TÜBİTAK BİLGEM is a R&D center which, instead of presenting prototype solutions for informatics and security needs of its customers both from the public and private sector, adopts the principle of providing each of its customer with tailor-made solutions. Consisting of approximately 1700 staff, 80% of whom are R&D staff, TÜBİTAK BİLGEM operates on information technology, information security and advanced electronics. Based upon its experience exceeding 40 years, the center is now one of the most competent R&D centers of Turkey.

The institutions within BİLGEM have so far attained hundreds of project achievements in the fields of information security, software and telecommunication. These institutions are namely National Research Institute of Electronics and Cryptology (UEKAE), Information Technologies Institute (BTE), Advanced Technologies Research Institute (İLTAREN), Cyber Security Institute (SGE) and Software Technologies Research Institute (YTE). Thanks to the projects of the afore-mentioned institutes, Turkey has become one of the few countries declaring its technological independence in the fields of information security and informatics.

Products and solutions developed by BİLGEM have gone beyond the country’s border, being used by many European and Asian countries and NATO as well. Thanks to these very contributions of the center, Turkey is no more a country which only imports informatics and information security; but also competes with the world’s leading countries in this regard.

By means of this Catalogue, the technologies and solutions developed under our Center will be closely acquainted and easily reached by the people requiring such information.
TÜBİTAK BİLGEM'S PLACE WITHIN TÜBİTAK

BİLGEM, operating in the fields of information technologies, information security and advanced electronics, stands out as one of the most important research centers of TÜBİTAK.

TÜBİTAK BİLGEM'S HISTORY

BİLGEM, founded in 1968, is the most efficient R&D center of Turkey.

TÜBİTAK BİLGEM TECHNOLOGY AND SOLUTION CATALOGUE

TÜBİTAK BİLGEM TECHNOLOGY AND SOLUTION CATALOGUE

It was established by the Scientific and Technological Research Council of Turkey (TÜBİTAK) under the name of the Scientific and Technological Research Council of Turkey (TEKEL).

Electronics Research Unit (ERTU) was established.

Electronics and Semiconductor Technologies (ERTU) was established.

Information Technologies, Electronics and Information Security Center was established.

Informatics and Information Security Center was established.

Cyber Security Institute (CGI)

Advanced Technologies Research Institute (ATRI)

Software Technologies Research Institute (STRI) was established.

National Research Institute of Electronics and Optoelectronics (NRIEO) was established.

1963
1968
1991
1995
2010
2011
2012

TAKİTAK BİLGEM'S HISTORY

TÜBİTAK BİLGEM TECHNOLOGY AND SOLUTION CATALOGUE

TÜBİTAK BİLGEM TECHNOLOGY AND SOLUTION CATALOGUE
BİLGEM conducts technological R&D activities for the purpose of Turkey’s technological independence in the fields of information security and informatics, and for the maintenance and advancement of military and civilian information’s security and integrity.

With its 80% R&D staff, BİLGEM has institutions mainly operating in the fields of advanced electronics, information technologies, cryptology, cyber security, software technologies, information security, electronic warfare and telecommunication.
The center produces national solutions for both military and civilian needs within the context of information systems and technologies.

BİLGEM develops original and high value-added technologies in order to sustain the competitive capacity of the country/Turkey for high-tech products.
BİLGEM, with its technological laboratories forming its infrastructure, meets technological needs of the country and directs the current technology abroad.

TÜBİTAK BİLGEM TECHNOLOGY AND SOLUTION CATALOGUE
TÜBAI / FUNDAMENTAL SCIENCES RESEARCH INSTITUTE

TBAE aims at increasing the scientific research capacity of Turkey especially in mathematics and physics among fundamental sciences. It also aspires to be the leading scientific hub for the other research centers and institutes specialized in fundamental sciences in Turkey. For this end, common ground where well-qualified scientists could collaborate and have an exchange of ideas in the fields of mathematics and physics is planned to be formed. Thus, it will be possible for researchers to maintain their researches, to initiate joint scientific studies and to interact both with each other and with foreign counterparts by using the facilities of the institute.

TBAE is home to advanced-level courses, seminars, workshops, research sessions and many other scientific events. Especially young scientists and doctoral students participate in these meetings. Thanks to this, researchers can find the opportunity of seeing and facing new and current scientific problems. Such activities are also transformed to scientific publications that are of international level.

TBAE, with its rich library and computer network, aspires to make joint scientific research with the world’s leading scientific research institutions as well.
## TÜBİTAK BİLGEM TECHNOLOGY AND SOLUTION CATALOGUE

### SECURE COMMUNICATION SOLUTIONS

<table>
<thead>
<tr>
<th>No.</th>
<th>Product Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>21</td>
<td>MILSEC-4 / Secure IP Terminal</td>
</tr>
<tr>
<td>22</td>
<td>MILSEC-3 / Secure Voice Device for HF/VHF/UHF Radios</td>
</tr>
<tr>
<td>23</td>
<td>AGC-G / Gigabit Network Security Device</td>
</tr>
<tr>
<td>24</td>
<td>IPKC-EG / Gigabit Network Security Device</td>
</tr>
<tr>
<td>25</td>
<td>IPKC-G / IP Crypto Device</td>
</tr>
<tr>
<td>26</td>
<td>IPKC-EG-YM / IPKC-EG Management Center</td>
</tr>
<tr>
<td>27</td>
<td>IP-YM / IP Crypto Management Center</td>
</tr>
<tr>
<td>28</td>
<td>IP-AYM / IP Key Management Center</td>
</tr>
<tr>
<td>29</td>
<td>SIR / Secure USB Flash Memory Storage Device</td>
</tr>
<tr>
<td>30</td>
<td>SIR-S / Secure Portable Hardisk</td>
</tr>
<tr>
<td>31</td>
<td>VERBAR / Portable Offline Crypto Device</td>
</tr>
<tr>
<td>32</td>
<td>SNC / Synchronous Data Encryption Device</td>
</tr>
<tr>
<td>33</td>
<td>MIS / Message Operating System</td>
</tr>
<tr>
<td>34</td>
<td>BARBAROS / Real Time Radio Network System</td>
</tr>
<tr>
<td>35</td>
<td>TAGEC / Radio Communication Gateway - RCG</td>
</tr>
<tr>
<td>36</td>
<td>MSK / FF-Identification Friend or Foe Mode 4/5 Crypto Unit</td>
</tr>
<tr>
<td>37</td>
<td>GKTURK-1 / Satellite Communication Crypto System</td>
</tr>
<tr>
<td>38</td>
<td>DOAK KEY GENERATOR / Hardware Security Module</td>
</tr>
<tr>
<td>39</td>
<td>DOAK HSM / Hardware Security Module</td>
</tr>
<tr>
<td>40</td>
<td>FIC-2 / Secure Fax Device</td>
</tr>
<tr>
<td>41</td>
<td>FASD-1 / Fax Analog-Digital Converter</td>
</tr>
<tr>
<td>42</td>
<td>GMS / Secure Messaging System - SMS</td>
</tr>
<tr>
<td>43</td>
<td>GMS / Secure Messaging Client - SMC</td>
</tr>
<tr>
<td>44</td>
<td>GMM / Secure Directory System Server</td>
</tr>
<tr>
<td>45</td>
<td>SRC155A / Point-to-Point SDH/SONET/Ethernet Digital Radio</td>
</tr>
</tbody>
</table>

### CRYPTO KEY MANAGEMENT SYSTEMS

<table>
<thead>
<tr>
<th>No.</th>
<th>Product Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>47</td>
<td>SRC400 / New Generation High Speed Digital Radio Link Device</td>
</tr>
<tr>
<td>48</td>
<td>SRC-YM / Digital Radio Device Management Center</td>
</tr>
<tr>
<td>49</td>
<td>MDSKX-E1 / Audio Multiplexing Device</td>
</tr>
<tr>
<td>50</td>
<td>SATEL / Underwater Telephone</td>
</tr>
<tr>
<td>51</td>
<td>KTDS / Level Shifter and Driver IC</td>
</tr>
<tr>
<td>52</td>
<td>KAMI / Cryptographic Algorithms, Protocol &amp; Architecture Design</td>
</tr>
</tbody>
</table>

### SMART CARD AND ID VERIFICATION SYSTEMS

<table>
<thead>
<tr>
<th>No.</th>
<th>Product Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>65</td>
<td>NATIONAL IDENTITY CARD / TR &amp; KKTC Identity Card</td>
</tr>
<tr>
<td>66</td>
<td>AVS / Smart Card Operating System</td>
</tr>
<tr>
<td>67</td>
<td>UKTUM / National Smart Card IC</td>
</tr>
<tr>
<td>68</td>
<td>GMM / Embedded Secure Module</td>
</tr>
<tr>
<td>69</td>
<td>AVS e-PASSPORT / Electronic Passport</td>
</tr>
<tr>
<td>ELECTRONIC CERTIFICATION MANAGEMENT SOLUTIONS</td>
<td></td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>79. ESYA SM / Certification Authority</td>
<td></td>
</tr>
<tr>
<td>80. KEREN / Public Key Infrastructure Desktop Client</td>
<td></td>
</tr>
<tr>
<td>81. ESYA API / Electronic Signature Libraries</td>
<td></td>
</tr>
<tr>
<td>82. ESYA 2D Server / ESYA Timestamp Server</td>
<td></td>
</tr>
<tr>
<td>83. INDAGER / Implementation of Desktop Signing</td>
<td></td>
</tr>
<tr>
<td>84. SECURE PDF / Implementation of PDF Signing / Encryption</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ELECTRONIC INTELLIGENCE SOLUTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>87. SGs / Spectrum Monitoring System</td>
</tr>
<tr>
<td>88. EDF018A / Broadband ELINT Frequency Converter</td>
</tr>
<tr>
<td>89. FDG00A / IF Converter</td>
</tr>
<tr>
<td>90. HF/F / HF Record and Playback Device</td>
</tr>
<tr>
<td>91. KAGIS / Record, Playback &amp; Review System</td>
</tr>
<tr>
<td>92. MFID18B / Microwave Frequency Downconverter System</td>
</tr>
<tr>
<td>93. YTA-018B / Software-Based Wideband Receiver</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>RAILWAY TRANSPORTATION SYSTEMS</th>
</tr>
</thead>
<tbody>
<tr>
<td>94. YTA-M901A / Software-Based HF/VHF/UHF Receiver</td>
</tr>
<tr>
<td>95. YTS2000 / Non-Linear Junction Detector 2000MHz</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DATA VALUATION SOLUTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>96. IFON SUITE / Forensic Image Enhancement &amp; Restoration Software</td>
</tr>
<tr>
<td>100. Allied Radio Frequency Computer Aided Data Exchange &amp; Spectrum Management Information Repository Online</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CIVIL AVIATION SOLUTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>101. AIRS / Aircraft Tracking System</td>
</tr>
<tr>
<td>102. HACF / Aircraft Tracking Device</td>
</tr>
<tr>
<td>103. ATCMS / Air Traffic Control Tower and Radar Simulator</td>
</tr>
<tr>
<td>104. ATCGES / Air Traffic Controller Selection System</td>
</tr>
<tr>
<td>105. KUSPACD / Bird-Aircraft Collision Avoidance Radar System</td>
</tr>
<tr>
<td>108. GOMSIS / Digital Radar Signal Processing Card</td>
</tr>
<tr>
<td>110. MGR / Air Traffic Surveillance Radar</td>
</tr>
<tr>
<td>111. NTERMACADE / Radar Test Software</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>RAILWAY TRANSPORTATION SYSTEMS</th>
</tr>
</thead>
<tbody>
<tr>
<td>113. STKMK / Railway Traffic Control Center</td>
</tr>
<tr>
<td>114. DAS / Railway Workstation System</td>
</tr>
<tr>
<td>115. TRENSIM / E43000 Locomotive Simulator</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ELECTRONIC DOCUMENT AND ARCHIVING SOLUTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>119. EBRU / Document Tracking System</td>
</tr>
<tr>
<td>120. SKCAS / Digital Storage Archive and Analysis System</td>
</tr>
<tr>
<td>121. e-BILGEM / Archive Management System</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ELECTRO-OPTICS AND LASER SYSTEMS</th>
</tr>
</thead>
<tbody>
<tr>
<td>125. UMKC / National Marker Control System</td>
</tr>
<tr>
<td>126. FORENCO-XP-40100 / Next Generation Questioned Doc. Exam. Tool</td>
</tr>
<tr>
<td>127. QDF / Quadrant Photodetectors</td>
</tr>
<tr>
<td>128. GEZK / Real-Time IR Track Prediction and Management System</td>
</tr>
<tr>
<td>129. FGKS / Fiber Optic Cable Audit System</td>
</tr>
<tr>
<td>130. EMBC / Electro-Optical Modulation Detection System</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CYBER SECURITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>133. STAMPS / Centralized Cyber Threat Sensor System</td>
</tr>
<tr>
<td>134. SORI / Cyber Space Trap System</td>
</tr>
<tr>
<td>135. VKOS / Data Leakage Prevention System</td>
</tr>
<tr>
<td>136. SIBERMEYDAN CTF / Cyber Security Sm. and Comp. Environment</td>
</tr>
<tr>
<td>137. Cyber Security Services</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>UNDERWATER DEFENSE SYSTEMS</th>
</tr>
</thead>
<tbody>
<tr>
<td>141. DABIS / Submarine Battery Monitoring System</td>
</tr>
<tr>
<td>143. D purchaser / Submarine Tactiscal Simulator</td>
</tr>
<tr>
<td>145. SEMADES / Energetic-Submarine Data Package Gen.</td>
</tr>
<tr>
<td>146. DOAKA / BTM / Acoustic Decoy Development For Submarine / Quest Of Acoustic Reactions For Anti-Torpedo</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DEFENSE SYSTEM SOLUTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>151. DRT TABLE / Digital Dead Reckoning Table</td>
</tr>
<tr>
<td>152. GIS / Real-Time Operating System</td>
</tr>
<tr>
<td>153. ETMTS-2 / Hand-Held Mine Detection System</td>
</tr>
<tr>
<td>154. TAKISS / Tactiscal Training System</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ELECTRONIC WARFARE SYSTEM SOFTWARE SOLUTIONS AND SYSTEM SOLUTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>157. SIMA / Simulation Modelling Infrastructure</td>
</tr>
<tr>
<td>158. MARSays / Management and Analysis of Radar Spectrum Sys.</td>
</tr>
<tr>
<td>159. IRGOMAS / IR Meas. Data Base Man. and Analysis Software</td>
</tr>
<tr>
<td>161. RASES / Radar Cross Section Computation</td>
</tr>
<tr>
<td>162. Electronic Warfare Systems Design &amp; Development</td>
</tr>
<tr>
<td>163. Electronic Warfare Analysis, Test &amp; Evaluation</td>
</tr>
</tbody>
</table>
TUBITAK BİLGEM / CONTENTS

HIGH POWER MICROWAVE SYSTEMS
161 CATHODE / High Power Microwave Technologies
166 TWT / Traveling Wave Tube Technologies
169 Magnetron Technologies

CLOUD COMPUTING SOLUTIONS
173 OANLAB / National Search Engine Prototype
174 B3LAB / Safe Product Family
175 B3LAB / Big Data Analytics Solutions

e-GOVERNMENT PLANNING SERVICES
179 e-Government Planning Services
180 Institutional Information and Communications Technologies (IICT) Capacity Analysis and IT Strategy Formulation
181 Current Status Analysis and Roadmap Development
182 Developing Technical Specifications
183 Technical Consultation and Process Guidance
184 Software Engineering Process Improvement

e-GOVERNMENT PROJECT MANAGEMENT SERVICES
187 e-Government Project Management Services
188 Investment, Incentive and Support Management Systems
189 Sectoral Supervising and Monitoring Management Systems
190 Social Relief and Services Management Systems
191 Geographical Information Systems

SECURE COMMUNICATION SOLUTIONS

e-GOVERNMENT POLICY MONITORING AND EVALUATION SERVICES
195 e-Government Policy Monitoring and Evaluation Services

e-GOVERNMENT ARCHITECTURE OFFICE SERVICES
199 e-Government Architecture Office Services

ADVANCED TECHNOLOGIES RESEARCH INFRASTRUCTURE
201 ATAM / Antenna Test And Research Center
202 Information Security Risk Analysis
203 COMSEC / Communications Security Laboratory
204 KDFM / Speech & Language Technologies Laboratory
206 Electro-Optics & Laser Systems Laboratory
206 IGAM / Advanced Genomics and Bioinformatics Research Laboratory
207 Biotechnological Devices and Systems Development Laboratory
208 KAMTAM / CATHODE and Microwave Vacuum Tube Research Laboratory
209 CRYPTANALYSIS / Cryptanalysis Laboratory
210 KYAS / Spherical Near Field Measurement System Laboratory
211 OKTEM / Common Criteria Test Center
212 RADAR-AGL / Radar Research & Development Laboratory
213 RAPPSIM / Radar Performance and Signature Analysis Center
214 RF-AGL / RF Research & Development Laboratory
215 TEMPEST Test Laboratory
216 YITAL / Semiconductor Technologies Research Laboratory
217 YTKDM / Software Test and Quality Assessment Center
218 YITAL / Wireless Telecommunication Technologies Research Laboratory

* As a result of ongoing research and development, the specifications in this catalogue and its content may change without prior notice.
SECURE COMMUNICATION SOLUTIONS

TÜBİTAK BİLGEM TECHNOLOGY AND SOLUTION CATALOGUE

SECURE COMMUNICATION SOLUTIONS

SECURE IP TERMINAL

TÜBİTAK BİLGEM TECHNOLOGY AND SOLUTION CATALOGUE

SECURE COMMUNICATION SOLUTIONS

SECURE IP TERMINAL

MILSEC-4 secure IP terminal offers state-of-the-art capabilities for both secure and non-secure calls over IP and PSTN networks, providing interoperability with legacy solutions while realizing the future of secure and reliable communications. MILSEC-4 devices can be configured, monitored, and updated via the Secure Management Center (SMC) over IP networks using NATO SCIP protocol. Unlike earlier generation secure communication devices, MILSEC-4 is capable of Over the Network Keying (OTNK) via SMC.

