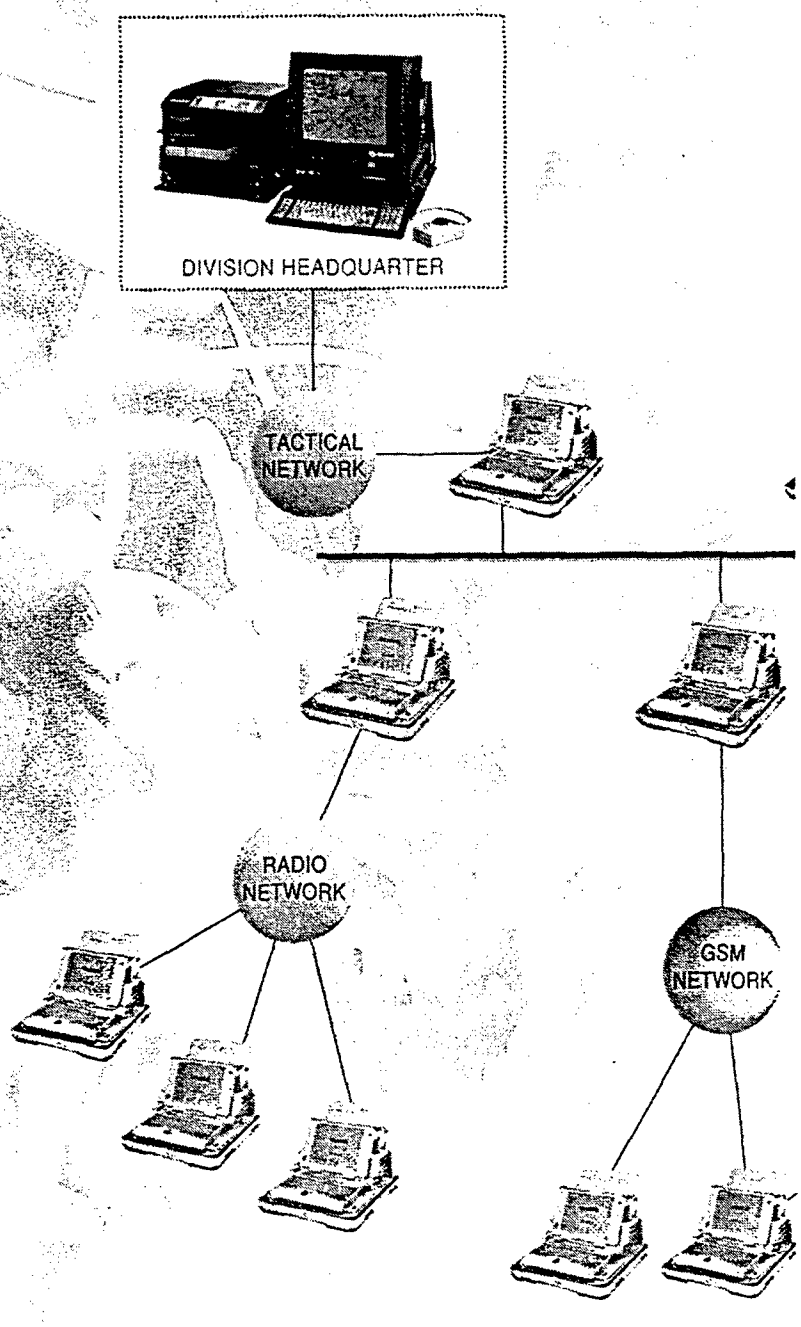
Le poste de commandement du régiment rassemble les stations directrices de sous-réseaux radio et les stations le reliant aux autres régiments et aux échelons hiérarchiques supérieurs.

Les messages sont de types formels ADatP 3 (messageries interarmes, génie, logistique) ou informels (textes, dessins, télécopies, fichiers informatiques).

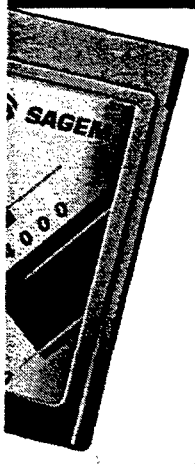
Le routage des messages est entièrement automatique. Il se fait de proche en proche, en mode point-à-point ou diffusion, avec ou sans accusé de réception.

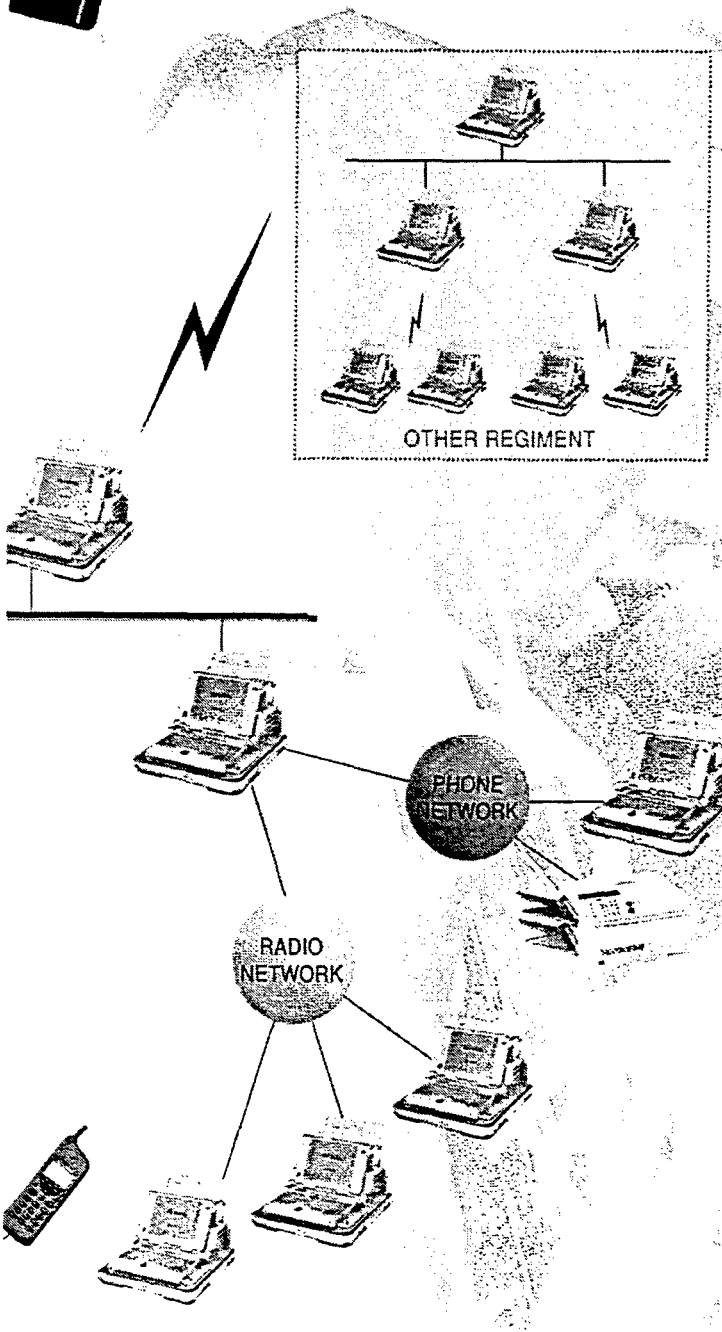
Toutes les stations du réseau sont banalisées et servent de commutateur de messages et de terminal d'abonné.

*Adopté par l'Armée française



s throughout the field of operations*





MESREG is a regiment-level message handling system. It will ease command and control by automating message handling within projected forces.

This message handling system is able to use all available links in operational contexts :

- local net (Ethernet)
- digital or analog HF or VHF radio nets
- satellite links
- switched telephone network
- mobile phone network.

Short and long range combined links give flexibility to the deployment.

A PC card ciphering unit, the DCS 4000 provides security: confidentiality and integrity of the message content.

An integrated digital map coupled with a GPS receiver is available to localize the station in real-time.

The battalion main post integrates the radio undernets and stations providing a link to the other battalions and up to the chain of command.

Messages are either of the ADatP3 formal type (message handling for combined forces, Engineer corps or Logistics) or informal (texts, drawings, faxes, data files).

Message routing is completely automatic. It is performed station-to-station or by broadcasting with or without acknowledgment.

All stations are unmarked and can be used both as a message switchboard and as a terminal.

*Adopted by the French Army

M E S R E G

CARACTERISTIQUES TECHNIQUES

• Système d'exploitation
-DOS*, Windows NT*

• Progiciels
-Pack office pro*
-Windows draw*

• Applications
-Messagerie ADatP3
-Messagerie libre
-Agent X400
-Télécopie
-Administration

• Communications
-Ethernet*
TCP/IP* , NFS*
Windows for workgroup*
-Radio
protocole FED STD 1052
CCE :Reed Solomon, convolution
TEB toléré meilleur que 0.2
port synchrone numérique 16 kb/s
port modem BPSK 1800 b/s
- Débit VHF (analogique) : 1800 b/s
- Débit HF : 75, 150, 225, 300 b/s
-Réseau téléphonique
télécopie groupe III avec ECM
9600 b/s avec repli jusqu'à 2400 b/s
- Réseau GSM 4800 b/s et 9600 b/s
-Ports V24 jusqu'à 19200 b/s

• Cartographie
- échelles : 50 000 à 5 000 000
- 1 000 km x 1 000 km

• Alimentation
-AC : 230 V, 50Hz
-DC : 24V véhicule

•Environnement
-Climatique 0° à 40° C
-Mécanique 25 G, 11ms
-Electomagnétique NFC 98020

Encombrement
-L xP x H : 380 x 450 x 190 mm
-Poids : 12,5 kg

* Marques deposées

Adopté par l'Armée française

TECHNICAL CHARACTERISTICS

• Operating system
-DOS, Windows NT**

• Softwares
*-Pack office pro**
*-Windows draw**

• Applications
-ADatP3
-Mail
-X400 UA
-Facsimile
-Administration

•Communications
*-Ethernet**
TCP/IP, NFS**
*Windows for workgroup**
-Radio
protocol FED STD 1052
ECC : Reed Solomon, convolution
max. BER better than 0.2
digital synchronous port : 16 kb/s
BPSK modem : 1800 b/s
- Rates: 1800 b/s VHF analog.
75, 150, 225, 300 b/s HF
-Telephone network
group III facsimile with ECM
9600 b/s with fall back to 2400 b/s
- Mobile phone network 4800 b/s and 9600 b/s
-RS 232 ports up to 19200 b/s

• Digital map
- Scales from 50 000 to 5 000 000
- 1 000 km x 1 000 km

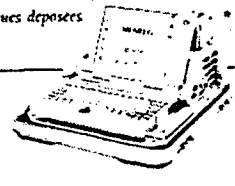
• Power supply
-AC : 230 V, 50 Hz
-DC : 24V vehicle

• Environment
-Climatic : 0° to 40° C
-Shocks : 25 g, 11ms
-EMC : EN 98020

• Physical
-W x D x H : 380 x 450 x 190 mm
-Weight : 12.5 kg

* *Trade marks*

Adopted by the French Army

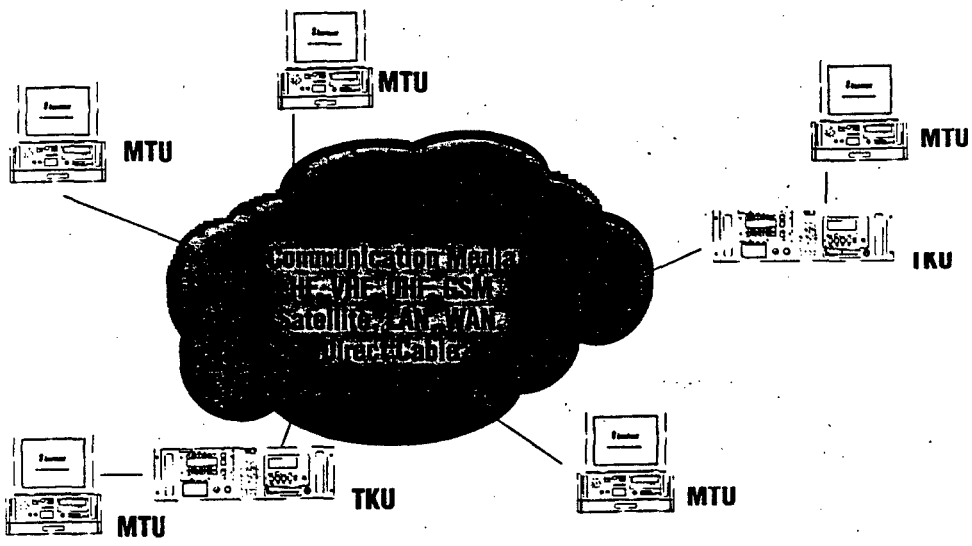


SAGEM SA
Defence and Security Division
PARIS - LA DEFENSE
61, rue Salvador Allende
92751 Nanterre Cedex - FRANCE
Phone: (33).40.70.63.63 - Fax: (33).1.40.70.68.68
http://www.sagem.com

SAGEM

Printed in France - Photos ECPA/SAGEM - Not contractual subject to change without notice - SIC/DIDS/2V/FE-12/97

A.3 Brochure van 'OTEMAS'



OTEMAS 2A

Automatic Message Handling System

OTEMAS is a Message Handling System designed for data and voice transmission over the various communication media. OTEMAS system uses MTU-2002 Message Terminal Unit and/or COTS (Commercial Of The Shelf) Personal Computers. MTU-2002 unit is the base hardware of the system supporting most demanding security and reliability issues. Low cost COTS computers can also be used to decrease the system hardware cost. TKU-2002A Radio Equipment Control Unit is used to communicate through HF, VHF and UHF channels.