MILSEC-4 devices are interoperable with MILSEC-1A, MILSEC-2, MILCEP K1, and MILCEP K2 secure phones. MILSEC-4 provides a smooth transition while replacing MILSEC-1A and MILSEC-2 legacy phones during the migration of PSTN to IP networks.

MILSEC-4 terminal offers a new generation secure communication solution for IP and PSTN networks, at the same time compatibility with legacy phones, which assures seamless communication service.

FEATURES

▪ Secure communications over IP and PSTN networks
▪ Secure end-to-end voice, video, and data transfer
▪ NATO SCIP compliant
▪ Interoperable with commercial SIP products
▪ Interoperable with MILCEP and MILSEC secure phones
▪ National and AES crypto algorithms
▪ Remote configuration/software updates
▪ Easy-to-use interface with LCD touchscreen

SECURE COMMUNICATION SOLUTIONS

MILSEC-4 / SECURE IP TERMINAL

SECURE COMMUNICATION SOLUTIONS

MILSEC-4 / SECURE IP TERMINAL

SECURE COMMUNICATION SOLUTIONS

MILSEC-4 / SECURE IP TERMINAL

SECURE COMMUNICATION SOLUTIONS

MILSEC-4 / SECURE IP TERMINAL

SECURE COMMUNICATION SOLUTIONS

MILSEC-4 / SECURE IP TERMINAL

SECURE COMMUNICATION SOLUTIONS

MILSEC-4 / SECURE IP TERMINAL

SECURE COMMUNICATION SOLUTIONS

MILSEC-4 / SECURE IP TERMINAL

SECURE COMMUNICATION SOLUTIONS

MILSEC-4 / SECURE IP TERMINAL

SECURE COMMUNICATION SOLUTIONS

MILSEC-4 / SECURE IP TERMINAL

SECURE COMMUNICATION SOLUTIONS

MILSEC-4 / SECURE IP TERMINAL
SECURE COMMUNICATION SOLUTIONS

SECURE VOICE SOLUTION FOR HF/VHF/UHF TACTICAL COMMUNICATIONS

MILSEC-3 is a half-duplex secure communication device that can transmit and receive plain and cipher voice or data over HF/UHF/VHF radio links. Due to its configurable interface, it can work with many voice, data and radio devices. Additionally, MILSEC-3 can communicate with other MILSEC-3 equipment using the national crypto algorithm and communicates with KY18 and KY100 devices by using NATO Crypto algorithm.

SECURITY FEATURES

- National algorithm (National mode)
- NATO Crypto Mode
- Preservation of crypto keys up to 60 days Emergency backup mode

ENVIRONMENTAL CONDITIONS

- Operating temperature: -40°C / +71°C
- Storage temperature: -57°C / +85°C
- Shock: MIL-STD-810E, Method 516.4
- Vibration: MIL-STD-810F, Method 514.5
- Gunfire vibration: MIL-STD-810F, Method 519.5
- Altitude: MIL-STD-810F, Method 500.4
- Humidity: MIL-STD-810E, Method 507.3
- Salt fog: MIL-STD-810F, Method 509.4
- Acceleration: MIL-STD-810F, Method 513.5
- Solar radiation: MIL-STD-810F, Method 505.4
- Rain: MIL-STD-810F, Method 506.4
- Sand and dust: MIL-STD-810F, Method 510.4
- Explosive atmosphere: MIL-STD-810F, Method 511.4

SECURE COMMUNICATIONS OVER GIGABIT NETWORKS

AGC-G provides secure communications at network level between IP local area networks, which communicates over insecure networks. The device is located between local network and edge router and establishes a secure gateway. It provides data confidentiality, authentication and integrity. AGC-G has a data processing capacity of up to 1.2 Gbps.

SECURITY SPECIFICATIONS

- "RESTRICTED" level data security
- Authentication
- Data integrity
- Emergency-erase feature against tampering
- Hardware-based random number generator
- Encryption: AES-CTR
- Authentication: AES-OMAC
- Key exchange: ECDH
- Signing: ECDSA
- Role-based access control
- Smart-card-based Crypto Ignition Key and User Card
- Saving event log, alarm log and transaction log
- Online key loading from Security Management Center

GIGABIT NETWORK SECURITY DEVICE

TECHNICAL SPECIFICATIONS

- Provides secure communications between IP/IPv6/IPv4 networks over TCP/IP stacks
- Enables gigabit data transmission from one point to multipoint simultaneously
- Performance: 600 Mbps (red to red, one direction)
- 2000 automatic/manual tunneling
- IPv4, IPv6, TCP, UDP, ICMP, SNMP, FTP
- 2x 10/100/1000 Mbps Gigabit Ethernet (IEEE 802.3), auto sense, auto crossover
- Command-based configuration by local management (console) port and user-friendly command set
- SNMP-based remote management by the Security Management Center
- Configuration Backup
- Local and Security Management Center based software update
- EMI/EMC and TEMPEST certified
GIGABIT NETWORK SECURITY DEVICE

SECURE COMMUNICATIONS ON GIGABIT NETWORKS
IPKC-EG provides secure communications of network level between IP local area networks. The device is located between the local network and edge-router and establishes a secure gateway. It provides data confidentiality, authentication and integrity. These services are provided by using national cryptographic algorithms. IPKC-EG is network compatible with legacy IPKC-E devices. With its high data throughput of 600 Mbps, it can simultaneously communicate with several legacy IPKC-E IP Crypto devices at the network.

TECHNICAL SPECIFICATIONS
▪ Provides secure communications of IP/Ethernet Networks over insecure and unprotected networks
▪ One point to multipoint gigabit data transmission
▪ Performance: 300 Mbps (red to red, one direction)
▪ 2000 automatic/manual tunneling
▪ IPv4, IPv6, TCP, UDP, ICMP, SNMP, FTP
▪ 2x 10/100/1000 Mbps Gigabit Ethernet (IEEE 802.3)
▪ Command-based configuration by local management (console) port, user-friendly command set
▪ Configuration backup
▪ Local and network-based software update

SECURITY SPECIFICATIONS
▪ "SECRET" level data security
▪ Authentication
▪ Data integrity
▪ Emergency-erase feature against tampering
▪ Hardware-based implementation
▪ Hardware-based random number generator
▪ Encryption: AES-CTR
▪ Authentication: AES-GMAC
▪ Key exchange: ECDH
▪ Signing: ECDSA
▪ Automatic key exchange with IKE protocol
▪ X.509 certificate-based body
▪ Two-stage access control with smart-card and password, role-based device access control
▪ Smart-card based Crypto Ignition Key and User Card
▪ Saving Event Log, alarm log and transaction log
▪ Offline key loading at MILAY mode by using key loader
▪ Online key loading by Security Management Center
▪ Backward compatibility with IPKC-E
▪ System and Security Management Center

IP CRYPTO DEVICE

SECURE COMMUNICATIONS ON GIGABIT NETWORKS
AGC-G provides secure communications between IP local area networks which communicate over insecure networks. The device is located between local network and edge-router and establishes a secure gateway. It provides data confidentiality, authentication and integrity. These services are provided by using national algorithms. AGC-G has a data throughput capacity of up to 310 Mbps.

TECHNICAL SPECIFICATIONS
▪ Provides secure communication of IP/Ethernet Networks over insecure and unprotected networks
▪ Enables gigabit data transmission from one point to multipoint simultaneously
▪ Performance: 155 Mbps (red to red, one direction)
▪ 2000 automatic/manual tunneling
▪ IPv4, IPv6, TCP, UDP, ICMP, SNMP, FTP
▪ 2 x 10/100/1000 Mbps Gigabit Ethernet (IEEE 802.3)
▪ Command-based configuration by local management (console) port, user-friendly command set
▪ Configuration backup
▪ Local and network-based software update
▪ EMI/EMC and TEMPEST featured

SECURITY SPECIFICATIONS
▪ "SECRET" level data security
▪ Authentication
▪ Data integrity
▪ Emergency-erase feature against tampering
▪ Hardware-based implementation
▪ Hardware-based random number generator
▪ Encryption: AES-CTR
▪ Authentication: AES-GMAC
▪ Key exchange: ECDH
▪ Signing: ECDSA
▪ Automatic key exchange with IKE protocol
▪ X.509 certificate-based body
▪ Two-stage access control with smart-card and password, role-based device access control
▪ Smart-card based Crypto Ignition Key and User Card
▪ Saving Event Log, alarm log and transaction log
▪ Offline key loading in MILAY mode by using key loader
▪ Online key loading by EKADAS-Electronic Key Generation and Distribution System and Security Management Center

IPKC-E / GIGABIT NETWORK SECURITY DEVICE

SECURE COMMUNICATION SOLUTIONS

IPKC-G / IP CRYPTO DEVICE

SECURE COMMUNICATION SOLUTIONS
IPKC-EG-YM

SECURE COMMUNICATION SOLUTIONS

IPKC-EG MANAGEMENT CENTER

FEATURES
- Remote management of devices from a single point
- Multi browser support
- Client-server architecture
- User management
- Log and report generation
- Online backup
- E-mail notification
- Device performance management with throughput monitoring
- Graphical monitoring of device MIBs (network parameters)
- Alarm management and reporting
- Device log management with SYSLOG support
- Built-in FTP server for file transfers to/from device

REMOTE MANAGEMENT
IPKC-EG Management Center (IPKC-EG-YM) is a server based system with a web based user friendly interface which enables administrators to manage IPKC-EG IP Encryptors centrally. It is capable of managing devices, configurations, alarms, and logs in a secure manner. IPKC-EG-YM has advanced features, which enables network administrators to perform their daily operations easily.

SECURITY FEATURES
- Smart card based user authentication
- Role based user authorization
- SSLv3
- SNMPv3
- Dedicated IPKC-EG used for management communication

IP-YM

SECURE COMMUNICATION SOLUTIONS

IP CRYPTO MANAGEMENT CENTER

FEATURES
- Remote management of devices from a single point
- Multi browser support
- Web based AJAX based user interface
- Client-server architecture
- Multi user support
- Role and permission based user management
- Log and report generation
- E-mail notification
- Device Alarm, Monitoring and Log Management
- Device performance management with throughput monitoring
- Graphical monitoring of device MIBs (network parameters)
- Alarm management and reporting
- Device log management with SYSLOG support
- Built-in FTP server for file transfers to/from device

REMOTE MANAGEMENT
IP-YM is a server based system with a web based user friendly interface which enables administrators to manage IPKC-G and AGC-G IP Encryptors centrally. It is capable of managing devices, configurations, alarms, and logs in a secure manner. IP-YM has advanced features which help network administrators to perform their daily operations easily.

SECURITY FEATURES
- Smart card based user authentication
- Role based user authorization
- SSLv3
- SNMPv3
- Dedicated IPKC-G/AGC-G used for management communication
- Grouping of devices in a hierarchical manner
- Tree based view of managed devices and groups
- Periodic device connection checking
- Automatic device recognition and management
- Device remote PING
- On demand device date-time configuration
- Detailed device IPSEC configuration management
- Device IPSEC configuration error detection and reporting
- Remote device software upgrade
- Device configuration backup and recovery
- Key groups management in participation with Key Management Center
- Device network configuration management
- Device network elements management
- Device local user management
SECURE COMMUNICATION SOLUTIONS

IP-AYM / IP KEY MANAGEMENT CENTER

IP-AYM performs IPKC-G/AGC-G devices key management operations centrally. IP-AYM is compatible with IPKC-G/AGC-G Management Center (IP-YM). The Symmetric and Asymmetric Keys of IPKC-G/AGC-G devices are generated by IP-AYM. For key generation, IP-AYM uses IPKC-G/AGC AU&IC device. Distribution, accounting, and management functions are included. Web based user interface enables management from any secure location. The system has been designed to operate on a 7/24 basis and physical and geographical backup is possible. The design of the architecture enables expandability.

GENERAL FEATURES
▪ Key generation by AU&IC device
▪ Key Distribution
▪ Key account management
▪ Key Destruction
▪ Certificate generation by AU&IC device
▪ Online certificate distribution
▪ Certificate account management
▪ Certificate Revocation List and erase management
▪ User account management and update operations
▪ Dynamic role management
▪ Smart card-based user identification
▪ User and system logs
▪ Geographical and physical backup

MINIMUM REQUIREMENTS
▪ 3 GHz Dual Core Processor
▪ 4 Gbyte RAM
▪ 4 Gbyte Hardisk
▪ PostgreSQL
▪ Windows 7/2008 Server
▪ CPU, RAM and Hardisk requirements may vary according to number of devices managed

SECURE USB FLASH MEMORY STORAGE DEVICE

SIR is an encrypted USB flash memory storage device which protects data fulfilling the security requirements on a full hardware based architecture, operated by a single user. The device has the storage capacity options of 2 GB/4 GB/8 GB flash memory with the ability of 10 MB/s write & read speeds.

The device protects data stored on itself, not while reading from or writing to the host.

SIR provides security for a single user. No other user can access the protected data using his/her own user token. Additional security measures like emergency erase and tamper switches are employed in the device.

The user is informed about any change about the status of the device by the help of visual indicators (login, key pressed, token, USB connected warnings) and an audio indicator. There is a write protect switch on the device to disable writing to the device if needed. The device is powered from single USB interface of the host computer. The embedded battery is charged via the USB interface of the host to preserve key memory for maximum 6 months without any power.

Designed to be commercial grade, tactical, ruggedized, portable equipment. SIR is fully compatible with the COMSEC, EMI/EMC, TEMPEST standards.

OPERATING SYSTEMS
▪ Platform independent (Offline mode) - Windows, Linux platforms
▪ Windows 7/VISTA/XP/2000, Linux Kernel 2.4 and newer versions

FEATURES
▪ 2 GB/4 GB/8 GB Data Storage Capacity
▪ Plug & Play
▪ Dimensions: 51 x 91 x 14 mm
▪ Weight: 90 gr

USER INTERFACE
▪ 12-key piezo ceramic keypad, 4 two coloured indicators
▪ 1 buzzer, 1 emergency erase switch, 1 write protect switch
▪ 1 user token reader slot

SECURE COMMUNICATION SOLUTIONS

SECURE USB FLASH MEMORY STORAGE DEVICE
VERISAR is a portable single user offline file encryption device. An unsecured computer can be used for classified message/file encryption and decryption by using VERISAR.

VERISAR contains a secured Linux-Based operating system to establish a secure working environment for cryptographic operations and this operating system is kept in encrypted partition.

When user wants to encrypt or decrypt a file, what s/he needs is a USB bootable computer (desktop or notebook). Host computer will be booted from encrypted Linux-Based read-only operating system. All network capabilities of the host computer will then be disabled by default.
**SVKC**

**SYNCHRONOUS DATA ENCRYPTION DEVICE**

**Feasible Solutions to Achieve Your Communication and Security Goals**

SVKC provides secure synchronous communication over E1 PCM Links and leased lines at high data rates up to 2 Mbit/s. With ITU-T V.11 (RS-530) compatible interfaces, SVKC is able to transmit and receive synchronous data at up to 2 Mbit/s multiples of 64 Kbits.

SVKC also has ITU-T G.703 compatible interfaces. It encrypts and decrypts framed or unframed data at 2 Mbit/s over E1 PCM Links.

Traffic keys are loaded into SVKC with either MILAY-1 (Fill Gun) or TELAYS (Electronic Key Management System).

**Interfaces**

- ITU-T G.703 compatible interfaces (64 Kbit/s)
- ITU-T V.11 (RS-530) compatible interfaces (up to 2 Mbit/s multiples of 64 Kbit/s)

**Security Features**

- National algorithm
- Periodically changing traffic keys
- Encryption of all 32 channels of an E1 PCM link
- Frameless or framed operation of the E1 PCM interface
- Selecting of clock source (DTE clock or DCE clock) in synchronous mode

**MIS**

**MESSAGE OPERATING SYSTEM**

**Feasible Solutions to Achieve Your Communication and Security Goals**

MIS is a system developed to satisfy tactical and strategic messaging requirements. This national military system has been integrated with other solutions in order to be used within all national and NATO military messaging environments.

**Supported Standards**

- **ACP 127**
  - ACP127 message standard transmission can be done in accordance with desired configuration via required number of RATT channels.
  - Full functional ACP127 message preparation terminal application

- **STANAG 4406 & ANNEX E (X.400)**
  - Message preparation and storage systems for STANAG 4406 and X.400 standards
  - Compatible with ACP142 (Proc)
  - STANAG S0660 message transport layer support
  - ACP127 - PT172 conversion functions

- **X.500 - Directory Access Protocol (DAP/LDAP)**
  - The provision of address and user record information within the directory hierarchy.

- **STANAG 5066**
  - STANAG 5066 compatible Data Link Protocol
  - BRASS compatible with infrastructure of Mialos Release and Ship-Shore.

**Other Features**

- High availability: Multiple MIS servers can be configured to function as master-backup setup. In this scenario, the backup system takes over automatically, as soon as the master system becomes unavailable.
- Single Message Box: All messages coming from X.400, HMTP, SMTP, ACP127 systems are collected and displayed in one single inbox.
**Simple and Comprehensive Communication Applications**

**HF E-Mail**
- Application enabling internet e-mail applications (SMTP) to communicate via HF.
- **HF Operator Orderwire Chat**
  - Compatible with STANAG 5066 Annex F Chat
  - Supports location tracking and chat groups in addition to STANAG 5066 specification
  - Supports plain text messages as an XMPP client (requires HFXMPP)

**MISMaps**
- Provides map services for MIS applications

**GeoPredictor**
- Calculates optimum medium, frequency and antenna for telecommunication between two elements
- Classifies different media such as HF, VHF, UHF, Ku Band, satellite and optical link
- Supports prioritization of data to be transmitted in accordance with its content
- Requires radio hardware, location, and actual environment conditions information about the other element
- Drives 2G and 3G ALE systems directly
- Capable of getting remote information via the integration with HFChat application

**Virtual DTE**
- Enables the concurrent usage of a single radio equipment with different applications
- Distributed data collection from different sources such as synchronous, asynchronous, packet data to different applications automatically
- **VDTE** enables the usage of base HF and VHF channels with maximum efficiency

**HFXMPP**
- Tactical Chat Gateway
- VoIP - Voice over HF
- Provides secure voice messaging over line broadcast lines.

**COSS - STANAG 5066 Serial Channel Emulator**
- Provides the ARQ transfer of serial channel data via STANAG 5066 protocol

**BFTP - Binary File Transfer**
- File transfer protocol over HF and VHF radio links.

**VoHF - Voice Over HF**
- Provides secure voice messaging via HF.

**COSS - STANAG 5066 Serial Channel Emulator**
- Provides the ARQ transfer of serial channel data via STANAG 5066 protocol

**BFTP - Binary File Transfer**
- File transfer protocol over HF and VHF radio links.

**GeoMESH**
- It is a cellular network system enabling the selection of the next element to which the data will be transferred based on information such as location and available radio hardware. GeoMESH provides dynamic routing over the network.
- GeoMESH can use any communication equipment to establish communications into any direction. For example, the pictures sent by field master can be transmitted via any radio network as mentioned above.

**BARBAROS**
- In NATO Use

**Intra-BARBAROS**
- BARBAROS is a radio communication solution, which integrates both moving and stationary elements into one communication network to provide transmission of real-time data. It aims at the establishment of a network among the elements, of which the location and communication capabilities are known, to transfer the data over the network.

**BARBAROS Data Link**
- Transfer of all types of data to other ends using multi-mode addressing

**Supported Standards**

**Geosafe**
- Provides secure voice messaging over line broadcast lines.

**GeoMESH**
- It is a cellular network system enabling the selection of the next element to which the data will be transferred based on information such as location and available radio hardware. GeoMESH provides dynamic routing over the network.
- GeoMESH can use any communication equipment to establish communications into any direction. For example, the pictures sent by field master can be transmitted via any radio network as mentioned above.

**Intelligent Relay**
- Enables the transfer of data to the receiver by routing the data from node to node.

**BARBAROS**
- In NATO Use

**Intra-BARBAROS**
- BARBAROS is a radio communication solution, which integrates both moving and stationary elements into one communication network to provide transmission of real-time data. It aims at the establishment of a network among the elements, of which the location and communication capabilities are known, to transfer the data over the network.
TAGEC is a radio communication solution combining mobile and stationary elements in a single network. It aims at the establishment of a network among the elements, which the location and communication capabilities are known, to transfer the data over the network.

- It is a message transmission gateway between strategic and tactical fields to transfer messages between these two domains without the need of human intervention
- It provides server services with advanced routing and protocol conversion capabilities at transmission, network and application layers
- It is a router and gateway device providing tactical field communication services for networked environments enabling generation and display of message data at different systems
- It supports low speed satellite (Globalstar, Iridium and widespread DVB-RCS services besides HF VHF/UHF radio links
- Provides fax and voice transmission and supports GSM/GPRS/HSDPA cellular and PSTN networks
- Has PSTN dial-up server and client capabilities
- Has full-fledged IP network gateway support and seamless switch between available service providers. (TAGEC device needs to be present at both ends)
- Enables efficient usage of network with automatic protocol conversion and compression support between network media
- Supports various applications like EKMS-308, DS-101 Key Fill Interface
- Supports other routers such as STANAG 5066 and STANAG 4538
- Supports various network interfaces such as radio, Ethernet and GSM
- Supports various communication interfaces for modem and radio control
- Supports various security protocols such as IP, SMTP, STANAG 5066 Annex F applications (HFCHAT, HF MAIL, HF BFTP, IPCLIENT) and XMPP
- Supports seamless transmission of AIS/WAIS data with compression
- Supports various applications for file transfer over file servers
- Provides gateway support to different network environments such as radios, Ethernet and GSM
- Supports automatic protocol conversion between networks
- Supports various security protocols such as IP, SMTP, STANAG 5066 Annex F applications (HFCHAT, HF MAIL, HF BFTP, IPCLIENT) and XMPP
- Supports various applications for file transfer over file servers
- Provides gateway support to different network environments such as radios, Ethernet and GSM

SUPPORTED STANDARDS
STANAG 5066 - 4308 ALE & DLP protocols
STANAG 4446 (X-KO) Message Transfer (MTM)
EN 14179-4/5 extender

FEATURES
- Plug-in Crypto
- STANAG 4193 compliant
- National Mode/NATO Mode Crypto Algorithm
- Mode 4 Encrypt/Decrypt
- Mode 5 Encrypt/Decrypt
- EN 14179-4/5 extender
- MIL-STD-461E (EMC)
- MIL-STD-41611 (EMC)
- 6 months of key storage

ENVIRONMENTAL
- Fully compliant with MIL-STD-810F/G
- Operating Temperature: -40°C to +71°C
- Storage Temperature: -55°C to +85°C
- Shock: 10g
- Vibration: 500 m/s² max (20Hz-20kHz)
- Altitude: 12,000 ft max (3658 m)
- Humidity: 95% @ 60°C and 95% @ 20°C
- Salt Fog
- Rain (Drip)
- Dust
GOKTURK-1

SATELLITE COMMUNICATION CRYPTO SYSTEM

SATELLITE COMMUNICATION CRYPTO SYSTEM

SECURE COMMUNICATION SOLUTIONS

SECURE COMMUNICATION SOLUTIONS

DIRAK KEY GENERATOR

HARDWARE SECURITY MODULE

SECURE COMMUNICATION SOLUTIONS

DIRAK RSA2048

DIRAK Series Hardware Security Module (HSM) is a module with a PCIe x1 module interface, developed to realize high-performance and secure encryption, signing, signature verification, cryptographic operations, such as getting, sending, and archiving data.

High security is provided for the device generated and stored in the module with its attack resistant architecture. Critical security operations such as user authentication, software updates, backup and initialization are performed after national smart card AKIS-based access authorization, which reduces potential security risks to a minimum. The module possesses Common Criteria EAL4+ security certificate.

The processing power of the RSA2048 version of the module has been dedicated for RSA2048 key-pair generation. The quality tests of the generated key-pairs are being done in accordance with June 2009 release of FIPS 186-3 standard. Quality tests of the real noise generated by the module are being done in accordance with FIPS 140-2 standard and the data is stored in secure memory. All noise data requirements including the functions performed on the software library of the module is satisfied by true noise generator. With these properties, RSA2048 version of the hardware security module is an ideal solution for high-performance RSA2048 key-pair generation requirements.

FEATURES

▪ National HSM solution
▪ Nationally certified noise generator
▪ National smart card (AKIS)-based authentication
▪ Secure storage medium for cryptographic key and data
▪ Secure backup and restore
▪ Common Criteria EAL4+ certified embedded software
▪ PCIe x1 interface
▪ 2 x USB 2.0 interface
▪ Protected metal casing
▪ 4 x tamper detection sensors
DIRAK HSM
HARDWARE SECURITY MODULE

DIRAK HSM
DIRAK Series Hardware Security Module (HSM - Hardware Security Module) is a module with a PCIEx1 module interface, developed to realize high-performance and secure encryption, signing, signature verification, cryptographic operations such as hashing/oversign.

High security is provided for the data generated and stored on the module with its attack-resistant architecture. Critical security operations such as user authentication, software updates, backing up and initialization are performed after national smart card AKIS based access authorization, which reduces potential security risks to a minimum. The module possesses Common Criteria EAL4+ security certificate.

The processing power of the PKCS11 version of the module has been optimized for high-performance signing and signature verification operations of PKCS11. Since the performance and security of RSA2048 signing and verification function is critical, this function has been relocated on hardware on FPGA. Quality tests of the real noise generated by the module are being done in accordance with FIPS 140-2 standard and the data is stored in secure memory. All noise data requirement including the functions performed on the software library of the module is satisfied by true noise generator. With these properties, PKCS11 version of the hardware security module is an ideal solution for high-performance RSA2048 signing and signature verification requirements.

FEATURES
▪ National HSM solution
▪ National certified noise generator
▪ National smart card (AKIS) based authentication
▪ Secure storage medium for Cryptographic key and data
▪ Secure backup and restore
▪ Common Criteria (Common Criteria) EAL4+ certified embedded software
▪ PCIEx1 interface
▪ 2 x USB 2.0 interface
▪ Protected hard metal cover
▪ 4 x tamper detection sensors

FGC-2
SECURE FAX DEVICE

FGC-2 provides secure fax communications with connection between the fax equipment and the PABX.

▪ Encrypting PC based fax communications
▪ RED-BLACK data isolation
▪ Low cost solution for secure fax communications
▪ AMSG 720B TEMPEST Compliance

SECURITY FEATURES
▪ Key loading with fill-gun
▪ Emergency erasure of keys with a single button
▪ Protection of keys during power failures
▪ At least 48 hours of storage
▪ Storage capacity of 100 keys

FEATURES
▪ Encryption for fax devices without crypto interface and using T.30 protocol
▪ RJ-11 input for telephone line
▪ RJ-11 input for fax device
▪ 14400, 9600, 7200, 4800 and 2400 bps
SECURE COMMUNICATION SOLUTIONS

FAX ANALOG DIGITAL CONVERTER

FASD-1

FAX ANALOG DIGITAL CONVERTER

SECURE FAX SOLUTIONS

FASD-1 is not an encryption device in itself but acts as an interface between the fax equipment, the data encryption device and the telephone exchange (PABX). It thus provides RED-BLACK data separation for encryption of PC based fax communication. FASD-1 is a low cost solution for secure fax communication when data encryption device is available.

SECURITY FEATURES

▪ It can be connected to any crypto device compatible with RS-232 standard, 19200/38400 asynchronous N-8-1 protocol

FEATURES

▪ Secure interface for fax devices without crypto interface and using T.30 protocol
▪ RJ-11 input for telephone line
▪ RJ-11 input for fax device
▪ 14400, 9600, 7200, 4800 and 2400 bps
▪ MIL-STD-461E EMC compliance
▪ ANMS-7208 TEMPEST compliance

SECURE MESSAGING SYSTEM - SMS

GMS

TRUSTWORTHY SOLUTIONS FOR MILITARY AND CORPORATE MESSAGING

Secure Messaging System (GMS) developed by TÜBİTAK BİLGEM is suitable for use in military and corporate strategic, operative and tactical field messaging requirements. GMS meets messaging requirements in an uninterrupted, fast, accurate, reliable and secure way through a single system.

GMS provides integrated messaging of strategic and tactical environments which have low bandwidth and high data loss. GMS consists of Message Transfer Servers (MAS), Directory System Servers (DSS), Messaging Clients which can work in both strategic and tactical field, and also Gateway Software developed for a more efficient and integrated messaging.

CAPABILITIES

▪ X.400 and SMTP/IMAP Message Transfer Servers
▪ Messaging Clients supporting corporate and military
▪ Messaging forms
▪ X.500 Directory System Server
▪ LDAP Gateway
▪ ACP 127-X.400 Gateway
▪ Mail List Agent for message delivery to Address Lists
▪ STANDARDS AIPS (ECC) support
▪ STANDARDS 4406 Annex E support for messaging in tactical field
▪ Advanced message reporting and tracking
▪ Extendable directory schema
▪ Advanced management tools

SECURITY FEATURES

▪ Transport Layer Security (SSL/TLS)
▪ Authentication (simple and strong)
▪ Smart card and HSM support
▪ Message security (signature and encryption)
▪ Access control
▪ PKI support
▪ PGP support
▪ Audit log
▪ Security policy

GMS / SECURE MESSAGING SYSTEM - SMS
Mesajlaşma İstemcisi, dizin erişimi ve kullanıcılar arası mesaj iletimi için kullanılan, platform bağımsız çalışabilen bir yazılım bileşenidir. İmzalı ve/veya şifreli mesaj göndermeye imkan vererek, çeşitli güvenlik seviyelerinde mesajlaşma sağlar. Tanımlı her kullanıcı, sadece kendisine izin verilen arayüzleri görebilmek ve ilgili işlemleri yapabilmektedir.

Ortalama bant genişliği için geliştirilen Mesajlaşma İstemcisi, düşük bant genişliği altında çalışmak üzere özelleştirilmiş ve Taktik Mesajlaşma İstemcisi geliştirilmiştir. Böylelikle, sisteme yük getiren işlevlerden arınmış ve sadece gerekli görülen verinin iletildiği, hafif bir kullanıcı arayüzü sağlanmıştır.

Askeri ve kurumsal mesajlaşma imkanı sağlayan, özelleştirilebilir arayüzler içerir.