By using MTU and TKU pair on wireless media, message generating and analyzing division is separated from the wireless Equipment Park. In this configuration all the data going to TKU is encrypted.

Key Points

- X.400 Compliant Message Handling
- Communication with ACP 127 Terminals
- Internet e-mail Sending, Accepting and Passing over
- NATO STANAG 5066 HF Communication Protocol
- Point-to-Multi-point Communications in HF Media
- Secure Communications
- Reliable Communications
- Key Distribution
- Digital Signature
- User Authentication
- User Friently

Communication Media

- HF, VHF and UHF
- PSTN
- GSM
- Satellite
- LAN/WAN Connectivity
- Direct Cable connection

FEATURES

User

- Easy and automated Use
- Message operations
- Routing operations
- Compression Functions
- Encryption Functions
- Printing functions
- Scanner Operations
- Authentication Management with
- Authentication Management wit
- On Line Help
- Tutorial

Database

- Secure database
- Automatic Secure Message
- Automatic Statistics Archiving
- Automatic Illegal Operations L
- Automatic Comm. Channel Qua
- Special Critical Memory

Automatic Peripheral Control

- Control of wireless equipm
- Control of Security Equipm and
- Control of TKU-2002A
- Control of MTU-2002

HF Communication

- No need to dedicated HF o
- ALE (Automatic Link Estab
- Frequency Management
- Passive Channel Quality An
- Active Channel Quality Ana
- Active Propagation Quality
- Automated control of wire equipment
- Suitable for Frequency Hopping (Anti Jam) operation
- STANAG 5066 compliant HF protocol
- Point to Point communication
- Point to Multi-point communication
- Full Duplex Comm emulation

Message Handling

- X400 compliant Message Handling Structure
- Secure Communication
- Reliable Communication
- Urgency Level Management

Security

- ine Crypto
- line Crypto
- Sec Level Management
- nana ent
- affi ecurity
- Di gnature

Voi mmu ation

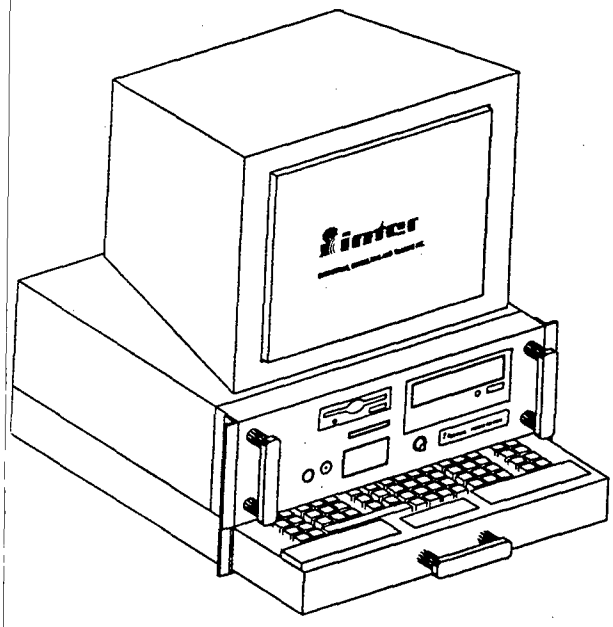
- Di Secur oice
- C10
- CELP 6

mmu ation Channels and Media

- HF, VH UHF
- PST (Public Switched Telephone Network)
- Le ed Line
- N/WAN
- ternet
- orld ide Web
- GSM
- Satelli Teleph ne

THE MANUFACTURER HAS A POLICY OF CONTINUOUS AMPROVEMENTS AND RESERVES THE RIGHT TO MAKE CHANGES TO THIS PRODUCT WITHOUT PRIOR NOTICE

DANISMANLIK TIC. A.S.
813 Kadikoy - ISTANBUL - TURKİYE
ax: 90 216 34 94 30 - 31 34 e-mail:milproj@inter.com.tr



MTU-2002
Message Terminal Equipment for OTEMAS

MTU-2002 is Message Terminal Equipment for OTEMAS Message Handling System. MTU-2002 includes computer and specific Hardware for message handling and security functions. MTU-2002 can communicate on PSTN (Public switched telephone network), leased lines, LAN, WAN, Internet, GSM, Satellite and mobile phone by itself and HF, VHF, UHF channels via TKU-2002A.

MTU-2002 has two crypto modules. Online crypto module is used in HF, VHF, UHF channels, leased lines and PSTN (Public switched telephone network). Off-line crypto module is used in LAN/WAN communication network. Also Off-line crypto is used to protect the data stored in hard disk via different key management protocol.

Digital signature function enables OTEMAS system ensures the originating terminal to be recognised.

Special memory hardware, holds critical information erasable with Emergency Erase Function even the computer is off.

Authentication functionality is provided by smart card.

Features:

- Pentium PC
- Hardware Data and Voice encryption
- Remote control of TKU-2002A by 3km.
- Intercom Facility with TKU-2002A
- Radio equipment control via TKU-2002A
- Ruggedized Aluminium Case
- Tempest AMSG788 (optional)
- Tempest AMSG720A (optional)
- On-line Crypto unit
- Off-line Crypto unit
- Digital Signature
- Smart Card Authentication
- Emergency Erase Function
- Secure Data Base

SPECIFICATIONS

PC Hardware

Pentium 233MMX processor
2.5 GByte Hard Disk
32 MByte RAM
32X CD Drive
33600bps dial-up modem
Ethernet Card
Sound Card

Monitor

14" SVGA Monitor
LCD Monitor (optional)

Security

On-line Crypto module
Off-line Crypto Module
Phone and in secure da
Smart Card: Used in Au
Special Memory: Used in
emergency (256Kbyte exp
Tempest (optinal): Tempest
Secure Data Base: All data store
Digital Signature

Test

BITE: Automatic Built-i
Active on-line Test
Remote Diagnostic of T

RADIO CONTROL: All functio
TKU Remote interface: Com
INTERCOM: Available for ope
Frequency Hopping: Suitabl
Emergency Erase Facility: C
Power Supply 220/110 VAC

Mechanical

S/W controllable electr
19" Rack mountable Al
Dimensions 19" x 17.5"
(482.6mmx444.5mmx117.8mm)

Environmental

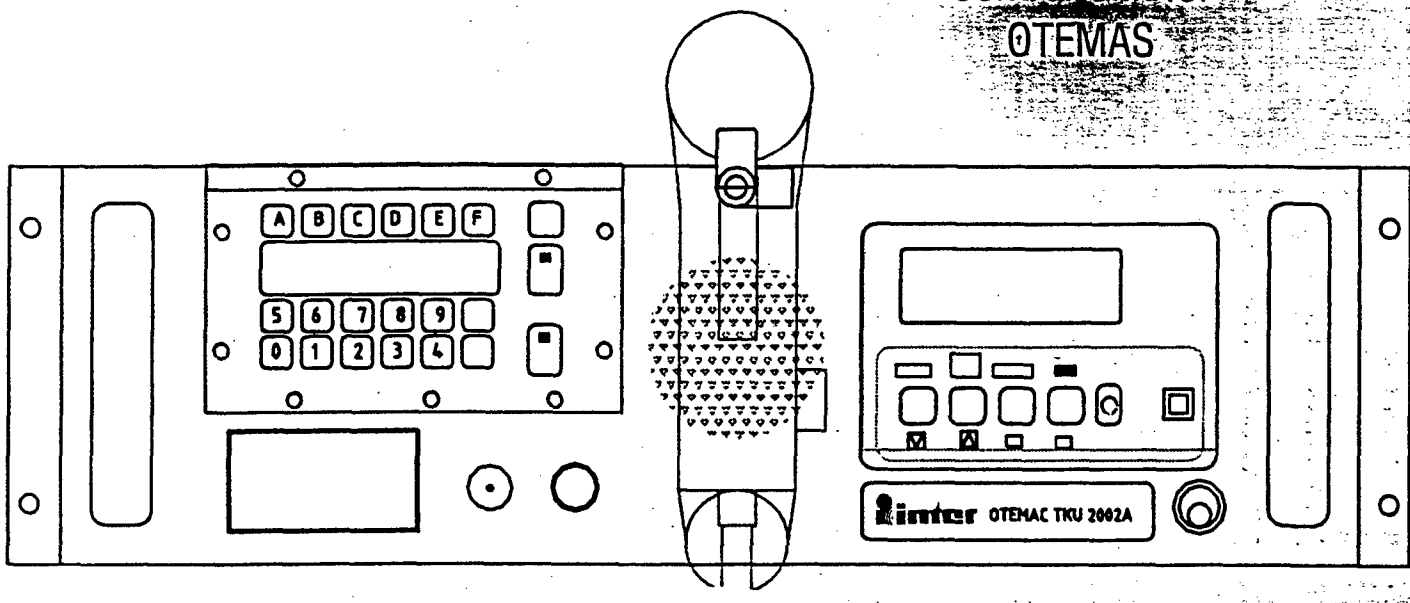
Operational Temperature	0°C to +45°C
Storage Temperature	-40°C +50°C

THE MANUFACTURER HAS A POLICY OF CONTINUOUS AMPROVEMENTS AND RESERVES THE RIGHT TO MAKE CHANGES TO THIS PRODUCT WITHOUT PRIOR NOTICE

İSTANBUL SAVUNMA SANAYİ TİC. A.Ş.
Kadıköy - İSTANBUL - TÜRKİYE
Fax: 90 216 34 94 30 -31-34 e-mail:milproj@inter.com.tr

TKU-2002A

Radio Equipment Control Unit for OTEMAS



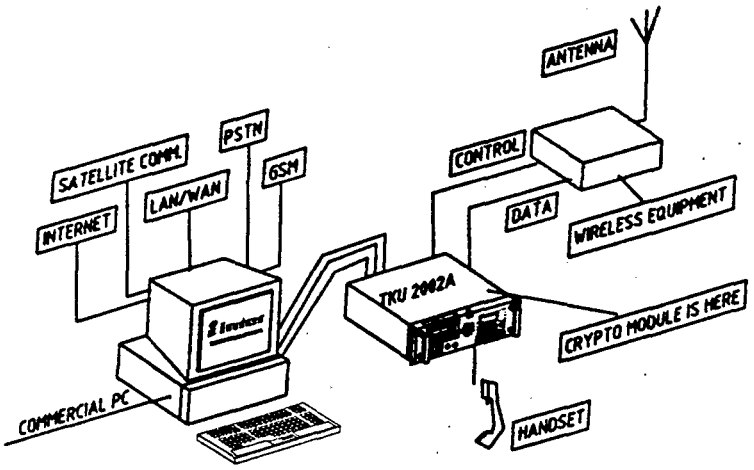
TKU-2002A is designed to control various wireless equipment in OTEMAS message Handling System. TKU-2002A provides OTEMAS to communicate via HF, VHF, UHF radio equipment's OTEMAS Message Handling System can send secure data and voice via HF, VHF, UHF channels by using TKU-2002A in local or remote configuration.

In local configuration, TKU2002A can be used together with ordinary COTS PC (Commercial Off the Self Personel Computer). In this case, crypto module is located inside the unit.

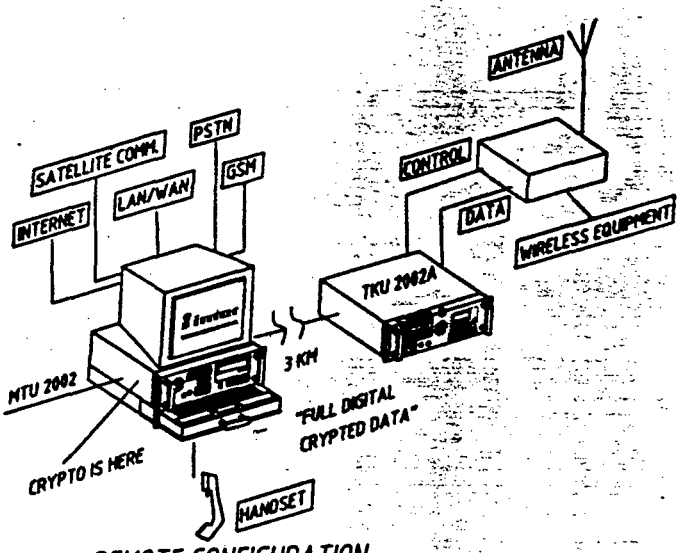
In Remote configuration, TKU2002A can be used together with MTU-2002 Message Terminal Unit. TKU can be controlled by MTU up to 3km. For this case, crypto module is located in the MTU-2002. All data carried between two units is encrypted. Intercom facility is available between MTU-2002 and TKU-2002A.