YETENEKLER
▪ ITU X.400 ve SMTP/IMAP mesajlaşma desteği
▪ ITU X.500 ve LDAP/S unikolu
▪ Varlık Adres Denetleme desteği
▪ Güvenlik mesajlaşma arayüzleri
▪ Bilgi yanıtlanması
▪ Gündelik mesaj raporları
▪ Platform bağımsız çalışabilme

GÜVENLİK ÖZELLİKLERİ
▪ Hat güvenliği
▪ Güven bilgileri koruma
▪ Mesajlaştırmaları şifreleme
▪ Mesajlaştırmaları imzalamak
▪ Günlük mesaj raporları

Güvenlik olarak, DSS外交部は以下の要件を満たしています。

▪ Hat güvenliği
▪ Güven bilgileri koruma
▪ Mesajlaştırmaları şifreleme
▪ Mesajlaştırmaları imzalamak
▪ Günlük mesaj raporları

DSS has been developed in accordance with international standards, it is compatible with the most detailed directory standards cluster ITU X.500, as well as supports the simplified LDAP protocol to access directory information. Thus, DSS can be used with different military and commercial directory applications.

SECURITY FEATURES
▪ Transport Layer Security (TLS/SSL)
▪ Authentication
▪ Access Control (SAC)
▪ The audit log
▪ Security policy
The SRC 155A series of Point-to-Point digital radio devices deliver highly flexible and reliable solutions for nxE1 (up to 4xE1) and nxE3 (up to 4xE3) in PDH hierarchy. STM1 in SDH hierarchy, up to 156 Mbps in Layer 2 Ethernet communication. The operating frequency bands are 7, 10.5, 15 and 26 GHz (ITU).

**CAPABILITIES**

- **Software based selection of data capacity, modulation type, RF channel frequency, transmission mode (redundant or non-redundant), output power and test facilities for operator needs**
- **Thanks to plug&play modules, already established links can have required capacity and interfaces**
- **Flexible installation and operation thanks to separated IDU (Indoor Unit) and ODU (Outdoor Unit) structures.**
- **Low infrastructure requirement and cost thanks to efficient built-in control system and optional RF Network Management System Software**
- **PDH data transmission at 16xE1, 32xE1 and 64xE1, 1xE3, 2xE3, 4xE3 without a need of additional multiplexer thanks to scaleable PDH multiplexer interface cards**
- **SRC155A system can be managed and monitored by using any SNMP-based network or device management system.**

**FEATURES**

- **Standard ITU-T licensed frequency bands (7, 10.5, 15 and 26 GHz)**
- **Mixed Mode working capacity, PDH and SDH communication (16-32-64xE1, 1-2-4xE3, STM1-o, Gigabit Ethernet)**
- **IEEE 802.3, ITU-T G.703 compliant data interface cards**
- **Suitable architecture for (1+0), (1+1) frequency diversity, (1+1) HSB Tx, (1+1) space diversity Rx, (2+0), (4+0) operating modes**
- **In the separated architecture, base band circuits (IDU: Indoor Unit) and Tx/Rx (ODU: Outdoor Unit) are connected with single coaxial cable connection for (1+0) and two coaxial cables for (1+1 and 2+0).**
- **Optimization of bandwidth efficiency with adjustable modulation type depending on data rate.**

**NEW GENERATION HIGH SPEED DIGITAL RADIO LINK DEVICE**

 SRC400

 SRC400 is a new generation, high-speed microwave point-to-point radio system. Design is optimized for Ethernet data transmissions up to 360 Mbps at L2. It is not only for the existing GSM and Telecommunication infrastructures but also for new generations of LTE networks that require high speed data package transmission capabilities. STM1 and Ethernet interfaces can be adapted to the system if required. Operating frequency bands are 7, 10.5, 15 and 26 GHz (ITU bands).
SECURE COMMUNICATION SOLUTIONS

SECURE COMMUNICATION SOLUTIONS

SECURE COMMUNICATION SOLUTIONS

SECURE COMMUNICATION SOLUTIONS

FEATURES
▪ Web based dynamic user interface
▪ Logical and location based grouping of devices
▪ Adding device automatically with device identifier
▪ Advanced reporting functions
▪ SNMP based management
▪ User operation logs
▪ Advanced role based and device group based access control
▪ Password based authentication
▪ E-mail notification
▪ English and Turkish language support

MAIN BENEFITS
▪ Managing devices remotely from single point
▪ Checking alarm and connectivity status of devices
▪ Monitoring instant status of devices
▪ Changing device configurations easily and quickly

SRC-YM
DIGITAL RADIO DEVICE MANAGEMENT CENTER

SRC Management Center is a software solution for remote management of SRC 155A Digital Radio Devices. It provides effectiveness which is a basic need in communication networks. This means quick and easy diagnosis of problems, cost savings from personnel, hardware and training, and high service quality.

SRC Management Center Users can easily register and manage all SRC 155A devices within the network. User can perform different operation on management center depends on their authorization level with multi-user support. Since it is a web based system, there is no need for a software setup in client computers. Only need is a computer with a modern browser having access to the server.

SRC Management Center has all required functionalities that a network administrator has.

FEATURES
▪ Web based dynamic user interface
▪ Logical and location based grouping of devices
▪ Adding device automatically with device identifier
▪ Advanced reporting functions
▪ SNMP based management
▪ User operation logs
▪ Advanced role based and device group based access control
▪ Password based authentication
▪ E-mail notification
▪ English and Turkish language support

MAIN BENEFITS
▪ Managing devices remotely from single point
▪ Checking alarm and connectivity status of devices
▪ Monitoring instant status of devices
▪ Changing device configurations easily and quickly

MDXS-E1
AUDIO MULTIPLICATING DEVICE

It multiplexes 12 or 24 audio channels in transmit and converts them to PCM data at E1 speed. In receive mode, it receives 12 or 24 audio channels from the E1 signal.

FEATURES
▪ Study of the PABX at the Subscriber side
▪ Software Adjustable Transmit and Receive Sound level setting
▪ Internal Ring Generator
▪ AC and DC Power Supply
▪ Control via RS232 Serial port

AUDIO CHANNELS
▪ Capacity: 12 or 24
▪ Backup: 0 % (per channel)
▪ Audio Coding: PCM (G.711), A-law

ANALOG AUDIO INTERCONNECTION
▪ Connectors: 6-pin RJ-12
▪ Nominal Level/Impedance: 0 dBm/200 Ohm
▪ Frequency Response: 300-3000 Hz: ±1dB, 350-3400 Hz: ±1.1 dB
▪ Volume Adjustment (by Software): Transmit > 6 dBm, Receive > 10 dBm, (with
▪ 0.5 dB steps)
▪ In/Channel Noise: < -65 dBm0 (+20dBm)

RING GENERATOR
▪ Generator: 48 VDC, 25 Hz
▪ Nominal Level: 0 dBm

POWER REQUIREMENT
▪ Input voltage: 85 to 264 VAC
▪ Power Consumption: 90 W (12 Channels), 110 W (24 Channels)
▪ Operating Temperature: 0°C - 50°C (ETSI doc. 300-018-1-2, Class 2.2)

MECHANICAL DIMENSIONS
▪ 19 inch x 1.5U (483 x 235 x 67 mm)
Underwater Telephone is a microprocessor controlled communication system which allows communication between surface/subsurface vessels through underwater acoustic waves.

The use of the upper or lower sideband respectively with suppressed carrier frequency (SSB-operation) guarantees a high signal-to-noise ratio at a high transmission bandwidth. The carrier frequency is designed as fixed (quartz stabilized) for NATO frequency or tunable from 1 kHz to 37 kHz for USB and from 4 kHz to 60 kHz for LSB.

While sailing in convoy, it is possible to communicate with suitable station using different frequencies.

Transmission bandwidth is reduced in telegraphy mode for optimum signal-to-noise ratio. Three transducer groups are selectable for nearly omni-directional or sectoral operation. Transducers in the system are placed in the bow and sail.

Inboard connection box which is attached to the pressure hull penetrator is placed in the vicinity of the Combat Information Center. The outboard cables are pressure-resistant and laid in separate cable ways.

The operation and display units are placed in the integrated navigation rack.

Hydrostatic pressure: Equipment exposed to the hydrostatic pressure is resistant to 5 MPa (50 bar). The test pressure can be up to 6.25 MPa (62.5 bar).

**TECHNICAL SPECIFICATIONS**
- Standard frequency: NATO frequency; quartz stabilized
- Tunable carrier frequency (in 3 Hz steps)
- Frequency indicated as numerical value and by a marker on Integrated LCD-display
- Upper side band (USB): 1 kHz to 37 kHz
- Lower side band (LSB): 4 kHz to 60 kHz
- Power output: 100W at 35Ω

Based on a 24V CMOS process packaged in ceramic LCC084 with 82 pin-outs, NTDS level shifter and driver IC provides 18 in, 18 out level shifting between FPGA and NTDS logic signals. This driver IC is comprised of two sub circuits:

- Nine channel (5, VDD) FPGA signal is shifted to nine channel (VCC, 0) NTDS signal
- Nine channel (VCC, 0) NTDS signal is shifted to nine channel (5, VDD) FPGA signal

- Complies with MIL-STD-1399 NTDS (A, B) protocols.
- In FPGA and PCI applications, supply voltages can be chosen as VDD = 3.3V and VCC = -12V
- In standard applications VDD = 5V and VCC = -15V can be used.
Cryptography is the science of information security by means of mathematical techniques. It provides solutions for the security needs such as data security, integrity, non-repudiation, authentication, and access control. These solutions are implemented in a very wide range of areas where security and privacy are necessary, to name a few: smart cards, satellites, network security devices, sensors. The building blocks of these solutions are the cryptographic structures (algorithms, protocols, and architecture).

To develop genuine cryptographic structures, it is mandatory to have qualified researchers who have expertise in the fields of mathematics, statistics, and electronics. TÜBİTAK BİLGEM has been working on cryptography to provide national solutions since 1980’s.

In this context, the following activities are carried out:

- Design of cryptographic algorithms (encryption, hash, key wrapping, message authentication codes, etc.)
- Design of cryptographic protocols (authentication, key agreement, etc.)
- Design of cryptographic architecture (all cryptographic structures in a device and/or system)
- Design of noise processing functions (refinement of random number generation)
- Education and consultancy
EKADAS generates cryptographic keys for crypto devices to be used in secure communication, stores and distributes these keys securely and keeps the accounting information of them.

EKADAS consists of Electronic Crypto Key Generation System (EKAUS), Electronic Crypto Key Distribution Center (EKADAM), Electronic Crypto Key Distribution Terminal (EKADAT), Electronic Crypto Key Loading Device (EKAYUC), Electronic Crypto Key Transport and Loading Device (EKAHAK), Crypto Key Loading Device (KAYC-S) and Line Encryption Device (EKAHAK) and provides solution for all key distribution needs.

**FEATURES**
- Automatic key generation
- Changeable Hierarchical distributed architecture
- Dial-up/radio/satellite communications
- Non-electrical connections with other EKMS
- Automatic monitoring of accounting information

**SECURITY FEATURES**
- Double encryption for key packages
- Offline encryption between EKAUS and EKAYUC/EKATH
- Pre-encryption for the new generation cryptographic devices
- Encryption for all information prior to the communication channel
- Cryptographic authentication between devices
- Role-based user access control
/crypto_key_management_systems

EKMI (EKADAS KMI)

Electronic Key Management Infrastructure

EKMI supports central or distributed generation of key materials. It also automatically delivers any type of crypto key materials to pre-planned crypto units, in a scalable, fast, and secure way.

EKMI have been designed with the primary goals of scalability, modularity and flexibility. Different security protocols and crypto algorithms can be applied with ease thanks to its updatable Security Module. Along with traditional EKMS scenarios, it also provides interfaces to work with other management systems, which facilitates constructing an umbrella key management system.

HVTC, new generation key transfer and fill device of EKMI, provides additional capabilities on top of the ones provided by most known key fill devices.

For reliability purpose, the system can be operated two redundant management sites. It also supports delivering crypto keys to remote locations using PSTN, H/F, Satellite and Ethernet connections.

KEY FEATURES

▪ Support for any kind of classified data (old keys, modern keys, certificates, codebooks, firmware, mission data, etc)
▪ High quality and controlled key generation (Quantum and true RNG combinations)
▪ Transition from EKMS to KMI infrastructure for key management of new generations ECUs
▪ ECU inventory-based keymat distribution and accounting
▪ Constructing a Common Key Management Framework
▪ National key management umbrella
▪ Key management in cooperation with mission management systems of ECUs
▪ Integrating existing key/mission management systems
▪ Replaces redundant EKMS components/systems
▪ Policy-based key management
▪ Built-in key generation capability for over hundred ECU types
▪ On-the-fly custom key format design capability
▪ Intelligent and automated key accounting
▪ Ability to define cryptographic and managerial relations between keymats
▪ Ability to create operational and cryptographic relationship between key materials
▪ Supports complex key usage scenarios such as IPTM® and Link-16
▪ Secure and remote software firmware update for EKMI devices
▪ Centrally managed ECU Fill Profile database of Tier3 devices
▪ Fast responses with on-line, 3-layered, star backbone
▪ NATO IEKMS interoperability
▪ Supports Platform Key Management Systems such as JSF and A400M
▪ Reliable architecture
▪ Built-in secure eMail support
▪ Compression & encryption mechanisms

Data security in the device is provided by system architectures based on red/black separation, filtering, tamper protection and emergency deleting. KAYC-S/N is a tactical device and it is compatible with CONSEC, EMSEC, TEMPEST standards.

FEATURES

▪ “NATO TOP SECRET” and below confidentiality levels
▪ User Access Control by smart card and password
▪ User-friendly interface
▪ Electrical and mechanical red/black isolation
▪ 320x240 TFT liquid crystal display and 7 stokes keypad
▪ External keyboard interface (PS/2)
▪ Emergency erase feature while it is on or off

INTERFACES

On 6-pin connector
▪ DS-102 (EKMS-308F)
▪ DS-101/RS-485 (EKMS-308F)
▪ DS-101/RS-232-D (EKMS-308F)

KAYC-S/N

Crypto Key Loading Device/NATO

KAYC-S/N is a crypto device which is used for storing the crypto keys and data received from interfaces and protocols identified by EKMI-308F standard securely, transporting them and key loading data transmitting to cryptographic terminals in NATO inventory.

KAYC-S/N has SECAN security approval for all NATO security levels, and is considered as a NATO product since it is approved by "Military Committee".

KAYC-S/N can securely store the red/black keys and cryptographic data which are received from local management devices (LMD/KP, DMD), data transportation devices (AN/CYD-10 (DTD), 07000000 (SDS), Simple Key Loader (SKL), EKATAC/EKYÜC) and key loading devices (KYK-13, KAYC-10, KAYC-32, KAOC-8, K0I-18). In addition, the device can transfer the keys to data carriers devices as black or red and load them to cryptographic terminals.

KAYC-S/N is capable of keeping account information of the keys safely and transfer the account information to local management devices such as LMD/KP, DMD. Moreover, the device supports COTS (Common Tier3) application software subsystems.

Data security in the device is provided by system architectures based on red/black separation, filtering, tamper protection and emergency deleting. KAYC-S/N is a tactical device and it is compatible with CONSEC, EMSEC, TEMPEST standards.

FEATURES

▪ "NATO TOP SECRET" and below confidentiality levels
▪ User Access Control by smart card and password
▪ User-friendly interface
▪ Electrical and mechanical red/black isolation
▪ 320x240 TFT liquid crystal display and 7 stokes keypad
▪ External keyboard interface (PS/2)
▪ Emergency erase feature while it is on or off

INTERFACES

On 6-pin connector
▪ DS-102 (EKMS-308F)
▪ DS-101/RS-485 (EKMS-308F)
▪ DS-101/RS-232-D (EKMS-308F)

56

57
KAYC-S
CRYPTO KEY LOADING DEVICE

FEATURES
▪ Storage and loading of national formatted keys
▪ Keys and cryptographic data receiving/transmission with the help of the user interface
▪ Cryptographic data receiving from EKADAS System
▪ Secure key and storing data
▪ 8 MB storage memory
▪ Ability to create and store accounts
▪ Turkish General Staff approved crypto algorithms

NATIONAL KEY LOADING SOLUTIONS
KAYC-S is a crypto device which is used for storing the crypto keys and data received from national formatted keys and protocols (DS-101, DS-102, MILAY) securely, transporting them and key loading/data transmitting to cryptographic terminals.