Features:

- Fully remote controllable by MTU in Remote Mode
- Fully local controllable by COTS PC in Remote Mode
- Intercom Facility
- Built -in HF Serial Modem
- Installable H/W crypto module (local mode)
- Ruggedized Design
- Full control of radio equipment
- Frequency Hopping Operation



LOCAL CONFIGURATION



REMOTE CONFIGURATION

OPERATORLESS Operation: No need for Radio Equipment Operator.
RADIO CONTROL: All functions of radio can be controlled.
INTERCOM: Available for operators of MTU and TKU without interrupting the operation.
BITE: Automatic Built-in-Test is available to module level.

- Active on-line Test
- Remote Diagnostic Facility
- Functional Testable via PC

Multi Processor design:
Frequency Hopping: Suitable for frequency hopping radio equipment
Emergency Erase Facility
HF Modem

- HF Serial Tone Modem
- STANAG 4285
- MIL-STD-188-100A

Power Supply

- 220/110 VAC
- 28VDC (optional)

Mechanical

- 19" Rack mountable Aluminum Ruggedized Case
- Dimensions 19" x 17.5" x 7.25" (Width-Depth-Height)
  (482.6mm x 444.5mm x 183.4mm)

Environmental
Operational Temperature

- -10°C to +45°C
- -30°C to +50°C (optional)

Storage Temperature

- -40°C to +50°C

THE MANUFACTURER HAS A POLICY OF CONTINUOUS AMPROVEMENTS AND RESERVES THE RIGHT TO MAKE CHANGES TO THIS PRODUCT WITHOUT PRIOR NOTICE

MÜHENDİSLİK DANIŞMANLIK TİC. A.Ş.
81310 Kadıköy - İSTANBUL - TÜRKİYE
Tel: 90 216 349 30 00 Fax: 90 216 34 94 30 -31-34 e-mail:milproj@inter.com.tr

OTEMAS 2001

Automation and Reliability in HF-SSB Communication

HF/SSB Communication Equipments have the capability of transmitting the information in the voice, data and fax form. In order to transmit these type of information, HF-SSB devices have various different functions which have to be manipulated in different modes. In addition, there are manual steps to be followed by the operators.

➢ Automation

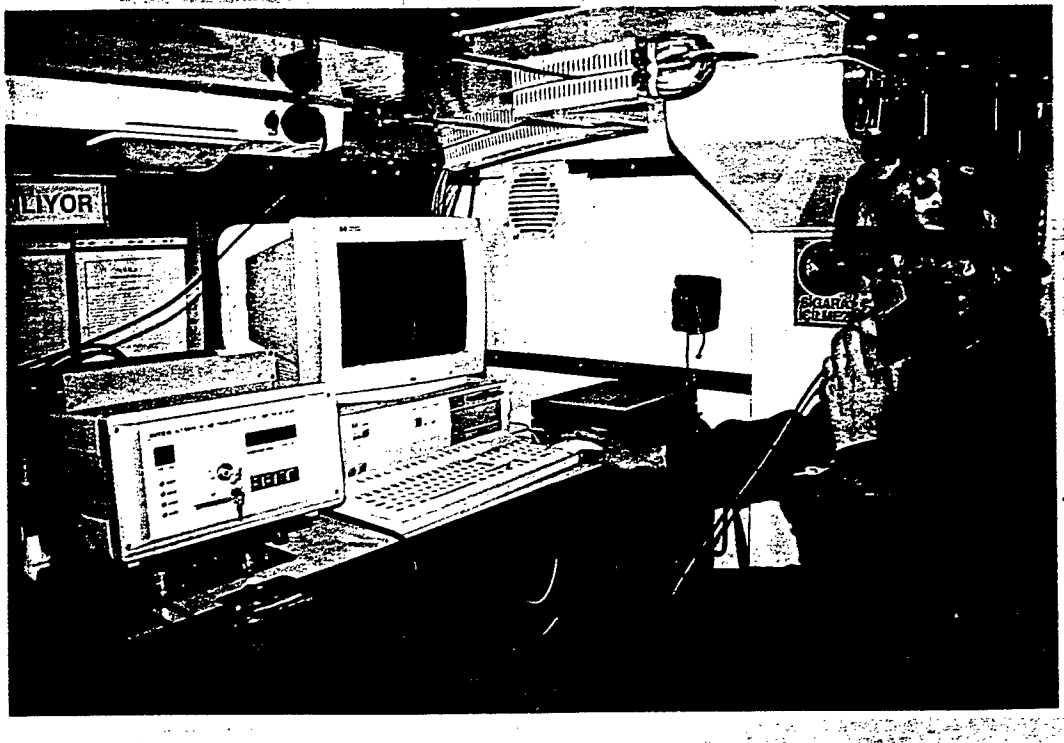
Automatic Message Handling System (OTEMAS) eliminates the manual steps, controls all functions of HF-SSB device, evaluates the status information and passes the required control commands. It also automatically selects the best frequency and determines the data transferring speed.

➢ Reliability

The Message is squeezed by eliminating the redundant information so that transmitting time can be shortened. For instance, a 2.7 Mbyte data can be converted to the one of 430 Kbyte. The transformed information is divided into packages and then a heading and CRC section are added to the beginning and end of the each package respectively. These message packages are transmitted in series. In this way, Tx and Rx stations establish a mutual agreement and continuously coordinate the receiving and transmitting functions. Receiving side checks every single package so that it was correctly intercepted, accepts the true packages and requests re-transmission for the false ones. This procedure automatically repeats until the false ones are correctly received. OTEMAS can handle any type of information by 100 percent truth.

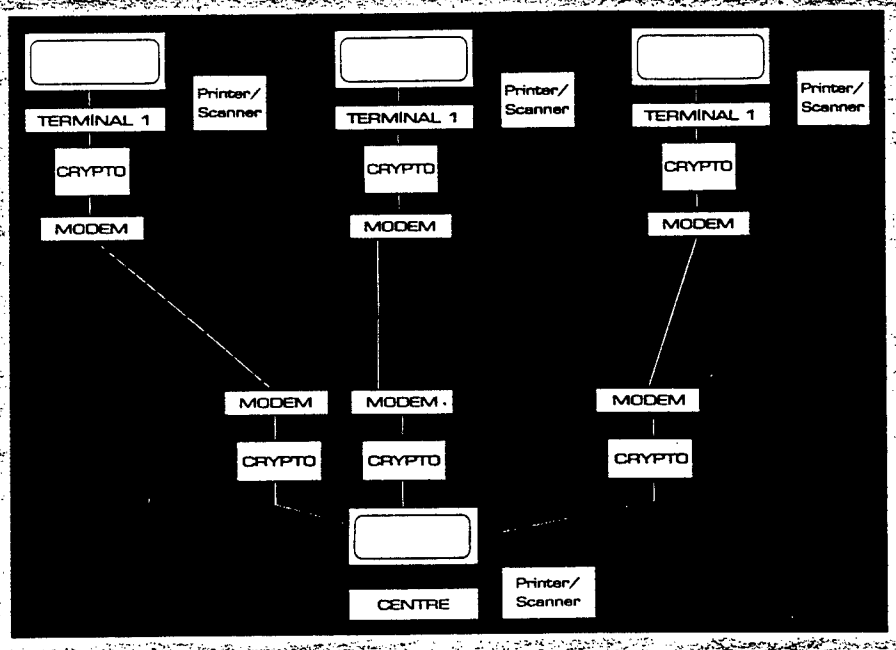
➢ Fast Communication

The information in the data format could be a Word file, an Excel file, a coded or un-coded messages, a scanned picture or a map information. Any kind of information, which is compatible to Windows/NT and can be send with a speed of 2400 bps, can be successfully handled by OTEMAS. In addition, various messages can be mutually transmitted and received at a time, i.e., the receiving side reports the true ones among the intercepted messages and sends his own messages while the other side continues to transmit the various information of the different messages in the mixed packages. So semi-duplex HF/SSB communication seems Full Duplex system to the users.



➢ Network

OTEMAS is a system composed of a main and various sub terminals. Every terminal can receive from and transmit to the other terminals. Since sub terminals have no direct connections, all information are passed through the central station. That's why all activities of the entire system can be continuously monitored and, if necessary, can be intercepted from the central station. System provides a secure communication due to the existence of the on-line crypto and the capability of handling any type of data. System communicates with both single tone serial modem and HF parallel modem. High performance is achieved when the single tone serial modems are used. In addition to HF/SSB devices, OTEMAS can also send messages via the commercial telephone lines.
A HF/SSB device connected to an OTEMAS terminal can be integrated to a Local Area Network (LAN) with an Ethernet card or can reach to a PC terminal having an OTEMAS system with a modem. So messages or information created at the sub terminals can be transmitted through HF/SSB unit to the other stations in long distance. On the other hand, an authorized central terminal can automatically apply "Slience MODE" to all OTEMAS terminals under his control and can also get the statistic or status information from their data bank.



➢ Basic Advantageous

- Archiving
- Data acquisition for the frequency planning
- Automatic frequency scanning
- Automatic speed adjustment
- Secure Communication
- Data squeezing
- Automatic link establishment
- RF Protocol
- Easy integration to a Local Area Network
- Capability of Automatic Communication Slience ???
- Compatibility to Windows NT 4.0
- Having SW for Fax transmission
- Easy operation

➢ Configuration

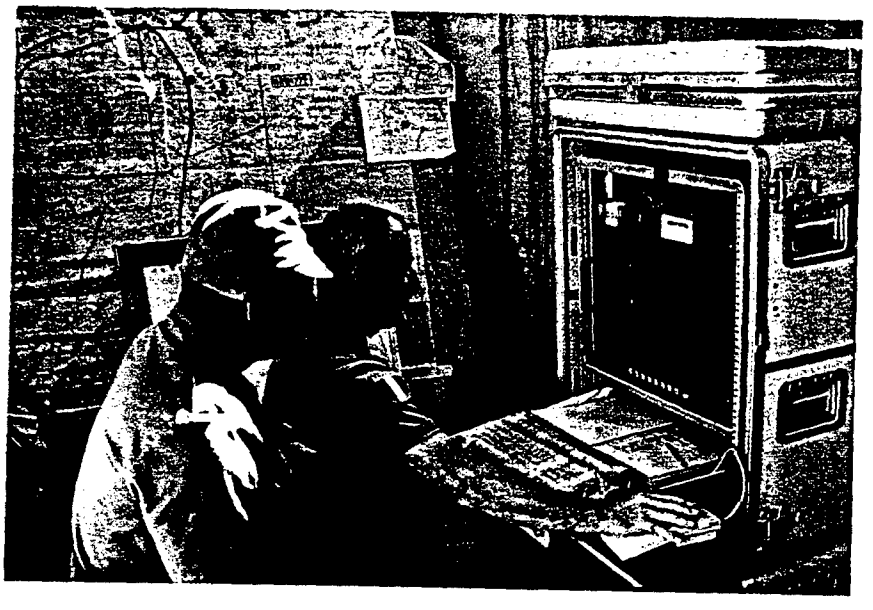
IBM compatible Pentium PC
SVGA Colour Monitor
OTEMAS 2001 Software and Hardware
Serial MODEM
Printer/Scanner
CRYPTO unit
HF/SSB device

İSTANBUL:
Hasırcıbaşı Cad. 55, 81310 Kadıköy İSTANBUL
Tel: +90 (216) 349 94 00 Fax: +90 (216) 349 94 34 Telx: 29245 inmd tr
ANKARA:
Kızkulesi Sok. 36/3-4, 06700 Gaziosmanpaşa ANKARA
Tel: +90 (312) 436 44 21 Fax: +90 (312) 436 44 93 Telx: 46780 iter tr

A.4 Brochure van 'SIPAC-NT'

SIPAC-NT

CCIS adapted to the new operational context



A changing environment

During the past years, the operationnal environment of Command and Control Information Systems (CCIS) has undergone major changes:

- The increasing number of out of area operations together with the diversity of mission types and operation theaters have required continuous adaptation of operational doctrines and command and control organizations.
- Moreover CCIS have to integrate desktop technology which has become of common use among most military staff officers.

Because of the continuity between peace-time/crisis-time/war-time, it has become essential to offer CCIS users easy to use tools.

A field proven solution

Relying on the experience of the development of a family of operationnal systems called "SCT-EMA" wich were deployed in the French Joint Forces Headquaters from 1993 to 1996 and relying on the experience gained through the use of the system during the recent opérations (in SOMALIA, in RWANDA, in BOSNIA), Alcatel ISR has been contracted by the French MoD (SICA program managed by DGA/SPOTI) to develop a Joint Forces CCIS kernel called SITRENS/ SIPAC-NT.

- SITRENS is used by the French Military Intelligence Head-Quarter (DRM). It is dedicated to crisis situation assessment and intelligence data repository management.
- SIPAC-NT is based on the same kernel as SITRENS. It is dedicated to situation assessment and opérations command and control. It has been experimented during the last EOLE Joint Forces and Multinational exercise. It is to be deployed for all the Joint Forces HeadQuarters in France.

A comprehensive set of integrated decision support services

The SIPAC-NT kernel features a set of services which can run on the same PC:

- send and receive messages,
- manage staff documents, sort and search document databases,
- circulate documents and sign them electronically,
- manage and graphically display operational data (Battle Order, forces locations and moves, enemy activities, logistic data, ...),
- memorize and restore the evolution of data,
- manage and display situation snapshots (own forces, enemy, logistics, humanitary),
- group and sort information in customised folders (crisis folder, sites of interest, ...),
- exchange data with other headquarters.

The integration of these services into the WINDOWS-NT environment facilitates information exchange with desktop applications such as WORD or POWERPOINT.

ALCATEL

A comprehensive set of interoperability tools

- The SIPAC-NT kernel enables to interoperate with allied systems through ADatP-3 messages and also with external databases.
- It integrates Lotus Notes MHS. It can also interface directly any other MAPI MHS and standard X400-88 MHS.
- A specialized tool allows to dynamically define the matching between the system data model and the structures of exchanged messages or files.

Adaptation to the operationnal environment

The SIPAC-NT kernel includes several tools for adapting the system to its environment:

- cartographic workshop for importing digitized maps in the USRP, ASRP, SPOTImage, DCW and VMAP formats as well as for paper map scanning, assembling and georeferencing,
- cartographic symbology definition workshop,
- graphical data model extension workshop,
- edition of data input form.

On the field deployment

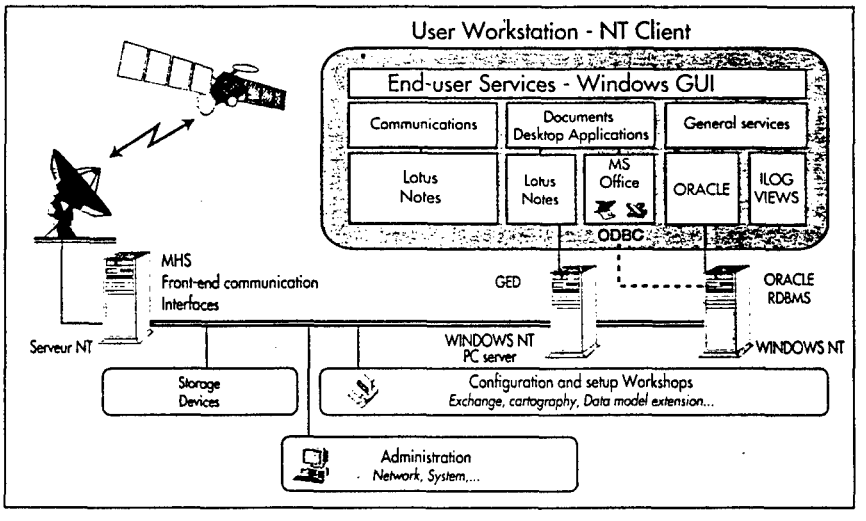
- The SIPAC-NT kernel enables the development of systems operating on the field with ruggedized and redundant hardware and offers tools to manage the progressive deployment of the system (scalabality).
- SIPAC-NT facilitates the deployment of multi-site command and control chains with the capability to manage the replication of database subsets.

Technical features

- **Integration of widely distributed commercial software:**
  - ORACLE RDBMS,
  - Lotus Notes for document management and MHS,
  - ILOG-VIEWS graphical library,
  - IRIS-MFS software for ADatP-3 messages formatting/deformatting,
  - MICROSOFT Office desktop applications.
- **Compliance to standards:**
  - ANSI SQL2,
  - Visual C++ development language,
  - MAPI interface,
  - WINDOWS-NT operating system.
- **Open architecture:**

The open architecture of the SIPAC-NT kernel enables to develop and to integrate specialized applications through the use of C++ API libraries which provide full access to the basic SIPAC-NT kernel services (object management, cartography, interoperability, ...).

Moreover, the relationnal database is accessible from external applications through SQL or ODBC.



ALCATEL

Alcatel ISR - 3, rue Ampère - 91349 Massy Cedex - France
Phone: 33 (0)1 69 76 21 41 - Fax: 33 (0)1 69 76 21 73 - Telex: 600 815 F

Imprimerie STEP - 7/98 - Non-contractual document.

A.5 Brochure van 'SICOA'


and Command System
Interoperable
Adaptable
Integrated
Flexible
Overseas Theaters
COMMUNICATIONS

SICOA

Air Force Information and Command System

→ **A coherent, integrated offer**

- Planning
- Tasking
- Control

} of the intelligence and air maneuver

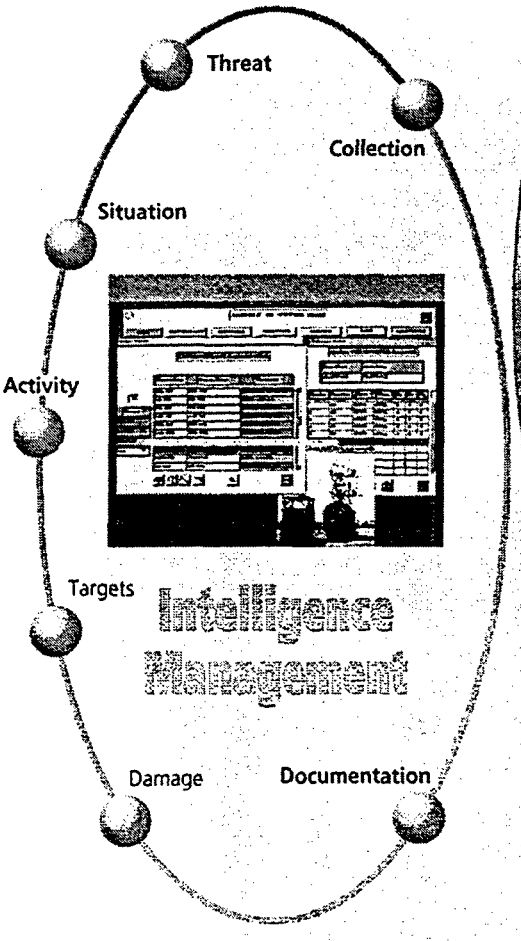
Systems adaptable to the Air Forces' requirements

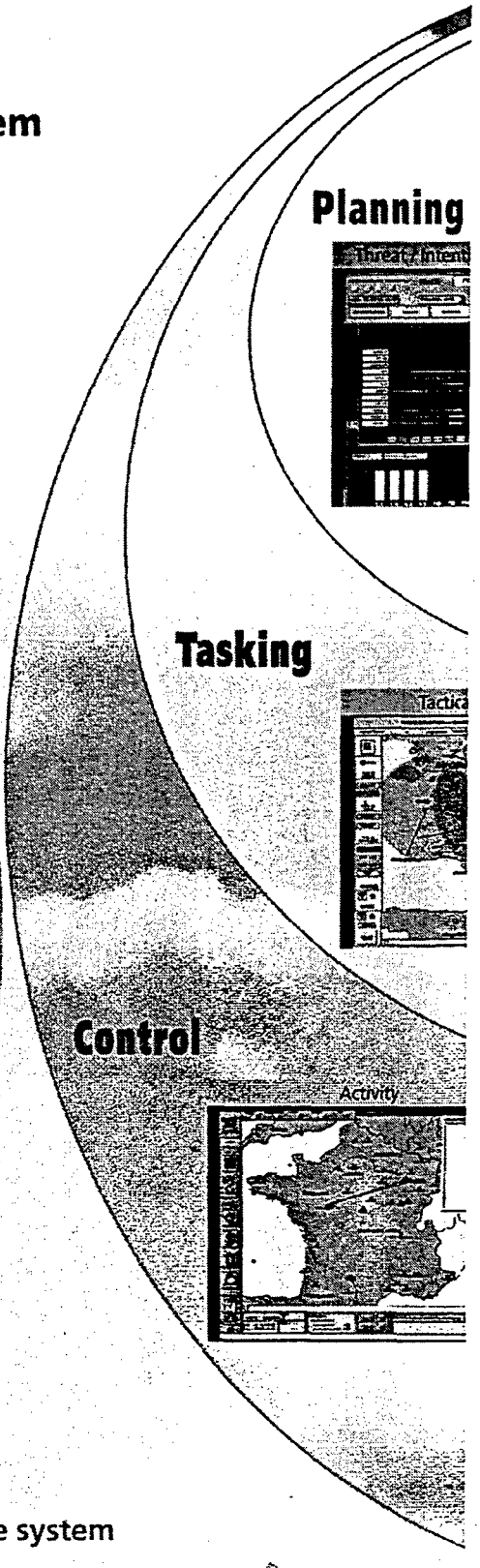
The new world context has deeply modified the concept of force engagement : many and remote operation theaters, multinational engagements, interventions in peace time, crisis or war time... require a continuous command function, able to adjust to any new situation, including immediate reaction and coordination capabilities.

Thomson-CSF Communications' information and command systems are designed to meet these new requirements for operations in **overseas theaters**. They make up a proven and reusable platform that can be easily **adapted** to the needs of any country.

Built on this open-architecture platform, SICOA is an **integrated** and **flexible** system with a wide range of operational services.

As a result, SICOA, in coordination with existing systems, addresses the **entire** Air Force chain of command.

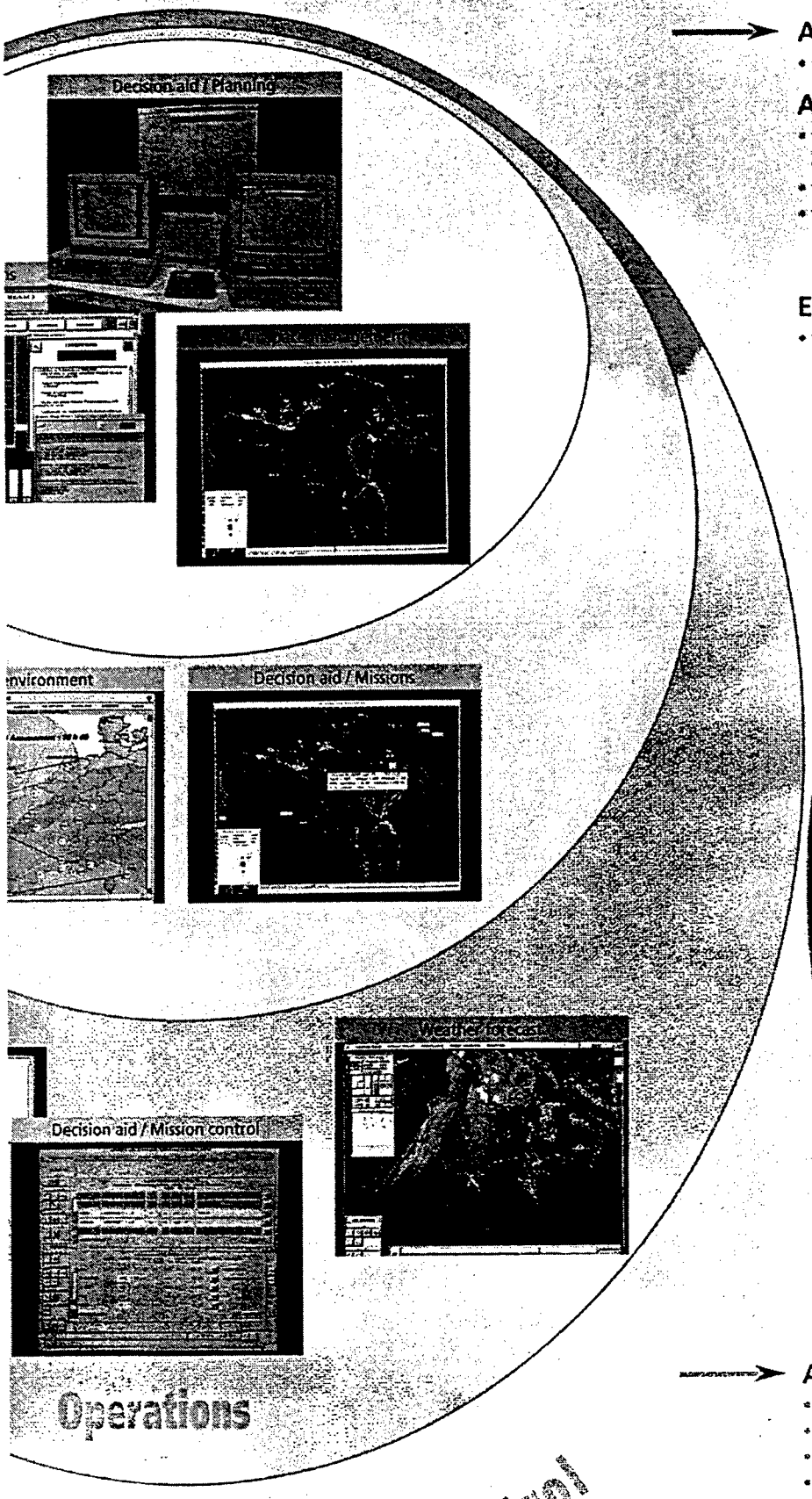




→ **An interoperable system**

Interoperable with :