KAYC-S, which is identified and activated through EKADAS (Electronic Crypto Key Distribution System), can take keys from EKADAS or other systems. KAYC-S has ability to take cryptographic data and keys from EKAVC (Key Loading Device) and EKATAC (Key Transport Device) which are EKADAS terminals or other data transfer devices (AN/CYZ-10 (DTD), DTD2000 (SDS), Simple Key Loader (SKL)) and key loading devices (KYK-13, KAYC-10, KAYC-32, KAYC-64, MILAY) with supported standard interfaces. It processes cryptographic data and keys with safety enhancer like integrity checking and encryption. KAYC-S can store cryptographic data and keys safely and load to several cryptographic key loading/transfer terminal devices. KAYC-S is capable of keeping account information of the keys safely. Moreover, KAYC-S supports the device-specific loading applications with infrastructure development.

Data security in the device is provided by system architecture based on red/black separation, filtering, tamper protection and emergency deleting. KAYC-S is a tactical device and it is compliant with COMSEC, EMI/EMC TEMPEST standards.

INTERFACES
On-6 pin connector
▪ DS-102 (EKMS-308F)
▪ DS-101/RS-485 (EKMS-308F)
▪ DS-101/RS-232-D (EKMS-308F)
▪ MILAY

HVTC
CLASSIFIED DATA TRANSFER DEVICE

KEY FEATURES
▪ Remote secure communication interfaces (between Tier2 and Tier3) (DS102, DS101, MILAY, Ethernet)
▪ High storage capacity (32 GB)
▪ Role-based access control (password and token)
▪ Physical sizes (22cm x 13cm x 4cm, ~1 Kg)
▪ Tamper-proof
▪ Dust-proof
▪ Temperature range (ambient condition): -30°C to +60°C
▪ Secure remote update of firmware & software
▪ User friendly man-machine interface
▪ Rugged, scratch resistant PCAP+ multi-touch-screen (16:9, 7 inch)
▪ High resolution GUI (1020x600)
▪ Gesture capable screen
▪ Versatile Security Module
▪ Secure data storage
▪ Crypto processor
▪ firmware updates
▪ Fill interfaces
▪ DTD1, DTD2, MILAY, RS232, USB (Smartcard, USB Memory), CD/DVDRW, Printer, Tape Puncher
▪ Built-in RNG & External RNG input
▪ Tamper-proof and TEMPEST compliant
▪ Zeros and Tamper indication inputs from host platform

HVTC is a new generation key transfer and fill device that provides all the capabilities of most known key management devices and more. It combines the key processor (strategic) and transfer device (tactical) utilities into one device. With adaptable security module, it can easily adapt to new scenarios that require different protocols and/or algorithms. It is designed to work in difficult tactical field conditions. Its secure GUI and touch screen allows fulfilling difficult key management functions.
**KAYC-32**

**CRYPTO KEY LOADING DEVICE**

**FEATURES**
- Key loading and storage in 5 different format
- Key loading from EKATAC/EKAYUC, KOI-18, KAOC-8, KAYC-32, KAYC-10, KAC-5, KAYC-32, KAC-10
- 32-key storing
- Deleting/Loading keys one by one or all keys simultaneously
- 4 separate buttons for each function
- LED display for warning the user and confirmations during operation
- Automatic key loading to counter device
- Easy and quick access to the keys
- MIL-STD-461 compliant
- AMSG-720B compliant
- DS-102 Common Fill Device Interface

**POWER SPECIFICATIONS**
- Operating Voltage: 6V (2 x 3V Lithium Battery)
- 1/2 AA size Lithium Batteries
- 1000 mA lithium batteries consumption with a shelf life of 10 years
- Consuming 75 uA current in operating mode
- More than one million hours of battery-saving in sleep state

**ENVIRONMENTAL AND PHYSICAL CONDITIONS**
- Storage temperature: -20°C to 70°C
- Relative humidity: %90 @40 °C
- Vibration: 1.5 g @5-200 Hz
- Altitude: 4000 m
- MTBF: over 25,000 hours @25 °C
- Weight: < 0.35 kg (Aluminium Die Cast)
- Dimensions: 138 x 56 x 31 mm (L x W x H)

**KAYC-10**

**CRYPTO KEY LOADING DEVICE**

**FEATURES**
- Loading from EKATAC/EKAYUC, KOI-18, KAOC-8, KAYC-32, KAYC-10, KAC-5, KAYC-32, KAC-10 devices
- 10 X 128 Byte key storing
- Ability to delete keys one by one or all keys simultaneously
- Three separate keys for each function
- LED indicator for operator
- Precaution with two keys against key deleting accidentally
- Automatic key loading to crypto devices
- Easy key selecting
- MIL-STD-461E
- AMSG-720B

**POWER SPECIFICATIONS**
- Operation with 6V (2 x 3V Lithium Battery)
- 1000 mA lithium batteries consumption with a shelf life of 10 years
- More than one million hours of battery-saving in sleep state

**ENVIRONMENTAL AND PHYSICAL CONDITIONS**
- Storage temperature: -30°C to 70°C
- Relative humidity: 10% to 90%
- Vibration: 1.5 g @25-200 Hz
- Altitude: < 4000 m
- MTBF: over 25,000 hours (at 25°C)
- Weight: < 0.25 kg (Aluminium Die Cast)
- Dimensions: 183 x 95 x 21 mm (L x W x H)
KAOC-8
CRYPTO KEY READING EQUIPMENT

CRYPTO KEY SOLUTIONS
KAOC-8 device transmits the key information on the strip hole to the cryptographic devices or key loading devices. KAOC-8 has approval of NATO Military Committee for whole NATO security levels (including NATO TOP SECRET). It can work with KAYC-10(B), KKY-13 key loading devices and devices with DS-102 standard key installation interface.

FEATURES
- Loading key information on the perforated strip to the cryptographic devices with DS-102 interface or key loading devices
- Operating with other common fill guns like KAYC-10, KKY-13, KAYC-32, AN/CYZ-10, KAYC-5, KAYC-20
- Loading key information with any length
- Optical key reading
- Comfortable use
- LED indicator for operator
- Capability of attaching directly to the devices without any cables
- MIL-STD-461E
- AMSG-7201

POWER SPECIFICATIONS
- Operation with 6V (2 x 3V Lithium Battery)
- 1/2 AA size Lithium Battery
- USB 5V Lithium batteries consumption with a shelf life of 10 years
- Shored key carrier: Less than 1 sec
- More than 1 million hours of battery life in stand-by

ENVIRONMENTAL AND PHYSICAL CONDITIONS
- Storage temperature: -20°C to 70°C
- Operating temperature: 0°C to 50°C
- Relative humidity: 0% to 100%
- Altitude: 4000 m
- Weight: < 0.35 kg (Innervations Die Casd)
- Dimensiones: 122 x 56 x 35 mm (L x W x H)
<table>
<thead>
<tr>
<th>SMART CARD AND ID VERIFICATION SYSTEMS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Turkish Republic &amp; Northern Cyprus Identity Card</strong></td>
</tr>
</tbody>
</table>

**Identity Card Application (Contact Card Feature)**
- Visual Authentication
  - Photo, Signature, Guilloche, Rainbow Printing, Multiple Laser Images, Microprinted Text, Raster Printing, Relief Printing, Optical Variable Ink, Ultraviolet Inks, OVD/DOVID
- Electronic Identity Authentication
  - Electronic Certificate, Digital Photo, PIN
- Biometric Authentication
  - Finger Print, Finger Vein Print, Palm Vein Print
- Role-Based Access
- Secure Messaging
- Cryptographic Algorithms
  - RSA-2048, SHA-256, AES-256

**Infrastructure of Electronic Signature Application (Contact Card Feature)**
- Qualified Electronic Certificate and Private Key Loading

**Travel Document Application (Contactless Card Feature)**
- ICAO 9303 Standard Compliant
- Ability to Travel to Bilateral Agreement Countries without Passport and Visa
- Machine Readable Zone (MRZ)
- Basic Access Control (BAC)
- Active Authentication (AA)

*As a result of ongoing research and development, the specifications in this catalogue and its content may change without prior notice.*
SMART CARD OPERATING SYSTEM

AKIS

SMART CARD OPERATING SYSTEM

AKIS (Smart Card Operating System) is a national operating system developed by TÜBİTAK BİLGEM UEKAE and it operates information security, ID recognition, digital signature and secure information exchange applications on smart card chips.

SMART CARD HARDWARE UNITS

- Microcontroller (microcomputer) unit
- File system memory (permanent EEPROM, transient RAM)
- Encryption engine for encryption operations
- Communication unit to communicate with the environment (contact or contactless)

FEATURES

- Communication with a card reader by using ISO 7816 (contact) and ISO 14443 (contactless)
- ISO 7816 and ICAO 9303 (passport) instruction deck support.
- Secure messaging
- Symmetric and asymmetric encryption techniques (DES, RSA, AES) for encryption
- Proprietary File Management System
- Proprietary Memory Management System
- Secure Key management and Structured Architecture
- Role-based Access
- PC/SC, PKCS11, CSP

UKTUM

NATIONAL SMART CARD IC

UKTUM is a contact-based Smart Card IC, developed by TÜBİTAK BİLGEM within the context of National Card Project, providing the capability of secure and fast data transactions. With its Common Criteria EAL5+ assurance level, it serves a competitive trusted choice on the Smart Card IC market in terms of functionality, performance, security measures and price for the e-Government, banking and security applications.

FEATURES

- 8051-based microcontroller (internal memory 358 b)
- 8 KB SRAM
- A total of 192 KB of Flash memory space
- 64 KB of ROM and 128 KB data memory, or 128 KB of ROM and 64 KB data memory can be defined.
- Contactless interface according to ISO/IEC 7816
- Side Channel Resistant Crypto Engines: DES and 3-DES coprocessor
- AES256 coprocessor
- RSA1024 and RSA2048 coprocessors
- Physical Random Number Generator producing True Random Numbers compatible with FIPS 140-2
Embedded security module is developed to use in security applications, such as secure storage, access control, authentication, for tablet PCs, mobile phones and similar devices. Embedded security module uses STM32H7 integrated circuit having EAL5+ certification and is a reliable alternative from the aspects of functionality, performance, and price.

Embedded security module is used in production of tablet PCs with its QFN package and implements the authentication function which enables the access of only authorized persons to a tablet PC.

**FEATURES**

- Microprocessor: 8051 based (Internal memory: 256 B)
- Flash Memory: Total 192 KB shared between ROM and data as 64 KB ROM and 128 KB data memory or 128 KB ROM and 64 KB data memory
- SRAM: 8 KB
- Interface: Compatible with ISO/IEC 7816 standard
- Hardware implemented crypto functions resistant to side-channel attacks: DES, 3-DES coprocessors, AES-256 coprocessor, RSA-1024 and RSA-2048 coprocessors
- RNG: Hardware true random number generator compatible with FIPS 140-2 standard
- Security: Common Criteria EAL5+ certified

**WHAT TYPE OF INFORMATION IS STORED IN THE ELECTRONIC CHIP OF THE e-PASSPORT?**

The electronic chip of the e-Passport contains number of data groups called as Logical Data Structure (LDS). DG1, DG2, COM and SOD of the LDS are mandatory data groups for the e-Passport, and the rest of the LDS are optional data groups depending on the country. DG1, which is one of the mandatory data group members, holds the MRZ data printed on the front of the e-Passport. DG2 data group contains the electronic machine readable of the e-Passport’s owner. COM and SOD data groups have data related to the e-Passport’s security.

**PROPERTIES**

- ICAO 9303 LDS v1.7
- ICAO Basic Access Control (BAC)
- ICAO Active Authentication (AA)
- ISO/IEC 14443 - 3,4 Type A
- 424 Kbps/848 Kbps communication speed
- RSA encryption,
- SHA-1, SHA-256 summary of Algorithms
- Security Certification BSI-CC-PP 0055 (CC EAL4+)
- Supports all e-Passport Readers that are compatible with the standards

**AKIS e-PASSPORT / ELECTRONIC PASSPORT**

e-Passport is a traditional passport book that contains an electronic chip used for authenticating the identity of travellers for border crossings.

The main differences between an e-Passport and a traditional passport is the electronic chip that is embedded in the front of the Passport. The standard of the electronic chip is determined by the International Civil Aviation Organization (ICAO).

**AKIS V1.4 SDK**

AKIS Application Development Kit (SDK) supports easy application developments through the use of API running on a PC, OB and software libraries (AKIS C6, PKCS11, CSP).
AKIS e-DRIVER LICENSE

E-DRIVER LICENSE APPLICATION
AKIS e-driving license application is developed being compatible with ISO/IEC 18013 standard. By means of the application running on the chip, forgery is prevented and the confidential data of the driver is kept on the chip safely. The information is kept on 11 data groups defined as Logical Data Structure (LDS) on the chip. The Data Group 1 (DG1) is supposed to be defined and the rest are shaped according to local needs of each country.

FEATURES
▪ ISO/IEC 18013 LDS
▪ Basic Access Protection (BAP)
▪ Extended Access Protection (EAP)
▪ Active Authentication (AA)
▪ ISO/IEC 14443-3 Type A
▪ 424 Kbps / 848 Kbps transmission speed
▪ SHA-1 and SHA-256 hash algorithm
▪ Security certificate (CC EAL 4+)

AKIS E-DRIVER LICENSE API
▪ API running on computer helps development of new software through language and software library.

SUPPORTED HARDWARES
▪ Infineon SLE78CL Series
▪ NXP P5 Series

PERSONALISATION
▪ AKIS e-driving license application lead data personalization process compatible with ISO/IEC 18013 standard
▪ Command set compatible with ISO/IEC 7816-4
▪ Active Authentication
▪ Flexible and dynamic file applications

VERIFICATION
▪ e-driving license application supporting ISO/IEC 18013 LDS data groups and digital signature
▪ Combined key compatible with ISO/IEC 7816-4
▪ Basic Access Protection
▪ Active Authentication against cloning

BAP-BASIC ACCESS PROTECTION
The mechanism is responsible for providing access to data on the chips from an authorized terminal and providing safe messaging between the chip and terminal. It is also responsible for the creation and validation of session keys by optically reading of MRZ data and start of secure messaging.

AP-EXTENDED ACCESS PROTECTION
It provides access to biometric data groups on chip accessible based certificate.

AA-ACTIVE AUTHENTICATION
It prevents cloning e-driving license application chip.

KYS is an integrity of applications capable of managing all the life cycle for official documents such as identity card, driving license, passport etc.

PERSONALIZATION
▪ Creating application package
▪ Managing application package
▪ Customizations of application package
▪ Quality control
▪ Capability of operation in both and desktop customization machines
▪ Terminal and user management
▪ Management system

GENERAL FEATURES
▪ Server: KYS is independent from platform and database management system and easily integrated with available vs web-servers. It enables the operation logic significantly. It offers role-authority based access and related operation support.
▪ Smart Card: KYS is compatible with National Smart Card Operation System (AKIS/UKIS) and JCOP it is integrated with identity, passport and driving license implementations.
▪ Security: KYS has two features, including authority based access, safe storage of sensitive data, SSL connection between terminals, operational records with electronic signature and card access to system.
▪ PKI: KYS operates in integration with National Public Key Infrastructure (NAI).

REPOSITORY
▪ Reporting in accordance with rules
▪ Card based reporting
▪ Machine based reporting
▪ Reporting based on operational records
▪ Parameter inquiry system
▪ Output capability in PDF, MS Excel and MS Word formats

INVENTORY
▪ Enrollment with multiple card serial numbers
▪ Card return, calculation and destruction operations
▪ Dissemination of cards to the personalization environment
▪ End of Day operations
▪ Card receipt and delivery
▪ Declaration of card status summary

AKIS e-DRIVER LICENSE / ELECTRONIC DRIVER LICENSE
This system performs authentication feature while a public service is served to a citizen. By this way, the system verifies whether the citizen who attends the service and the person who serves it are the ones that are declared to be.

**IDENTITY AUTHENTICATION FACTORS**
- Physical Authentication
- Secure Message
- Electronic Certificate
- PIN
- Biometric
- Digital Photo

This feature is one step of the identity authentication and requires confirmation of the photograph by the operator after registration. The KEC can get access to the data fields such as the personal message and biometric data of the cardholder, which cannot be accessed with the standard card reader.

KKEC displays the photograph of the cardholder within the card on its colored graphic display. This feature is one step of the identity authentication and requires confirmation of the photograph by the operator after registration. The device is tamper-proof and its application software has CC EAL4+ (ALC _ DVS.2) security level certificate.