- higher echelons
- operational echelons
- other forces
- Allies



A flexible system,

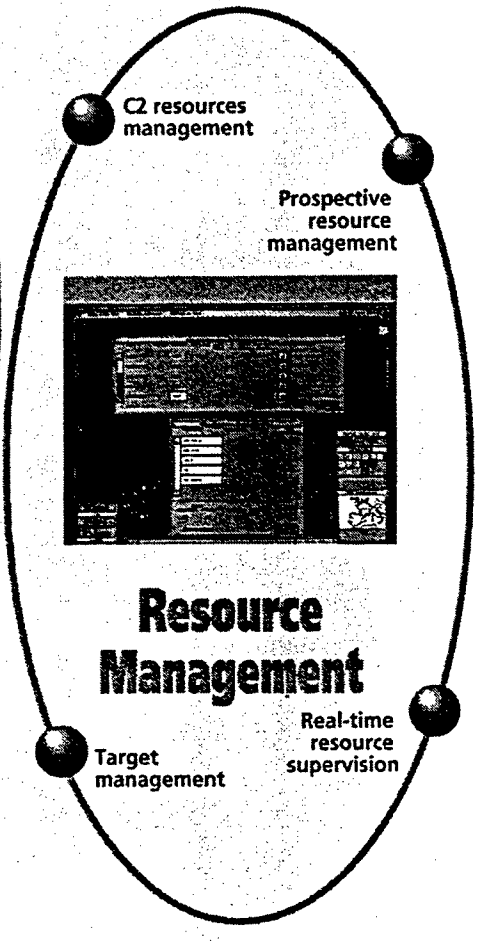
- modular, multisite, multiposition

Adaptable

- to organizational structures of any country
- to various operating constraints
- to available communication means (tactical and infrastructure networks, satellites,...).

Evolutive

- taking into account any situational context.



Advanced

- open architecture
- object technology
- standards and COTS
- office automation environment

User-friendly

- ergonomy
- graphic-oriented man-machine interface
- high-performance cartography

...d, Command and control

EXPERIENCE AT YOUR SERVICE

Major references

- Air Force : IRIS 7/OSIRIS
- Land Forces : SICF/SCEA
- Joint Forces level : ENTAME

Requirement understanding

- Several years in close cooperation with the Air Forces in France and throughout the world

All-skill combination

- Technical, managerial and industrial know-how within the same company

The power of innovation

- Motivated and expert teams, supported by the huge R&D potential of Thomson-CSF

Program management

- A capacity demonstrated on many programs based upon mastered methodologies

The guarantee of durability

- Operational maintenance guaranteed throughout the life-cycle of the system

THOMSON-CSF
COMMUNICATIONS
Information and Communication Systems Group
(6, boulevard de Vaux - BP 55 - 92704 Colombes Cedex - France
Tel. : (33) 1 41 30 30 00 - Fax : (33) 1 41 30 44 57
http://www.tcc.thomson-csf.com

Design : PILOTE Image & Conception - EPCOM - Mai 1996

A.6 Sheets van 'JFACC-AOC'

JWID 98

JFACC - AOC

Sponsored by Thomson Communications ------ Supported by French Air Force

THOMSON-CSF

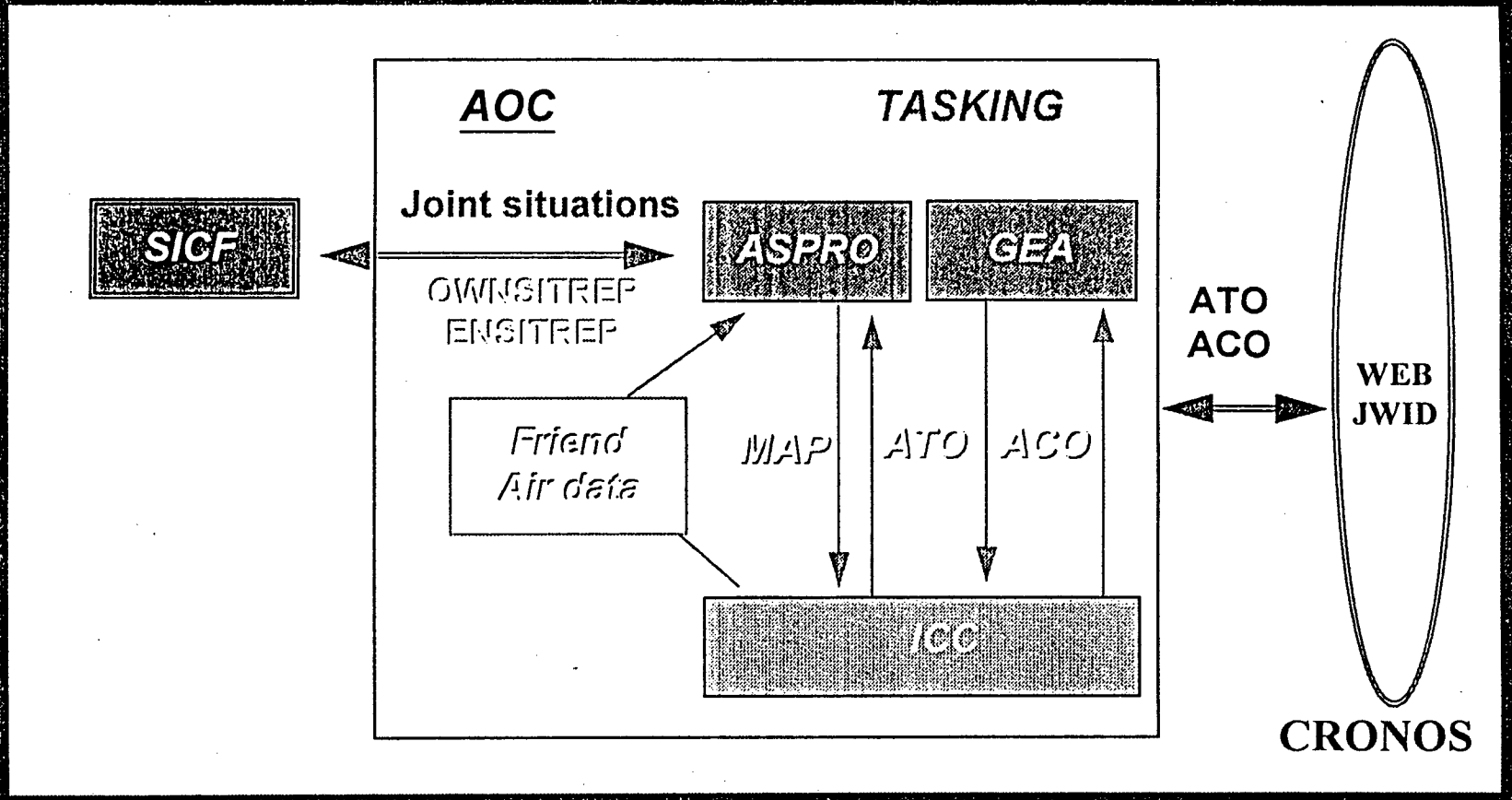
CDAOA/CASPOA

07/98 - FR JFACC-1

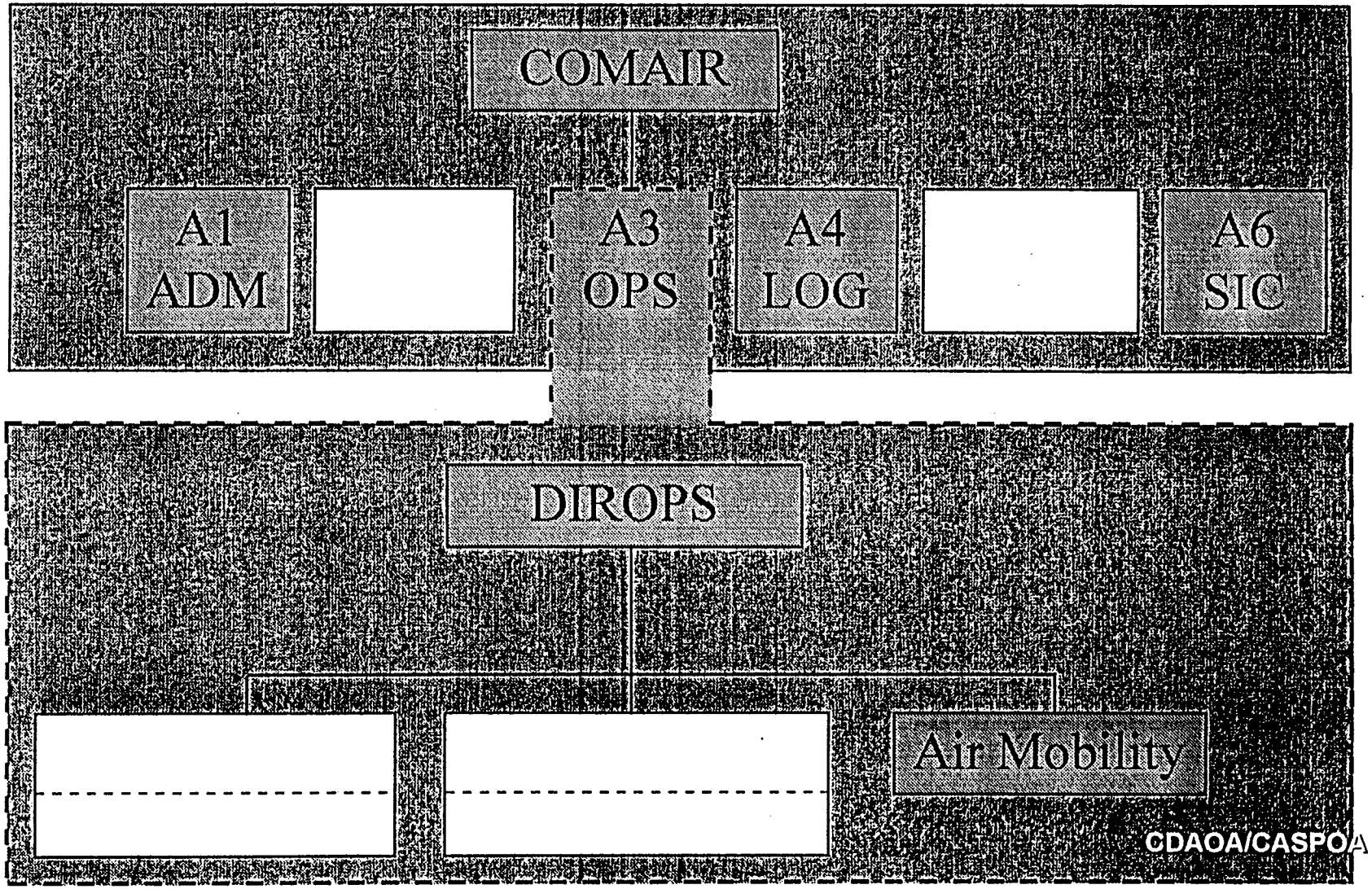
JWID 97 : Combat Plan

- **Operational capabilities :**
  - **Integrated tasking : ASPRO & ICC**
  - **Joint and Combined operation : ASPRO & SICF**
- **Technical feasibility :**
  - **Data exchange through CRONOS and LAN using ADatP3 or specific formats**

JWID 97: ARCHITECTURES & SYSTEMS



JWID 98: Supported Functions

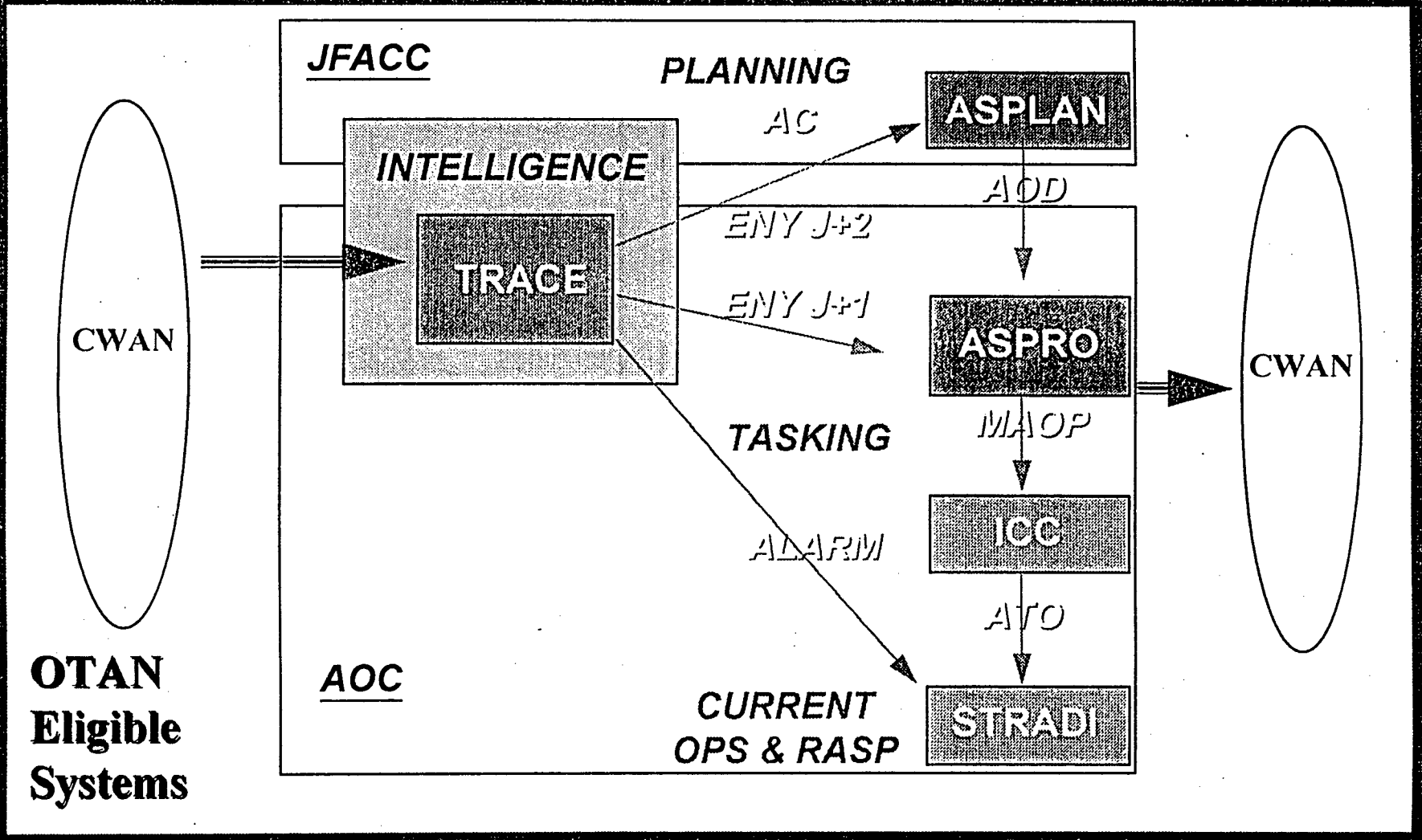


JFACC - AOC SUPPORT SYSTEM

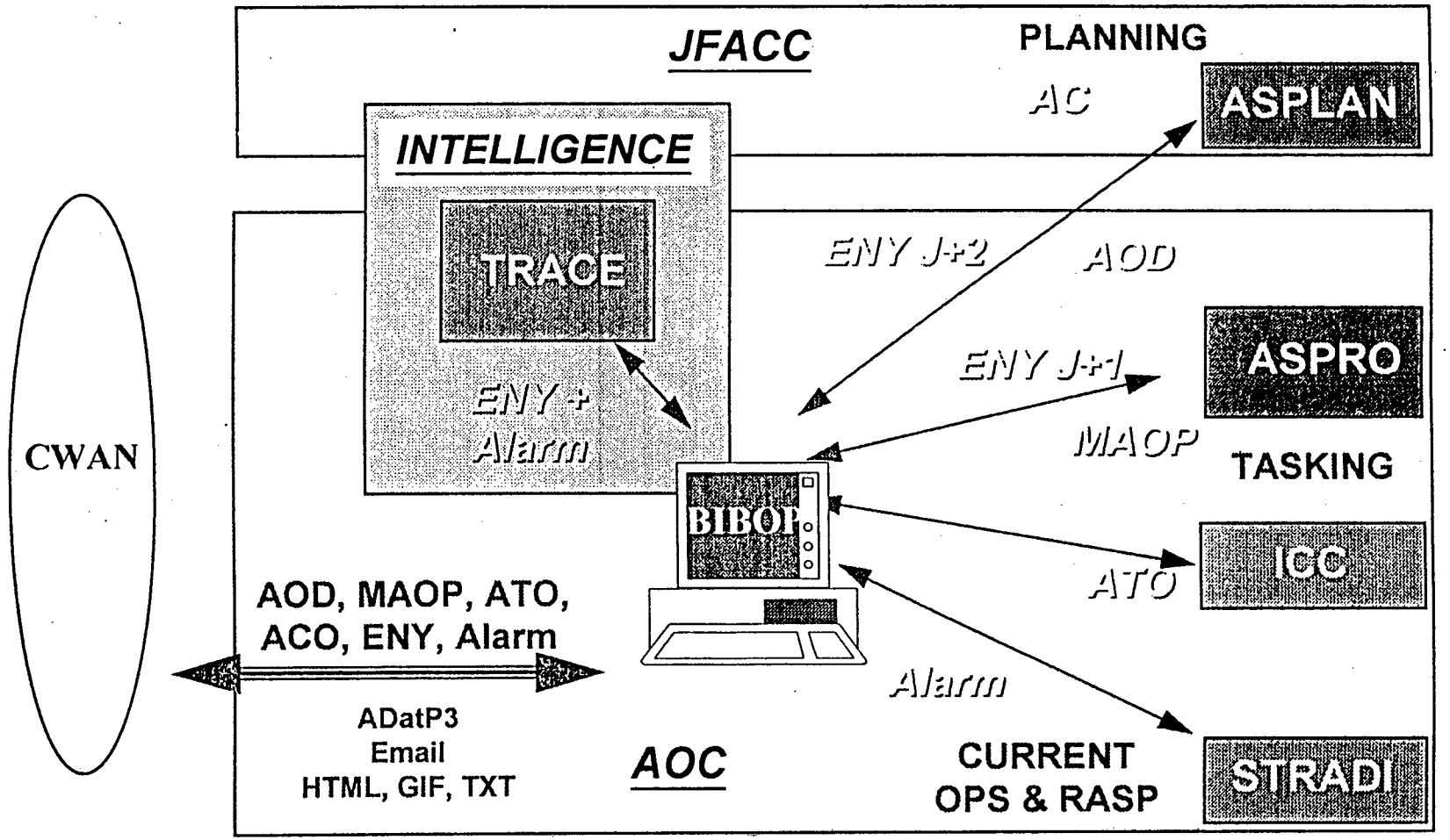
Coherent chain :

- **JFACC**
  - **Planning : ASPLAN**
  - **ENY Sit. elaboration & exchange : TRACE**
- **AOC**
  - **Combat Plan : ICC, ASPRO**
  - **Current Ops & RASP : STRADIVARIUS**
  - **ENY Sit. elaboration & exchange : TRACE**