**SECURITY FEATURES**
- Authentication using certificate
- Authentication using certificate and PIN
- Authentication using certificate and biometrics
- Authentication using certificate and photograph
- Authentication using certificate, photograph and PIN
- Authentication using certificate, photograph and biometrics
- Authentication using certificate, photograph, PIN and biometrics
KIOSK-KEC is one of the terminal devices of the Electronic Authentication System. Using KIOSK-KEC, the cardholder, on their own, can test their ID card, change their personal message and PIN, remove PIN blockage and display the information within the card.

With the help of the Secure Access Module (SAM) included in the device, KIOSK-KEC can get access to the data fields such as the personal message and biometric data of the card holder, which cannot be accessed with the standard card reader. The device is tamper-proof and the card access application inside has CC EAL+ (ALC _ DVS.2) security level certificate.

With KIOSK-KEC, the operation of both contact and contactless interfaces of the card can be tested; authentication certificate, PIN and biometric data inside the card can be verified. Additionally, personal identity information and photograph of the citizen within the card can be displayed on the screen. KIOSK-KEC allows the user to change the PIN of the card and remove PIN blockage as well. The PIN can be changed by entering the current PIN of the card or through biometric verification. For the PIN blockage removal operation, it is required for the citizen to enter the card’s PUK information. If the citizen doesn’t know the PUK information of the card, this procedure can be done also by biometric verification without the need of the PUK.

SAFETY FEATURES AND FUNCTIONS
- Card test (certificate, photograph, PIN and biometric verification)
- PIN verification
- Defining the new PIN with the current PIN
- New PIN assignment with biometric verification
- PIN blockage removal with PIN verification
- PIN blockage removal with biometric verification
- Displaying personal identity information (after PIN verification)
- Personal message change
- Displaying contactless interface information

GEM is the security module of Card Access Device which is developed to verify National Identification Card in electronic applications and authenticate the owner of that card. In other words, GEM implements the cryptographic functions of Card Access Device. By means of GEM, it becomes possible to access data fields such as the biometric data of the card owner, and to execute READ/WRITE operations on these fields. Besides, the use of certificates and keys embedded in GEM ensures a secure communication with National Identification Card. Concisely, GEM is the module which provides the secure use of Card Access Device and consequently enables the secure authentication of identity information in electronic environment.

SPECIFICATIONS
- Communication with ISO 7816 (with contact) standard message sets
- Support of ISO 7816 command set
- Secure messaging
- Symmetric and asymmetric encryption (DES, RSA, AES)
- Secure file and memory management system
- Security architecture and secure key management
- FIPS specification
- Support of PKCS11, CSP
- Common Criteria CE EAL4+ certified
- Compatible with Infineon, NXP and UKTUM chips
ELECTRONIC CERTIFICATION MANAGEMENT SOLUTIONS
**Public Key Infrastructure (PKI)** is a technology built on electronic certificates. Certification Authority (CA) and other supporting software are required in order to create electronic certificates. CA creates certificates for other CAs, users, servers and devices.

ESYA Certification Authority is the basic product of National Public Key Infrastructure (MA3) project. ESYA Certification Authority supports industrial electronic certificate standards (X.509, CVC etc.) and provides certificate service providers (CSP’s) with all services required throughout the life cycle of electronic certificates (creation, renewal, revocation, etc.) via a user-friendly interface.

### PUBLIC KEY INFRASTRUCTURE SERVICES
- X.509 v3 Certificates, X.509 v2 Certificate Revocation Lists (CRL)
- Online Certificate Status Protocol (OCSP/Offline)
- Key Recovery and Update
- Qualified Electronic Certificate
- SSL (Host and Client), VPM
- Windows Smart Card Logon Certificate, Windows Domain Controller Certificate

### CRYPTOGRAPHIC FEATURES
- RSA algorithm (1024, 2048, 4096 bit key lengths)
- ECDSA algorithm (163, 192, 256, 384, 521 bit key lengths)
- SHA1, SHA256, SHA384, SHA512 hash algorithms

### CRYPTOGRAPHIC HARDWARE SUPPORT
- PKCS11 compliant smart cards and tokens
- HSM (Hardware Security Module) support
Thanks to widely used internet and computer systems, companies and organizations can require their employees cooperate together and share information extensively even if they are located at different places. E-mail services play significant role as means of information sharing and they gain importance day by day. It has become very usual to have reports, plans and design documents containing proprietary corporate data flowing over e-Mail servers. These e-Mails and documents mostly remain accessible to unauthorized people. Having accessed by malicious people, the leakage of those valuable e-Mails can cause severe commercial damage and weaken the brand power of the company which makes e-Mail protection and desktop computer security solutions clear requirements for desktop and portable computer.

**MAIN COMPONENTS**

- Secured e-Mail module
- Desktop computer security module
- Kermeo

**SECURITY SERVICES**

- Secure e-Mail (SARME)
- File signing/encrypting
- Secure index
- Certificate validation
- Secure deletion

**CRYPTOGRAPHIC FEATURES**

- Work with X.509 v3 Certificates which are prepared by using RSA, DSA and Elliptic Curve algorithms
- Using X.509, AES algorithms for PESC/CMS
- SHA-1 and SHA-2 family, message digest algorithms
- PKCS12 and PKCS5, password based encryption algorithms

**CRYPTOGRAPHIC HARDWARE SUPPORT**

- Work with PKCS11 compatible smart cards and tokens
- Files not suitable for crypto cards are stored, the keys are issued by PKI and securely stored in local storage

**SUPPORTED STANDARDS**

- ETSI TS 101 733 CAdES electronic signature format (ASN data structure)
- ETSI TS 101 903 XAdES electronic signature format (XML data structure)
- ETSI TS 102 918 Associated Signature Containers

**SUPPORTED SIGNATURE TYPES**

- Basic Electronic Signature (ES-BES)
- Electronic Signature with Time (ES-T)
- Explicit Policy-based Electronic Signature (ES-EPED)
- ES with Complete Validation Data References (ES-C)
- Archival Electronic Signature (ES-A)
- Extended Electronic Signature (ES-X)
- Extended Long Electronic Signature (ES-XL)
- Extended Long Electronic Signature (ES-XL)
- Electronic Signature Libraries

**CRYPTO HARDWARE SUPPORT**

- Working with PKCS11 compatible smart cards and tokens
- Working with Hardware security modules (HSM)

**ADVANTAGES PROVIDED**

- Electronic Signature Libraries: International and national E-Signature standards, laws, regulations and full compliance with the regulations
- Full compliance with P14 certificates and effortless access to legacy systems
- High Technology: Security smart card in order to maximize/bar use
- National software compatible with international safety standards
- Mobile Technology: Android devices, interoperability, Microsoft mobile signature interface
- Smart Card Support: smart card transactions from different brands. APDU smart with the flow better processing in making cards
- Ease of use: after the approval in your habits. Turkcell support

**TIME STAMP SUPPORT**

- Authorization of time stamp information can be checked like signatures
- All information related to the time stamp of a document can be reached

**ANOTHER KEY INFRASTRUCTURE SERVICES**

- X-509 certificate validation
- X-509 certificate-based encryption
- Mobile signature
Timestamp, as defined in international standards, provides legal proof of existence of a digital data at a particular time. Timestamp Server creates timestamps for received digital data compatible with these international standards. For e-documents such as a signed agreement, a transaction or an application, proof of the existence at a particular time is very crucial for current e-trade and e-government applications. Timestamp is also required for varying kinds of digital data that need copyright including a new idea, photograph, model, drawing, research, book formula or an algorithm.

According to the Turkish Law No: 5070 on Electronic Signature
Timestamp: an electronic data, manufactured, modified, sent, received and/or recorded in order to determine the time, the electronic certification service provider of electronic signature verified by the record.

FEATURES
▪ RFC 3161 compatible timestamp creation.
▪ NTP support
▪ High performance by using HSM (Hardware Security Module)

CRYPTO FEATURES
▪ RSA and ECDSA algorithms, support for the signature timestamp
▪ AES encryption algorithms
▪ SHA-1 and SHA-2 family of hash algorithms

SECURITY SERVICES
▪ Timestamp using X.509 certificates and public key signing algorithms
▪ Client authentication using PKCS11

CRYPTO HARDWARE SUPPORT
▪ Work with PKCS11 compliant smart cards and tokens
▪ Work with Hardware Security Modules (HSM)

ADVANCED CUSTOMER MANAGEMENT
Timestamp server provides the ability for defining customers with prepaid credit by an advanced customer management interface. Timestamp server creates responses to timestamp requests based on customer information.

TIMESTAMP FILES ARCHIVING
Timestamp Server stores timestamp responses to be able to verify them afterwards.

HIGH PERFORMANCE OPERATION
Timestamp Server processes simultaneous client requests in parallel and responds with high performance.

IMPLEMENTATION OF DESKTOP SIGNING
As computers become more prevalent, many business processes have been reimagining over electronic media resulting in the declined use of paper. Electronic signature, which is taking places of paper signatures, is one of the technologies that brought about this trend. It enables digital documents to be signed and stored securely with protected integrity. Nowadays, electronic signature has become a security mechanism defined by international standards and governmentality. For an electronic signature to legally valid, it must be created in the correct way and be compatible with these standards, which are quite detailed and frequently updated. For the end-users to follow and stay in accordance with these standards is a difficult and time consuming process. Therefore a simple application for creating signed documents compatible with the standards has become a very valuable tool. Also, Electronic writing (e-Writing) standard package which supports public enterprise’s correspondence among themselves by using electronic signature becoming widespread day by day. For those reasons, the tool has been considered necessary for creating and verifying e-writing package. Imzager meets those requirements with modern user friendly and comprehensive interface.

SUPPORTED STANDARDS
▪ ETSI TS 101 733 CADES e-signature format
▪ ETSI TS 101 903 XADES e-signature format
▪ ETSI TS 102 778 PADES e-signature format
▪ Support of e-Writing package
▪ X.509 v3 certificates
▪ Cancel list of X.509 v2 certificate (CRL)
▪ RFC 5280 certificate verification
▪ RFC 2560 online certificate status protocol (OSIP/OCSP)
▪ RFC 3161 Time stamp

CRYPTOGRAPHIC FEATURES
▪ Work with X.509 Certificates which are prepared by using RSA, DSA and Elliptic Curve algorithms
▪ SHA-1 and SHA-2 family, message abstract algorithms

CRYPTOGRAPHIC HARDWARE SUPPORT
▪ Work with PKCS11 compliant smart cards and tokens
▪ Work with Hardware Security Modules (HSM)
SECURE PDF
IMPLEMENTATION OF PDF SIGNING / ENCRYPTION

PDF FILE SIGNING
Supported by many operating systems, PDF file format gained a wide range acceptance and is now a commonly used de-facto standard. Besides, the security of electronic documents becomes more important as they take the role of paper day by day. Signing a document is one of the basic security operations that preserves its integrity and identifies the author of the document in a secure way. Secure PDF is one of the application supporting widely accepted digital signature standards on PDF files.

SECURE PDF
Secure PDF supports ETSI PAdES compliant e-signature by using HSM or smart card and X.509 Certificate based encryption for PDF files in a directory.

FEATURES
▪ Password-Based System
▪ Bulk PDF File Signing
▪ Bulk PDF File Encryption
▪ Multiple Signatures
▪ Timestamp Support
▪ Keyword Filter
▪ HSM and Smart Card Support
▪ Signing with Configuration File and Database

SUPPORTED STANDARDS
▪ X.509 v3 Certificates
▪ ETS 102 778 PAdES
▪ RFC 3161
▪ PKCS#11 Structure

CRYPTOGRAPHIC FEATURES
▪ Work with X.509 v3 Certificates which are prepared by using RSA, DSA and Elliptic Curve Algorithms
▪ SHA-1 and SHA-2 Hash Functions

CRYPTOGRAPHIC HARDWARE SUPPORT
▪ Work with PKCS11 Compliant Smart cards and HSM

* As a result of ongoing research and development, the specifications in this catalogue and its content may change without prior notice.
SGS
SPECTRUM MONITORING SYSTEM

With its unique RF hardware and spectrum monitoring software SGS 3.0 provides wideband monitoring capability in the 9 kHz-2.7 GHz frequency range. The upper limit of this frequency range can be easily be upgraded to 18 GHz. SGS simultaneously demodulates and records the outputs of 64 analog signals in a 40 MHz span using the Multi-Channel Signal Monitoring and Analysis (CITA) algorithm.

SGS has many spectrum monitoring capabilities like setting alarms for target frequencies, masking signals that are not of interest, spectrogram analysis and controlling multiple receivers through serial and ethernet connection. SGS can also be accessed remotely over network. The system outperforms its competitors with a frequency sweeping rate over 15 GHz/s and extraordinary reception sensitivity.

FEATURES
- Frequency Range: 9 kHz-2.7 GHz (Can be upgraded to 18 GHz)
- Real Time Bandwidth: 40 MHz
- Number of Demodulator Channels: 64 (in 40 MHz span)
- Supported Modulation Types: FM, AM, LSB, USB, CW
- Sensitivity: < -140 dBm (270 Hz RBW, Pre-Amplifier enabled)
- Pre-Amplification: 0/20 dB
- Dynamic Range: > 80 dB (100 kHz IFBW)
- Adjustable Input Attenuation: 0-60 dB (in 5 dB steps)
- Frequency Sweeping Rate: > 15 GHz/s (100 kHz IFBW)
- Phase Noise: < -80 dBc/Hz (1 kHz)
< -115 dBc/Hz (1 MHz)
< -145 dBc/Hz (10 MHz)
- Dimensions: 2U height, 19 inch width
**EFD18A**

**BROADBAND ELINT FREQUENCY CONVERTER**

EFD18A is a frequency converter which detects signals in 30 MHz-18 GHz frequency range and down-converts them into 3 different intermediate frequency (IF). 70 MHz, 140 MHz and 160 MHz, selectable by the user. In addition to different IF output options, BAND@ 1 GHz, Real-time bandwidth is 500 MHz at 1 GHz output. There are 8 bandwidths at 70 MHz IF output: 0.5, 1, 2, 5, 10, 20, 30 and 45 MHz. Only 80 MHz bandwidth is provided at 140 MHz and 160 MHz IF output. In addition to them, PAN IF output is given at 70, 140 and 160 MHz.

Technical specifications of EFD18A satisfies the requirements of a high performance microwave receiver. EFD18A is designed to detect high data rate PCM/TDM signals and radar signals which require high pulse accuracy. Modern digitally modulated signals, like high level QAM, can be detected by EFD18A having low group delay distortion and ultra-low phase noise.

**FEATURES**

- **Frequency range:** 30 MHz-18 GHz
- **Real time bandwidth:** 700, 400, 100, 20, 5, 2, 1, 0.5 MHz
- **IF output frequency:** 70, 140, 160 MHz and 1 GHz
- **Gain from RF to IF:** > 42 dB
- **Dynamic range:** -110 dBc/Hz (100 kHz offset)
- **Dimensions:** 2U height, 19 inch width
- **Remote Control:** Ethernet

**FD300A**

**IF CONVERTER**

FD300A is designed to solve incompatibility issue between microwave receivers with multiple frequency outputs and devices that record, digitize, display and analyze IF outputs used in electronic intelligence systems.

Besides the FD300A converts 10-300 MHz carrier frequencies to 70, 140, 160, 10.7, 21.4 MHz standard intermediate frequencies and frequencies between 10-65 MHz in steps of 5 MHz, it can also convert 1 GHz carrier frequency to the specified intermediate frequencies. Moreover, in bypass mode, the input signal is transferred to the output either filtered or unfiltered. The device has a filter block, allowing the user to choose eight different bandwidths around 70, 140, 160 MHz, at the output and provides automatic and manual gain control.

With the help of video output at 160 MHz, FD300A makes it easy to measure pulse modulated signals. All the functions of the device can be controlled via its keypad or a computer connected to its RS-232/Ethernet interface.

**SPECIFICATIONS**

- **Input Frequency Range:** 10 MHz-300 MHz & 1 GHz (Resolution: 100 kHz)
- **Output Frequencies:** 70, 140, 160 MHz (IF OUT)
- **Noise Level:** 14 dB (typical)
- **OIP3:** +18 dBm (minimum)
- **P1dB:** +17 dBm (typical)
- **Max. Gain from RF to IF:** 45 dB (typical)
- **Phase Noise:** -109 dBc/Hz (100 kHz offset)
- **Image Frequency Suppression:** 90 dB
- **Device Management:** Keypad or a computer connected to RS-232/Ethernet interface
- **Connector Type:** BNC
- **Power Supply:** 198-242 VAC, 47-53 Hz
- **Weight:** 9.5 kg
- **Input-Output Impedance:** 50 Ohm (IF In & Out), 93 Ohm (Video Out)
- **Dimensions:** 2U height, 19 inch width, 53 cm depth

**IUKEAE**
HFKS

HF RECORD AND PLAYBACK DEVICE

HFKS digitizes and records the data within the 0.1-20 MHz frequency range which is vital in military telecommunications.