ARCHITECTURES & SYSTEMS



SYSTEM INTEROPERABILITY



ASPLAN

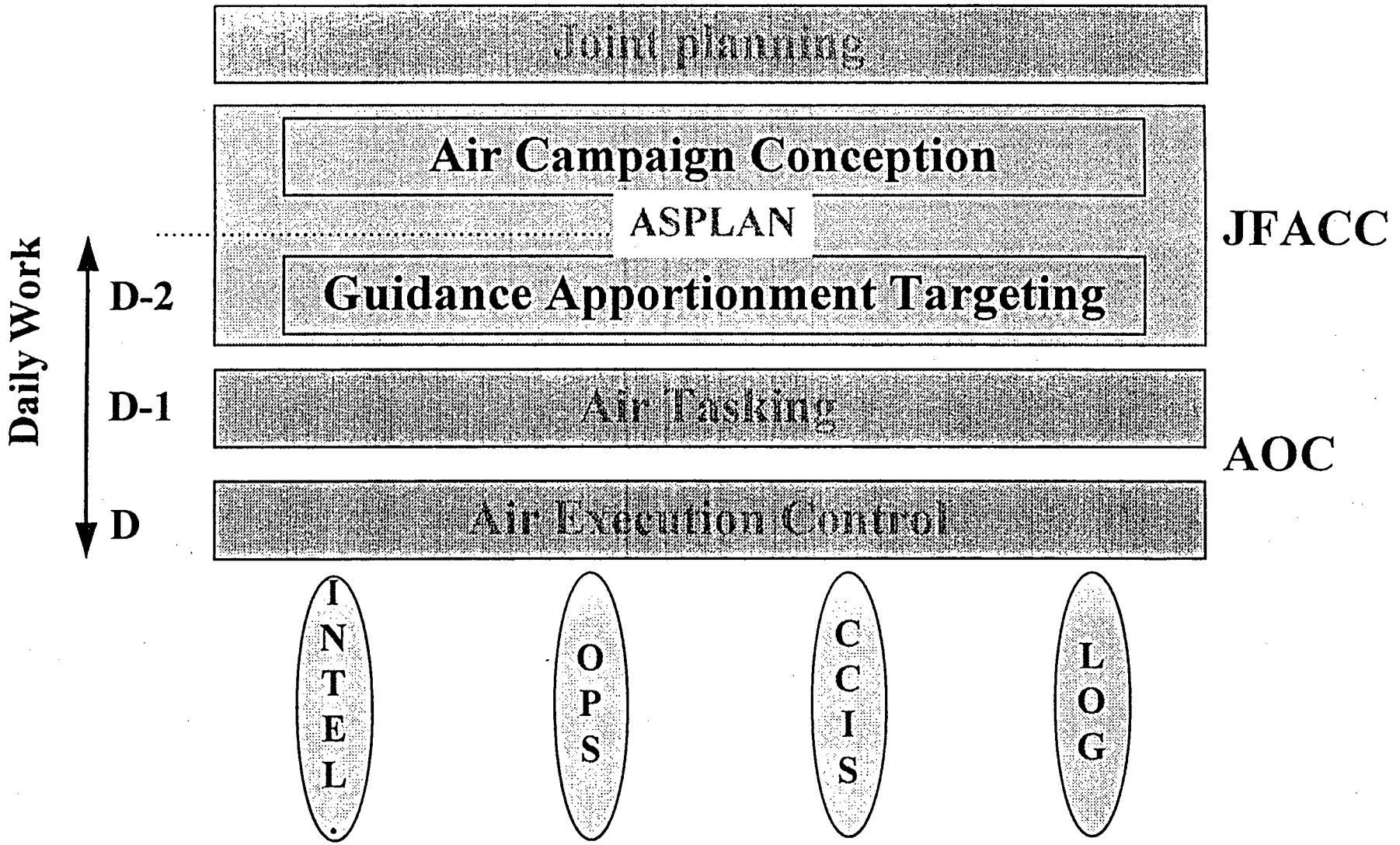
JFACC Planning System

THOMSON-CSF

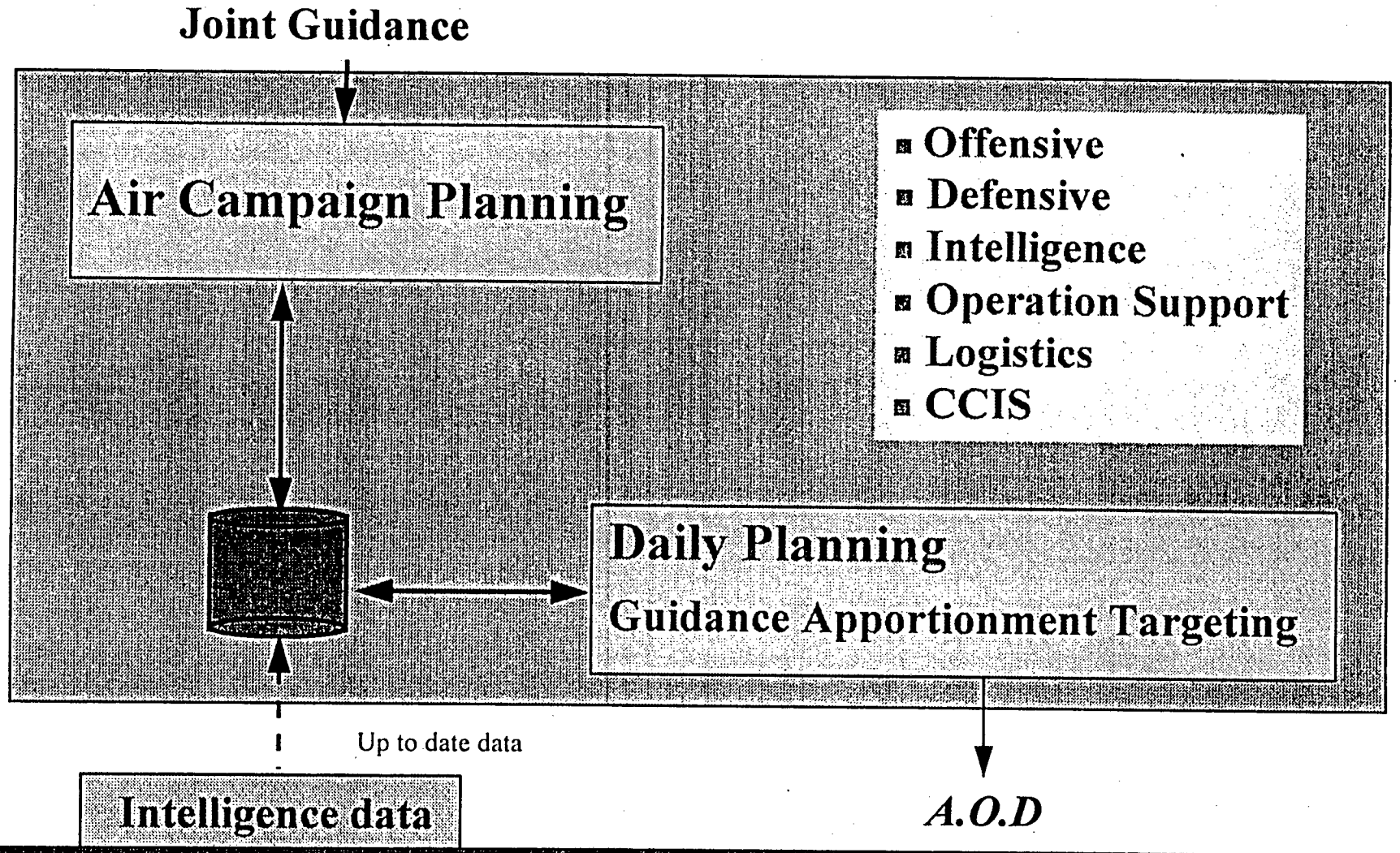
CDAOA/CASPOA

07/98 - FR JFACC- 8

JFACC PLANNING SYSTEM



AC- AOD SYSTEM

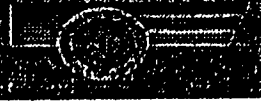


ASPRO

MAOP, Weaponeering & Tasking system

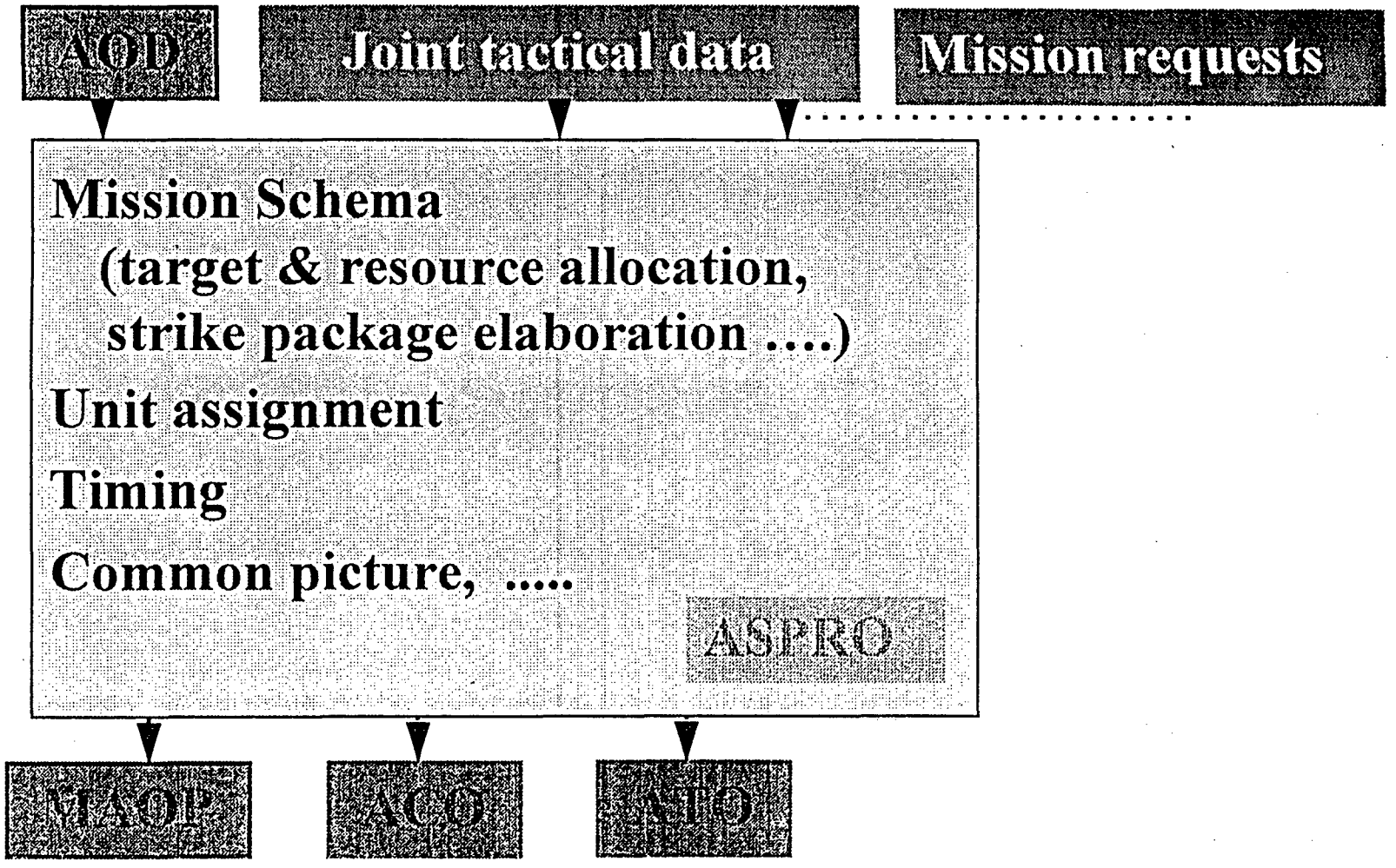
THOMSON-CSF

CDAOA/CASPOA



07/98 - FR JFACC-11

AOC - MAOP SYSTEM



TRACE

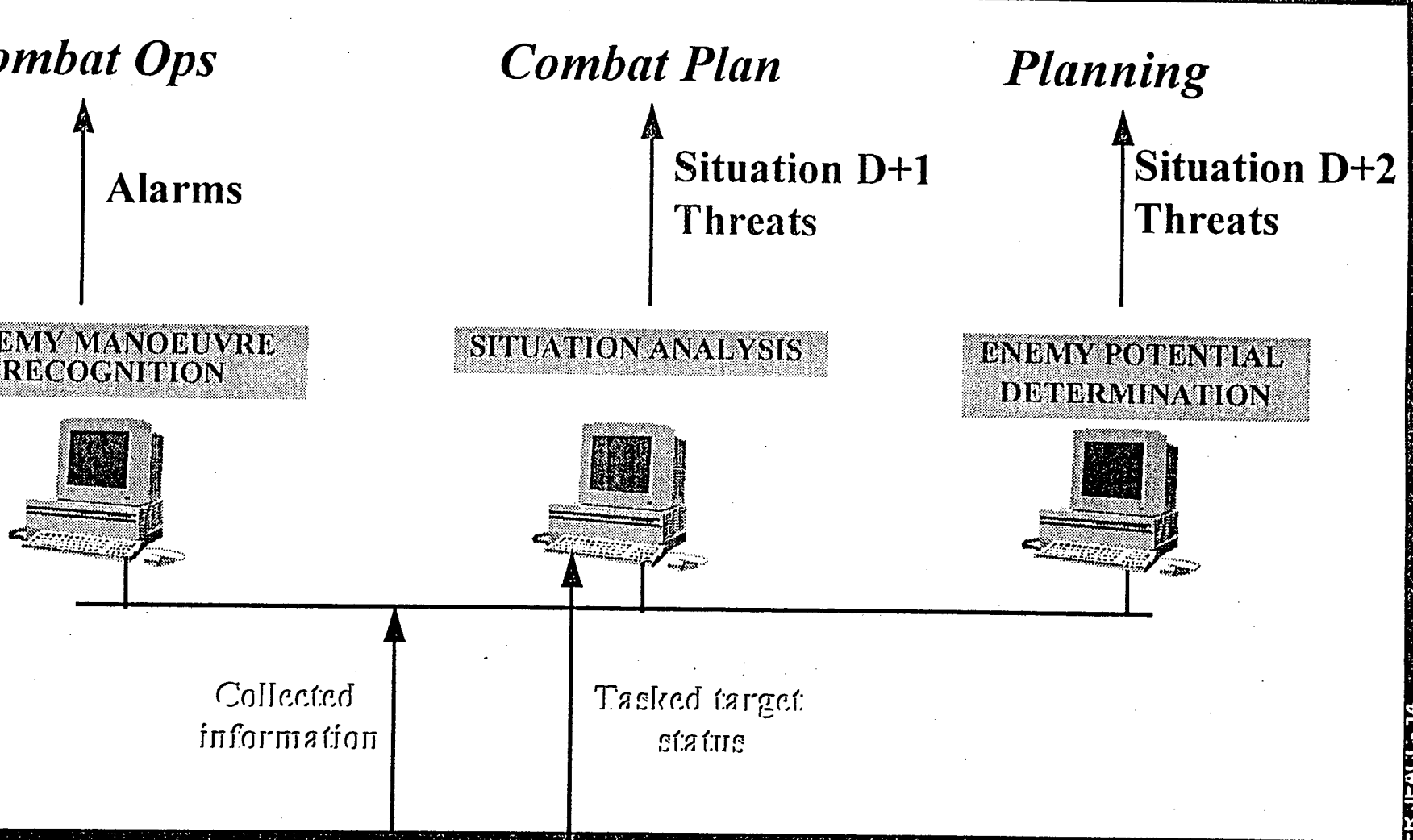
Air Intelligence Processing System

THOMSON-CSF

CDAOA/CASPOA

07/98 - FR JFACC- 13

TRACE : INTEL INTEGRATED APPROACH



TRACE FEATURES

Enemy manoeuvre recognition

- Enemy activity information fusion
- Enemy activity level determination
- Current manoeuvre recognition, manoeuvre assumption

Tactical Situation elaboration and management

- Equipment and facilities status update (sites)
- Targets status compilation
- Tactical situation data update

Threat assessment & evolution presentation

- Threat and potential new target determination
- Enemy capacities evolution and predicted situation determination
- Threat assessment (sam rings, air offensive and defensive assessment)

BIBOP

Systems Integration

THOMSON-CSF

CDAOA/CASPOA

07/98 - FR JFACC-16

BIBOP FEATURES

- **Aims :**
  - Information handling
    - Data exchange control & validation
    - Data repository function
  - System integration solution
- **Technical features :**
  - PC Windows/NT
  - Exchange Server (Netscape clients)
  - WEB Server
  - Data Base : ACCESS + RDBMS