The device can be used to record all telecommunications data within this frequency band (0.1-20 MHz) for further detailed examination. It also provides the option to record only the most heavily used frequency band (3-8 MHz). Besides, HFKS can be controlled remotely and can also be monitored and managed by multiple users. The device continuously monitors the spectrum while recording and the user can examine any desired part of the spectrum in a narrow or wide range. Listen to and record the voice data obtained from up to four analog signals demodulated by channelizing application.

SPECIFICATIONS

▪ Operating Frequency Range: 0.1-20 MHz / 3-8 MHz (Optional)
▪ Number of Demodulator Channels: 4 channels
▪ Supported Demodulator Types: FM, AM, USB, LSB, CW, ISB
▪ Dynamic Range: > 80 dB
▪ Gain: from -37 to +75 with 1 dB intervals
▪ Noise Level: 4 dB @ 0.1-20 MHz, 5 dB @ 3-8 MHz
▪ Filtering: > 80 dB @ 30 MHz
▪ Record Time: 80 hours

KAGIS

RECORD, PLAYBACK & REVIEW SYSTEM

KAGIS allows the monitoring of instant RF spectrum in real-time and multi-channel. Recorded signals can be shown later to be examined and can be played back in analog.

KAGIS provides a suitable infrastructure to allow detailed analysis of the recorded signals. Amplitude-Time, Frequency-Time, Phase-Time and Time-Frequency graphs can be plotted for digitized signals. Multiple signals can be displayed on one screen, a variety of measurements can be done automatically or manually on the signals and the measurement results can be saved for analysis.

KAGIS especially allows additional capabilities for recording and analysis of radar signals. For example, in addition to the RF signals, the video signal defined as the envelope of IF signal can be recorded simultaneously. Moreover, voice data, which is produced from video signal in order to distinguish pulse signals by ear, can be listened to and recorded. Operations like Automatic pulses listing on recorded signals and offline filtering can be performed.

FEATURES

▪ Records Center Frequencies: 70, 140, 160 MHz
▪ Record Bandwidth: Up to 80 MHz
▪ Record Type: IF, Video (IF envelope)
▪ Sampling Rate: Up to 2000 MHz
▪ Monitoring: Up to 8 Canal
▪ Record: Up to 4 Canal
▪ Review: Up to 4 Canal
▪ Playback: Up to 4 Canal
▪ Capacity: 24 TB (Can be increased)
YTA-018D is a software receiver which detects the signals between 10 kHz-18 GHz frequency range and then demodulates the common modulation types such as AM, FM, M, SSB, DSB, PSK, QAM. The system can process and monitor the signals coming from antennas and also it can down convert them to 70 MHz and give off through IF output at the front panel. Therefore, this system is a spectrum monitoring system and a highly sensitive receiver, as well.

As the dynamic range of YTA-018D is high (12 dB typical noise level, 0 dBm IIP3) and as it has a highly sensitive performance (130 dBm/Hz), the system can be used to receive the radar and other communication signals too. Moreover, the system has high image frequency suppression by suppressing minimum 90 dB, typically 100 dB through whole working band.

In addition to self test and calibration functions, the system can also be controlled remotely through Ethernet interface. The power consumption of the system is 80W at spectrum scanning mode. The power is supplied from a battery and the system operates 2 hours continuously.
YTA-MK01A is a software-based wideband receiver which receives the radio signals between 9 kHz-2,7 GHz and a highly sensitive receiver, as well as to 70 MHz. The electrical and mechanical design of YTA-MK01A gives availability to increase the upper-limit of the operating frequency range to 18 GHz. The system has a dynamic range which exceeds 80 dB and 15,0 GHz’s scanning speed. Due to its high sensitivity and phase noise performance, YTA-MK01A is an ideal receiver for today’s complex SIGINT signals.

YTA-MK01A
SOFTWARE-BASED HF/VHF/UHF RECEIVER

SPECIFICATIONS
▪ Frequency Range: 9 kHz-2,7 GHz (Availability to increase up to 18 GHz)
▪ Real-Time Bandwidth: 40 MHz
▪ Pre-Amplifying: 0/20 dB
▪ Dynamic Range: > 80 dB at 100 kHz IF Bandwidth
▪ Adjustable Input Attenuation: 0-60 dB with 5 dB steps
▪ Frequency Scanning Speed: 15 GHz/s at 100 kHz CBG
▪ Phase Noise: < -90 dBc/Hz (10 kHz Offset)
▪ Size: 2U height, 19” width
▪ Remote Control Interface: Ethernet and RS-232

YTA-MK01A is a software based wideband receiver which receives the radio signals between 9 kHz-2,7 GHz and a highly sensitive receiver, as well as to 70 MHz. The electrical and mechanical design of YTA-MK01A gives availability to increase the upper-limit of the operating frequency range to 18 GHz. The system has a dynamic range which exceeds 80 dB and 15,0 GHz’s scanning speed. Due to its high sensitivity and phase noise performance, YTA-MK01A is an ideal receiver for today’s complex SIGINT signals.

YTA-MK01A
SOFTWARE-BASED HF/VHF/UHF RECEIVER

SPECIFICATIONS
▪ Frequency Range: 9 kHz-2,7 GHz (Availability to increase up to 18 GHz)
▪ Real-Time Bandwidth: 40 MHz
▪ Pre-Amplifying: 0/20 dB
▪ Dynamic Range: > 80 dB at 100 kHz IF Bandwidth
▪ Adjustable Input Attenuation: 0-60 dB with 5 dB steps
▪ Frequency Scanning Speed: 15 GHz/s at 100 kHz CBG
▪ Phase Noise: < -90 dBc/Hz (10 kHz Offset)
▪ Size: 2U height, 19” width
▪ Remote Control Interface: Ethernet and RS-232

NON-LINEAR JUNCTION DETECTOR 2000MHZ
YTS2000

SYSTEM FEATURES
▪ Semiconductors can be detected in high accuracy and precision.
▪ Hand-held and user friendly.
▪ Hidden any electronic devices (audio/video record systems etc.) can be detected in high performance.
▪ High RF transmit power and receive sensitivity. Hence most of the electronic devices can be detected.
▪ Hand-held operation gives an opportunity to find small electronic devices.
▪ Circular transmit and receive antennas. This feature provide both less scanning time and high accuracy.
▪ Touchscreen LCD display.
▪ Provides both audio and display indicators to alert the operator.
▪ Provides signal analysis algorithm to operator for detailed evaluation.
▪ Both English and Turkish interface.

APPLICATIONS
▪ Detection of any hidden electronic record systems.
▪ Detection of any active/passive RF transmitter/receiver.
▪ Detection of any hidden open/closed mobile phones.
▪ Localization of detected electronic devices.
▪ Detection of electronic controlled explosives.

TECHNICAL SPECIFICATIONS

RF Transmitter
▪ Operating Frequency Range: 2000MHz - 2050MHz
▪ Channel Number: 50
▪ Frequency Hopping Range: 1MHz
▪ RF Transmit Power: 33dBm (15dB tune range)
▪ Modulation: Pulsed/CW
▪ RF Transmit Antenna: Circular polarized, 6dBi

RF Receiver
▪ Operating Frequency Range: 4000MHz – 4100MHz (2. Harmonic)
▪ RF Sensitivity: -135dBm
▪ RF Receiver Antenna: Circular polarized, 4dBi

HMI
▪ Video: 3.2” colour touchscreen LCD display
▪ Audio: Buzzer and headphone
▪ Batteries: Li-Ion battery (1 hour life-span), spare battery
▪ Size: 20cm x 30cm x 11cm
▪ Weight: About 2kg
▪ Extension Range: 1m (Telescopic Extension Arm)
As a result of ongoing research and development, the specifications in this catalogue and its content may change without prior notice.

TÜBİTAK BİLGEM TECHNOLOGY AND SOLUTION CATALOGUE

DATA VALORISATION SOLUTIONS
IYON SUITE

FORENSIC IMAGE ENHANCEMENT & RESTORATION SOFTWARE

TECHNICAL SPECIFICATIONS

IYON SUITE presents solutions and tools as a software package in the field of image and video processing. This software has advanced video/image filters that are designed specifically for needs of criminal image investigation labs.

IYON SUITE, for video and images:
▪ Enhancement/Reparation
▪ Focus distortion/Noise removal
▪ Geometric distortion removal
▪ Interpolation/Dimensional change
▪ Compression error removal
▪ Video fusion
▪ Domain conversion
▪ Video moving estimation
▪ More than 70 advanced filters, for instance, super resolution filters

It is distinguished from similar softwares with following features:
▪ Block-based filter interface
▪ Advanced ability of adding new algorithms as plug-ins
▪ Advanced tools for image/video processing

APPLICATION PROPERTIES

▪ Update with Novel Methods.
The application is not limited to the present image enhancement methods and algorithms. Due to the ability of adding novel methods as plug-ins, the methods and algorithms can always be updated included or excluded to satisfy the current requirements.

▪ Defining New Methods in Block Applications
While enhancing distorted images, usage of multiple methods may be required in certain cases. The developed application has the capability of combining many methods into a single method and by this feature, which is called Block Applications, the user is provided with creative and flexible solutions.

* As a result of ongoing research and development, the specifications in this catalogue and its content may change without prior notice.
**DATA VALORIZATION SOLUTIONS**

**NATO ARCADE & SMIR-ONLINE**

**ALLIED RADIO FREQUENCY COMPUTER AIDED DATA EXCHANGE & SPECTRUM MANAGEMENT INFORMATION REPOSITORY ONLINE**

**ARCADE (ALLIED RADIO FREQUENCY COMPUTER AIDED DATA EXCHANGE)**

Developed to simplify the processes of construction, synchronization, querying and management of spectrum data in SMADEF-XML format by NATO Spectrum Management Community and NATO SMIR (Spectrum Management Information Repository).

**GENERAL ABILITIES**

- Packaging, downloading and querying SMADEF-XML formatted data in a local database
- Displays frequency assignments on a geographic map
- Intermodulation calculations
- Spectrum analyzer
- Assignment usage periods, occupancy charts
- Synchronization of local database from a central database

**SMIR-ONLINE (Specturm Management Information Repository- ONLINE)**

Developed using SOA architecture to access central SMIR database and manage spectrum assignment processes using up to date data through network, using web services and web interface.

**GENERAL ABILITIES**

- Access to up to date data in central SMIR database
- Provides all abilities of ARCADE without a setup, through a web browser over a network
- Simplifies application of NATO spectrum management processes
- Easy SMADEF-XML data construction via Designer Wizards
- Frequency Nomination Tool
- Peer to peer HF and VHF analysis
- VHF Coverage Analysis
- Ability to display map background from online map servers

---

**CIVIL AVIATION SOLUTIONS**
As a result of ongoing research and development, the specifications in this catalogue and its content may change without prior notice.

## AIRCRAFT TRACKING SYSTEM

The Aircraft Tracking System consists of an Aircraft Tracking Device (HATC) fitted to the aircraft, and an Aircraft Tracking Center (HATM) on ground. Aircraft location, speed and altitude data is periodically transmitted to the monitoring center where it is displayed on a map. Aircraft in distress are highlighted on the monitoring center map display and an audio warning is sounded. Voice communication between aircraft unit and the monitoring center using a “push-to-talk” interface is made possible over GPRS.

As both GSM and satellite links are used for communications, system is both cost effective and reliable. Even if the aircraft unit discontinues functioning after a crash, the last reported location will greatly help search and rescue efforts.

## FEATURES

- uninterrupted data acquisition, processing and recording
- an extendible server architecture with back-up mechanisms
  - Double back-up server stack
  - Data storing with back-up
  - Back-up network and power connections
- secure access through internet with defined users/client authorization
- displaying clients supported by high performance geographical information system and vector maps
- authorisation for continuous tracking and retrospective querying capability
- authority groups and aircraft groups determination capability
- push-to-talk (PTT) voice communications with aircraft
- automatic emergency declaration for loss of communications with an aircraft
- declaration of emergency status with SMS and e-Mail

### AIRCRAFT TRACKING SYSTEM

Low altitude aircraft in VFR flight such as helicopters are not trackable by RADAR systems. Fatal helicopter crashes in the past have underlined the need to track and locate such low altitude flights. The Aircraft Tracking System (HATS) is expected to aid in the quick determination of aircraft’s exact location after accidents.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uninterrupted data acquisition, processing and recording</td>
<td></td>
</tr>
<tr>
<td>Extensible server architecture with back-up mechanisms</td>
<td></td>
</tr>
<tr>
<td>Secure access through internet with defined users/client authorization</td>
<td></td>
</tr>
<tr>
<td>Displaying clients supported by high performance geographical information system and vector maps</td>
<td></td>
</tr>
<tr>
<td>Authorisation for continuous tracking and retrospective querying capability</td>
<td></td>
</tr>
<tr>
<td>Authority groups and aircraft groups determination capability</td>
<td></td>
</tr>
<tr>
<td>Push-to-talk (PTT) voice communications with aircraft</td>
<td></td>
</tr>
<tr>
<td>Automatic emergency declaration for loss of communications with an aircraft</td>
<td></td>
</tr>
<tr>
<td>Declaration of emergency status with SMS and e-Mail</td>
<td></td>
</tr>
</tbody>
</table>

* As a result of ongoing research and development, the specifications in this catalogue and its content may change without prior notice.
HATC / AIRCRAFT TRACKING DEVICE

HATC is the vehicle mounted part of the Air Vehicle Tracking System. The device gets the location, speed and altitude data from the air vehicle sensors and sends these data to the Air Vehicle Tracking Center through GSM and LEO Satellite communication interfaces. HATC also creates availability to make push to talk based voice communication through GPRS network.

HATC has internal and external crash sensors for automatic emergency notification. The device also has a manual emergency feedback button. Furthermore, LED warning indicators provide feedback regarding the emergency situation and device self-test results.

HATC is powered from 28VDC power supply located in the air vehicle. In case of a power loss, there is an internal battery which allows the device to operate for a minimum of 30 minutes. The battery is regularly charged by a smart charging unit. The power loss during the flight is evaluated as emergency and reported to the Air Vehicle Tracking Center.

MECHANICAL INTERFACES

HATC is designed to be placed in the operator console by 4 DZUS screws.

Width: 145.50 mm
Height: 104.00 mm
Depth: 144.95 mm
Weight: 2700gr

ENVIRONMENTAL CONDITIONS

HATC has DO-160G Characteristics.

<table>
<thead>
<tr>
<th>Section</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Height</td>
<td>Category</td>
</tr>
<tr>
<td>5.0</td>
<td>C</td>
</tr>
<tr>
<td>Temperature Variation</td>
<td>78.4</td>
</tr>
<tr>
<td>Shock &amp; Crash Safety</td>
<td>8.0</td>
</tr>
<tr>
<td>Vibration</td>
<td>18.0</td>
</tr>
<tr>
<td>Water proof</td>
<td>14.0</td>
</tr>
<tr>
<td>Salt &amp; Fog</td>
<td>15.0</td>
</tr>
<tr>
<td>Magnetic Effect</td>
<td>16.0</td>
</tr>
<tr>
<td>Power Input</td>
<td>17.0</td>
</tr>
<tr>
<td>Voltage Spikes</td>
<td>21.9</td>
</tr>
<tr>
<td>Radio Frequency Energy Emission</td>
<td>25.0</td>
</tr>
<tr>
<td>Electrostatic Discharge</td>
<td>A</td>
</tr>
</tbody>
</table>

ATCSIM / AIR TRAFFIC CONTROL TOWER AND RADAR SIMULATOR

ATCSIM is an integrated system that provides realistic training environments for air traffic controllers. It simulates the air traffic control tower environment and radar functions to train air traffic controllers for real-world scenarios.

This system is designed to enhance the capabilities of the air traffic controllers by allowing them to practice their job in a controlled environment. The system provides various features such as a realistic visual experience, radar simulation, and real-time training exercises.