STRADIVARIUS

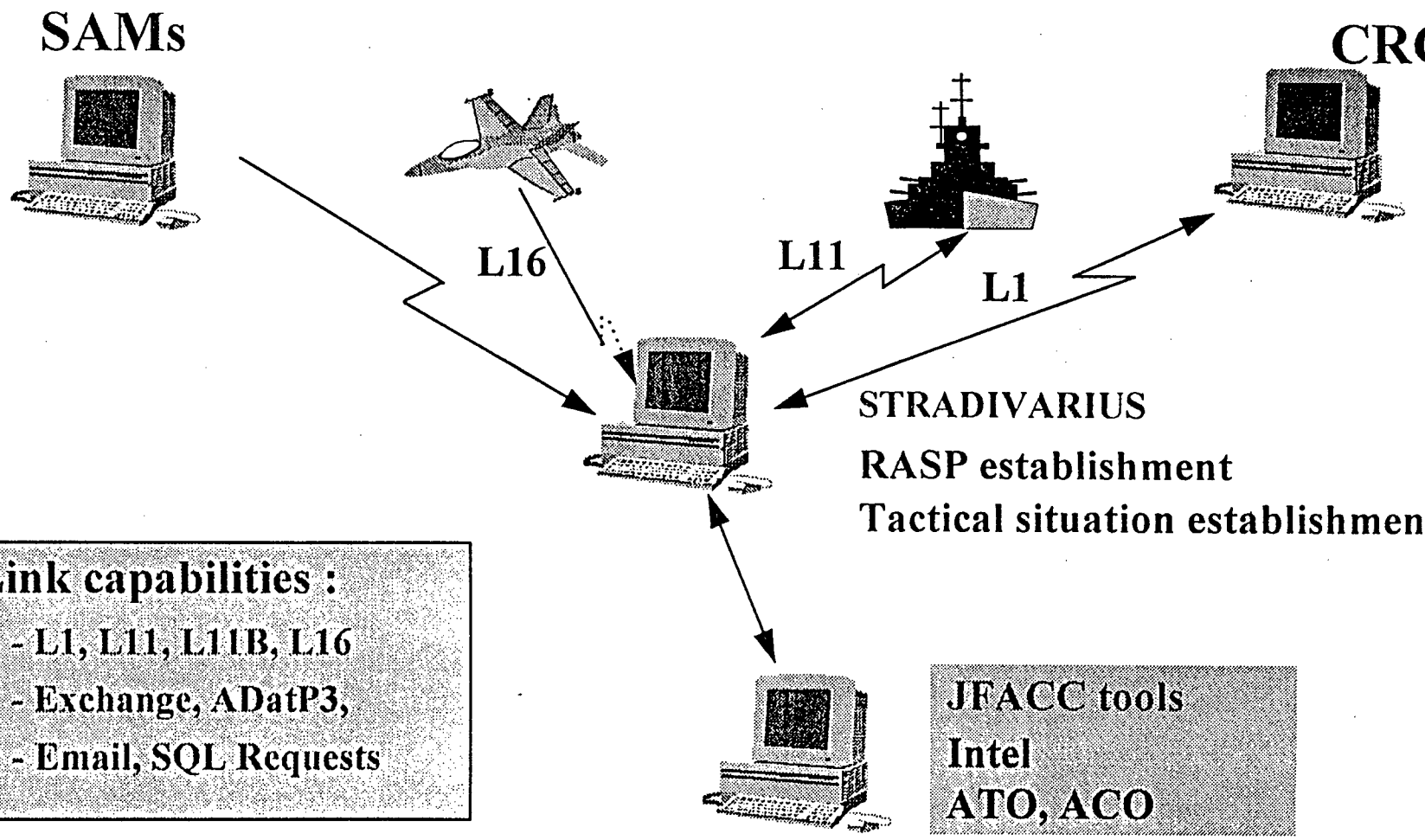
JFACC Combat Ops Tool

THOMSON-CSF

CDAOA/CASPOA

07/98 - FR JFACC- 18

STRADIVARIUS : COP PRODUCTION



STRADIVARIUS

- **Current ops :**
  - COP establishment & management
    - Tactical data links
    - ATO / ACO deconfliction
    - Replay & Archivage functions
- **Training & Support :**
  - Exercises
    - Scenario generation / animation
    - Replay & Archiving functions
    - Detection modelling capability
  - Simulation
    - War-gaming
    - HLA compliance (under development)

A.7 Brochure van 'SDA'

SPECIFICATIES VOOR DRAAGBARE DIGITALE COMMUNICATIE

De landmacht werkt vaak in moeilijke omstandigheden. Overzicht houden en de juiste beslissingen nemen is van levensbelang. Vandaar dat er hoge eisen worden gesteld aan de technologie die de communicatie vormt tussen de troepen te velde onderling en bijvoorbeeld het hoofdkwartier.

Tot voor kort ontwikkelde de landmacht steeds een eigen uniek informatie systeem. Tegenwoordig wordt ervan uitgegaan dat er een breed aanbod van commerciële hardware en software snel en flexibel is in te kopen. De landmacht schaft deze aan, waarbij wordt gelet op gebruikersspecificaties en de software-specificaties.

vraagstelling

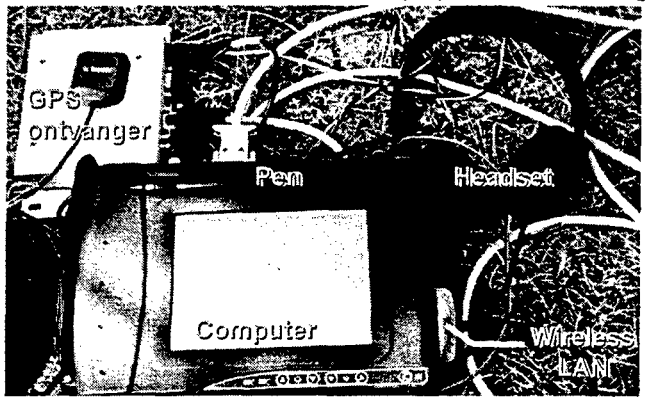
De landmacht vraagt TNO de technologische specificaties te formuleren waaraan een individuele communicatieset voor de gevechtssoldaat moet voldoen. De communicatie is gebaseerd op radiocontact en maakt gebruik van internettechnologie. Spraak en de mogelijkheid schetsmatige informatie of positie-informatie uit te wisselen staan hierbij centraal. Voor de uitvoering van het apparaat gelden de gebruikelijke randvoorwaarden van de landmacht: het dient handzaam te zijn, gemakkelijk te bedienen en het moet tegen een stootje kunnen.

TNO-onderzoek

Op de IT-markt koopt TNO hardware in waarmee het prototype is gebouwd. Het onderzoek richt zich op de koppeling van verschillende softwaretoepassingen, op de integratie van uiteenlopende hardware en de ontwikkeling van software tot een gebruikersinterface op maat.

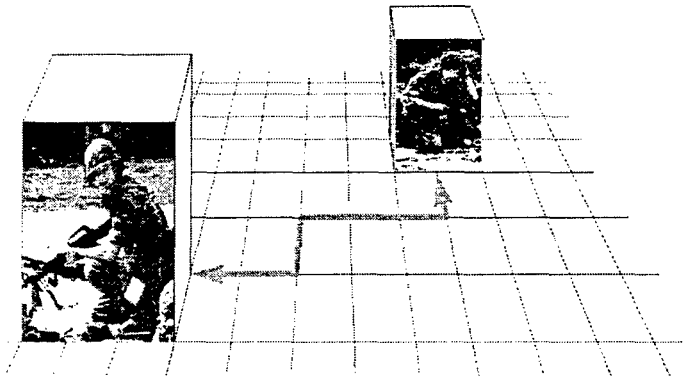
resultaten

TNO ontwikkelt de Soldier Digital Assistent, een prototype van een handzame communicatieset. Het betreft een multimedia-computer met de afmetingen van een sigarenkist. Het apparaat heeft een display en aansluitmogelijkheden voor koptelefoon en microfoon. De Digital Assistant wordt bediend met behulp van pen en display, een toetsenbord is overbodig. Met dit systeem kan de individuele infanterist communiceren via een radionetwerk.



mogelijkheden

De kennis rond de Soldier Digital Assistant kan worden ingezet in iedere omgeving waar een handzame draadloze digitale uitwisseling van gegevens gewenst is. Te denken valt daarbij aan alle beroepsgroepen die in de buitenlucht werken en contact onderhouden met de thuisbasis, bijvoorbeeld bij hulpdiensten als politie, ambulance of brandweer of in de geodesie. Andere mogelijkheden zien we in de gezondheidszorg: artsen of thuiszorg kunnen gebruikmaken van de handzame portable computer.



Voor verdere informatie:
TNO FEL
ir. P.H. Zwaard

Postbus 96864
2509 JG Den Haag
Oude Waalsdorperweg 63
2597 AK Den Haag
tel. 070-374 0326
fax 070 374 0651
Zwaard@fel.tno.nl

S M P
soldier
modernisation
programme

TNO

REPORT DOCUMENTATION PAGE
(MOD-NL)

1. DEFENCE REPORT NO (MOD-NL)	2. RECIPIENT'S ACCESSION NO	3. PERFORMING ORGANIZATION REPORT NO
TD98-0194		FEL-98-A248
4. PROJECT/TASK/WORK UNIT NO	**5. CONTRACT NO**	**6. REPORT DATE**
28323	A98D755	December 1998
7. NUMBER OF PAGES	**8. NUMBER OF REFERENCES**	**9. TYPE OF REPORT AND DATES COVERED**
100 (incl appendix, excl RDP & distribution list)	-	Final

10. TITLE AND SUBTITLE

JWID'98: een impressie
(JWID'98: an impression)

11. AUTHOR(S)

P.H. Zwaard

12. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

TNO Physics and Electronics Laboratory, PO Box 96864, 2509 JG The Hague, The Netherlands
Oude Waalsdorperweg 63, The Hague, The Netherlands

13. SPONSORING AGENCY NAME(S) AND ADDRESS(ES)

Min. van Defensie/Defensiestaf/CIS

14. SUPPLEMENTARY NOTES

The classification designation Ongerubriceerd is equivalent to Unclassified, Stg. Confidentieel is equivalent to Confidential and Stg. Geheim is equivalent to Secret.

15. ABSTRACT (MAXIMUM 200 WORDS (1044 BYTE))

The objective of JWID '98 is to demonstrate technologies which contribute to the interoperability of C2 systems. JWID '98 has shown that the functionality of the World Wide Web and Internet technology allows to combine commercial systems and military systems into a C4I network which provides access to the digital battlefield information of various NATO partners. The exchange of information between C2 systems is however still cumbersome. Although message standards are used (e.g. AdatP-3 or OTH-G) there remain differences in implementation of these standards and differences in the datamodels used by these C2 systems. Question marks remain about the security aspects and survivability aspects of the demonstrated technologies when applied in a military environment. Also it is questioned whether military communications networks can provide sufficient bandwidth to support C4I networks.

16. DESCRIPTORS	IDENTIFIERS
Command & Control Telecommunication Message Handling	Internet

17a. SECURITY CLASSIFICATION (OF REPORT)	17b. SECURITY CLASSIFICATION (OF PAGE)	17c. SECURITY CLASSIFICATION (OF ABSTRACT)
Ongerubriceerd	Ongerubriceerd	Ongerubriceerd

18. DISTRIBUTION AVAILABILITY STATEMENT	17d. SECURITY CLASSIFICATION (OF TITLES)
Unlimited distribution	Ongerubriceerd

Distributielijst

1.	DWOO
2.	HWO-KM*
3.	HWO-KL*
4.	HWO-KLu*
5.	HWO-CO
6 t/m 15.	Ministerie van Defensie/Defensiestaf/CIS, t.a.v. Lkol F.W.J. van Weverwijk
16.	DM&P TNO-DO
17.	Directeur TNO-PML*
18.	Directeur TNO-TM*
19.	Accountcoördinator KM *
20.	Accountcoördinator KL*
21.	Accountcoördinator KLu*
22.	Accountcoördinator CO*
23 t/m 25.	Bibliotheek KMA
26.	Bibliotheek IDL
27.	KL/LAS/CIV t.a.v. Kol Ir. A.P. Coppens
28.	KLu/DOPKLu/ACIS t.a.v. Kol P. Arts
29.	KLu/DOPKLu/ACIS t.a.v. LKol Ing. C.S.M. v. Veen
30.	KM/MARSTAF/CIS t.a.v. KTZ J. Buzepol
31.	KM/DMKM/WCS/COM t.a.v. KLTZ F.K.J. Henkelman
32.	KL/DM/Systeemgroep C3I t.a.v. Kol Ir. G.H. van Haastert
33.	KL/DM/Systeemgroep C3I t.a.v. Kol Ir. W. Folkers
34.	Directeur TNO-FEL
35.	Adjunct-directeur TNO-FEL, daarna reserve
36.	Archief TNO-FEL, in bruikleen aan MPC*
37.	Archief TNO-FEL, in bruikleen aan Accountmanager KM
38.	Archief TNO-FEL, in bruikleen aan Accountmanager KL
39.	Archief TNO-FEL, in bruikleen aan Accountmanager KLu
40.	Archief TNO-FEL, in bruikleen aan Accountmanager CO
41.	Archief TNO-FEL, in bruikleen aan D.W. Fikkert
42.	Archief TNO-FEL, in bruikleen aan Ir. C.J. van Waveren
43.	Archief TNO-FEL, in bruikleen aan Ir. J.P. Dezaire
44.	Archief TNO-FEL, in bruikleen aan Ir. R. Overduin
45.	Archief TNO-FEL, in bruikleen aan Ir. H.A.M. Luiijf
46.	Archief TNO-FEL, in bruikleen aan Ir. J.F.C.M. de Jongh
47.	Archief TNO-FEL, in bruikleen aan Ir. E.C.C. van Woerkens
48.	Archief TNO-FEL, in bruikleen aan Ir. P. Schulein
49.	Archief TNO-FEL, in bruikleen aan Drs.Ing. C.W. d' Huy
50.	Documentatie TNO-FEL
51 t/m 54.	Reserve

Indien binnen de krijgsmacht extra exemplaren van dit rapport worden gewenst door personen of instanties die niet op de verzendlijst voorkomen, dan dienen deze aangevraagd te worden bij het betreffende Hoofd Wetenschappelijk Onderzoek of, indien het een K-opdracht betreft, bij de Directeur Wetenschappelijk Onderzoek en Ontwikkeling.

* Beperkt rapport (titelblad, managementuittreksel, RDP en distributielijst).