The system is equipped with advanced technology, including 3D modeling, weather simulation, and real-time communication tools. It also offers customizable scenarios to meet the needs of different training requirements.

The ATCSIM system is used by air traffic control centers around the world to improve the skills and abilities of their staff. It is an effective tool for training and maintaining the necessary knowledge and expertise required for the safe and efficient management of air traffic.
ACTSES / AIR TRAFFIC CONTROLLER SELECTION SYSTEM

17 test applications for measuring 9 different skills and one character analysis test are developed. ATCSES tests skills that are required for being an air traffic controller (reflex, three-dimensional thinking, quick decision making, memory, attention, etc.) in an electronic platform.

▪ conscientiousness) and other features like self-confidence, team work, emotional stability.

▪ English Listening Comprehension Test: The ability to understand spoken English
▪ Mathematical Insight Test: The ability to perform fast arithmetic operations
▪ Psychomotor Test: The subject’s ability of hand-eye coordination and reaction speed
▪ Audial Memory Test: The subject’s ability to memorize heard sounds.
▪ Complex Attention Test: The ability to follow the situation without breaking concentration in altering conditions.
▪ Cross-check test: The ability to fulfill the intended duty with following multiple cases
▪ Reasoning Test: The subject’s ability to make correct inferences with analysis.
▪ Visual Memory Test: The subject’s ability to memorize numbers, letters or objects
▪ Mind Picture Test: The ability of mind picturing of possible results of a scenario, according to given data

▪ Item analysis
▪ SPSS analysis of results
▪ Application to different groups
▪ Determination of order of questions in a test
▪ Adjustment of level of hardness, number, percentage and duration of questions
▪ Following state of candidates
▪ 3 sessions for each test group, introducing video, practice operations
▪ Flexible user authorization infra-structure
▪ Automatic session making according to the number of candidates
▪ No interference to questions and results of test
▪ Test on only identified computers
▪ Database security and encryption
▪ Dynamic question production for each test
▪ Addition and removal of new tests
▪ Entrance to the system over web
▪ Turkish-English language support
▪ Supporting all platforms (Win, Linux, Pardus)
▪ 3 sessions for each test group; introducing video, practice operations, adjustment of level of hardness, number, percentage and duration of questions

▪ BIRD-AIRCRAFT COLLISION AVOIDANCE RADAR SYSTEM

The KUSRAD system is designed to operate uninterruptedly 24 hours a day with a coverage volume of a maximum 40 km range in horizontal axis. It can detect targets and classify them as “Bird”, “Flock of birds” and “Aircraft”. It provides operationally targeted data in detecting target range, altitude, heading, mode and trajectory and velocity. The system can be used to track migratory bird movements in critical airspaces and operators can evaluate their route’s safety, and can help in the planning of scheduled flights to reduce accident risk.

▪ Operator Control Panel: The place for connecting and operating the radar system
▪ Operation Center: (Data Recording Unit, Operator Graphical Interface Console, server and storage units, printer and UPS)

COMPONENTS
▪ Radar Location (Shelter): VR, signal processing unit of detection & tracking configuration & monitoring system with vertical & horizontal radar system, meteorological measurement sub-system, GSP system, SAR system, meteorological measurement sub-system, GSP system
▪ Operator Center (Data Recording Unit, Operator Graphical Interface Console, server and storage units, printer and UPS)

FEATURES
▪ 3D Detection & Tracking of avian targets
▪ Classification of avian targets into Bird, Flock of birds and Aircraft
▪ Visual and/or audio operator detection of targets classified as “Bird” or “Flock of birds” in operator defined critical regions
▪ Detailed (Doppler) analysis of any operator designated target
▪ Recording and statistical analysis of detection and tracking skills
▪ Remote access to statistical data and network connection
▪ Vertical and horizontal Radar data fusion
▪ Reporting outputs in ASTERIX standard
▪ Video recording and replay
CIVIL AVIATION SOLUTIONS

DIGITAL RADAR SIGNAL PROCESSING CARD

GOMSIS

GOMSIS is a high performance, scalable microcomputer platform capable of real-time signal processing. It is implemented on a single Power PC card for use in radar applications.

**TECHNICAL SPECIFICATIONS**
- MPC7457 PowerPC processor
- SYSCLK = 166 MHz, 1.27 GHz, 200 MHz DDR
- L3 Cache, MPI-680bus
- MV64460 Bridge Integrated Circuit
- Dual processor support
- 200 MHz (SYSCLK = 166 MHz) DDR SDRAM Memory
- 4* CS, 64 bits, 512 MB
- Device interface for slow interfaces; 5* CS, 133 MHz max. speed
- Devices: USB 2.0 host, 64 MB STRATA Flash, 2* UART
- RTC (32 KB NVRAM)
- 3* Gbit Ethernet interface (2 active) 256 KB SRAM
- 2* PCI-X unit
- 33 MHz, 66 MHz, 133 MHz, 3.3-6.4 bit TMR@32/32 interface B/A EEGFM
- 32 pieces general I/O/POR/Q, Interrupt, Serial lines
- Calibration resistance (Signal driving adjustment)

AIR TRAFFIC SURVEILLANCE RADAR

MGR

This primary surveillance radar (PSR) system is an S-Band solid state pulse Doppler radar. It has been developed for civil or military air traffic control and precipitation status determination.

The system has been designed in accordance with ICAO and EUROCONTROL standards and guidelines. By using coherent advanced signal processing, aircrafts up to 60 nautical miles under different weather conditions can be detected and tracked. The system can simultaneously track up to 1,000 targets via Moving Target Detection (MTD) and Clutter Reduction capability by using low/high beam selection, sensitivity time control (STC), adaptive clutter map and Doppler filter. Also, the weather channel can provide 6 levels of rain strength information at 1.4° to 0.95 nautical miles resolution and 2D location of rain zones. The system has a clean spectrum output in accordance with the limits defined by NTIA.

**TECHNICAL PROPERTIES**
- S-Band solid state pulse Doppler radar
- Coherent signal processing
- Pulse compression (Nonlinear FM)
- PRI/PRF Staggering
- Frequency Staggering
- Doppler filter banks and MTI
- Antenna beam (modified cosecant squared 45° vertical (low and high beam), 1.8° horizontal)
- Circular and linear polarization
- Antenna rotation speed >= 12 rpm
- Max. Range: 60 nmi
- Range resolution: < 200 m
- Power: >=18 kW peak
- PRF: staggered PRF (320 Hz average)
- Doppler processing: >4bank Doppler filtering
- Target tracking speed interval 60-300 m/s
- Maximum number of targets 1,000
- Weather channel resolution 1.4°-0.95 nmi / 6 levels rain information
- Interface PPI console
- System interface EUROCONTROL ASTERIX CAT40/42, CAT34 service messages, ASTERIX CAT040/42 plot

**CAPABILITIES**
- Detection and tracking of airborne targets
- Detection of precipitation level and zones
- User friendly GUI design
- Static (ground) clutter reduction
- Radar remote management and monitoring
- Video recording and playback
- Output reporting in ASTERIX format
ASTERIXCARE
RADAR TEST SOFTWARE

ASTERIXCARE is a powerful and extendible tool set for testing, analysis and validation of surveillance data. The software enables recording, replay and export of recorded data into different formats such as excel, txt, etc.

ASTERIXCARE has user-friendly graphical interface and flexible software for ATC environments and radar system operators. Data is decoded according to ASTERIX which is a Eurocontrol referenced standard.

KEY FEATURES
- Online monitoring: Simultaneous recording and synchronized replay of multiple data streams
- Plug-in based software: New categories can be added
- Expansible radar data into other formats (excel, txt, etc.)
- Offline running is possible by replaying record files
- Radar data recording in ASTERIX final format (Eurocontrol standard)
- Radar data filtering by different parameters
- Traffic and track informations can be displayed in 2D or 3D
- Weather data display
- GPU based graphical display environment and software architecture
- Alerts and notifications for invalid and non-compliant data to standard
- Mode S, ADS-B, ATN2C2 and Multilateration data format support
- Different map layers can be added (e.g. airspace layers)
- Accessing to all ASTERIX data fields
- Zoom, distance measurement, history trail and track labels

AsterixCARE is a powerful and extendible tool set for testing, analysis and validation of surveillance data. The software enables recording, replay and export of recorded data into different formats such as excel, txt, etc.

ASTERIXCARE has user-friendly graphical interface and flexible software for ATC environments and radar system operators. Data is decoded according to ASTERIX which is a Eurocontrol referenced standard.

KEY FEATURES
- Online monitoring: Simultaneous recording and synchronized replay of multiple data streams
- Plug-in based software: New categories can be added
- Expansible radar data into other formats (excel, txt, etc.)
- Offline running is possible by replaying record files
- Radar data recording in ASTERIX final format (Eurocontrol standard)
- Radar data filtering by different parameters
- Traffic and track informations can be displayed in 2D or 3D
- Weather data display
- GPU based graphical display environment and software architecture
- Alerts and notifications for invalid and non-compliant data to standard
- Mode S, ADS-B, ATN2C2 and Multilateration data format support
- Different map layers can be added (e.g. airspace layers)
- Accessing to all ASTERIX data fields
- Zoom, distance measurement, history trail and track labels
**DTKM**

**RAILWAY TRAFFIC CONTROL CENTER**

DTKM provides monitoring and control capability for rail traffic on the railway network. Traffic Control Operators, also known as Dispatchers, are able to fulfill their duties using this system safely and efficiently.

**GENERAL CAPABILITIES**

- **FIELD MONITORING AND CONTROL**
  - Real-time monitoring of the railway network
  - Management of train traffic
  - Single and group control of trackside equipment
  - Real-time visual/audible warnings and alarms
  - Coordination with interlocks, instant monitoring of delays
  - Authorization based user identification
  - Communication with neighboring traffic control centers

- **TRACGRAP**
  - Storage and graphical display of the location-time data of all trains on the network
  - Capability to analyze the traffic density in the network
  - Monitoring of train synchronization between stations
  - Detection of red light violation of the trains

- **PROTOCOL DATA RECORD**
  - All events on the network, commands given to the system and system responses are securely logged for later examination
  - Logs may be retrieved using a wide range of filtering criteria
DAS has been developed to meet the need for reliable, safe and cost-effective interlocking systems for conventional railway lines using commercial off-the-shelf hardware.

The open interfaces of the system provide interoperability with different manufacturers and trackside equipment thus providing the flexibility necessary to meet the interlocking needs of varied railway lines.

The scalable and functional architecture of the system makes it applicable for use with isolated junctions and signals as well as for extensive station regions, whereas the modular architecture leads to expandability. Comprehensive failure detection capabilities provide instant fault diagnosis contributing to the sustainability of system operation.

TECHNICAL SPECIFICATIONS

- Protection Class: IEC/EN 61131-2 (Protection Class II)
- Operating Temperature: 0°C - 60°C
- Humidity: 25°C/55 °C, 95% Relative Humidity
- Operating Voltage: 24 VDC
- Idling Power Consumption: 12W
- Maximum Power Consumption: 192W
- Security Standards: CENELEC SIL4, IEC 61131, IEC 61511, IEC 62061, EN 50156, EN 954, EN 54, EN 13849-1, NFPA 85, NFPA 72, ATEX

TRENSIM is an E43000 electric locomotive simulator using advanced virtual environment technologies for the purpose of carrying out driver training comprised of basic driver training, advanced driver training in varying weather conditions, development of fault and risk avoidance techniques, and monitoring and improvement of driver performance. The E43000 model locomotive simulator has been delivered to Turkish State Railways Eskişehir Training Center.

FUNCTIONS

- To improve train driver skills
- To assure the proper use of cab instruments
- To impart skills necessary in all types of road and climate conditions
- To provide familiarity with operational procedures, speed limits and safety regulations
- To improve use of traction motor and brake for energy efficiency
- To impart experience in handling equipment malfunctions
- To objectively evaluate and score driver’s performance
- To provide distance learning facilities in support of simulator training

GENERAL FEATURES

- 3-D locomotive, wagon, rail line and environment modeling
- Real-rims simulation
- Mathematical models of locomotive behavior (movement, electric, air brake, etc.)
- Cab-mounted simulator on moving platform
- Integrated distance learning
- Real-rims and off-line performance evaluation
ELECTRONIC DOCUMENT AND ARCHIVING SOLUTIONS
EBRU / DOCUMENT TRACKING SYSTEM

EBRU is a document tracking system designed for the security of printed documents. Documents are stamped before print with a specified pattern generated by Ebru system. The stamp process is applied automatically when the document is sent to print within any document processing application. The algorithm of the pattern generator is uniquely developed by TÜBİTAK BİLGEM. With the capabilities of Ebru, it is possible to answer questions like to whom the document was printed, when, and using which printer.

GENERAL PROPERTIES

- **Stamping the Document**: Any document will be stamped with the generated pattern before print.
- **Decoding the Pattern**: With the Stamp Decoder Desktop Application, details of the printed document can be extracted, i.e., the document was printed by whom, when and using which printer, etc.
- **Pantograph**: Invisible specific pattern is used to stamp document to increase the document security. The pattern becomes clear when the document is reproduced with any photocopier.
- **Improved User Interface**: With friendly interfaces users can get results easily.

SYSTEM MANAGEMENT PROPERTIES

- **Adding New Printers**: New printers can easily be added into the Ebru system with the Printer Wizard.
- **User Profiles and Groups**: System allows to add unlimited user profiles and groups.
- **Printer Profiles and Groups**: System allows to add unlimited printer profiles and groups.
- **User Management**: New users can be added easily with the wizard. System allows to assign printer devices for each user or group. System allows to migrate existing users from any user management system into Ebru system. User authorization can be done easily with the friendly interface. System allows to deactivate any user/user group or printer/printer group.
- **Monitoring**: User’s printing behaviours and Ebru usage frequency can be monitored.
- **Search within the Printed Document**: Full text search in printed documents can be done.

*As a result of ongoing research and development, the specifications in this catalogue and its content may change without prior notice.*
SKAAS
DIGITAL STORAGE ARCHIVE AND ANALYSIS SYSTEM

Digital Storage, Archive and Analysis System (SKAAS) digitally stores and analyzes TV and radio channel live contents (video and audio) of satellite, cable, terrestrial and IPTV broadcasters. The system is compatible with International Standards and adaptable to future broadcast technologies. It is capable to stream, archive and analyze up to 400 TV and 1500 radio channels, simultaneously. It has almost unlimited storage capacity.

GENERAL FEATURES
▪ TV and radio channels can be received from satellite, cable, terrestrial and internet medium continuously and hierarchically
▪ IP streaming (PTV) for operators on the local network
▪ Media files can be stored for unlimited time
▪ Scene boundaries, channel logos can be detected, video clips can be searched on video files, texts can be extracted from video and keyword scan be captured from audio files
▪ High Availability; observation of signal level and state of broadcast, and automatic switching to redundant device
▪ Hundreds of users can watch/listen stream and archive, and give analyzing orders at the same time without any bottleneck
▪ Two-step archive architecture; short term files are stored with high resolution in primary storage, long term files are stored with lower resolution in secondary storage
▪ Checking of archive records against damage and distortions
▪ Authorized users can upload or update records
▪ Support to any size of TV Wall for both live streams and recorded content

RECEIVER INPUT
▪ SD and HD broadcasts in DVB-S, DVB-S2
▪ Encrypted broadcasts
▪ Analog TV and radio broadcasts
▪ DVB-T terrestrial digital broadcasts
▪ Analog and digital Cable (DVB-C) broadcasts
▪ Internet TV and radio (IPTV Streams)

RECEIVER OUTPUT
▪ H.264 coded IPTV streams in selected bitrate and resolution
▪ MP3 coded Radio streams in selected sample rate and bitrate
▪ MPEG2 Transport Stream support (ISO/IEC 13818-1)
▪ File Recording according to time duration or size

ARCHIVE MANAGEMENT SYSTEM
E-BELGEM
ARCHIVE MANAGEMENT SYSTEM THAT COMPLY WITH TSE STANDARDS
Records in paper form can be digitally recorded in the Electronic Record Management System (E-BELGEM) using fast and precision scanners. E-BELGEM provides advanced features such as metadata modifications and recent modifications on the records for operators.

DOCUMENT DIGITIZATION
▪ Drag and drop
▪ Microsoft Office and Email import integration
▪ Optical Character Recognition (OCR)
▪ Advanced precision and fast scanner integration

RECORD SHARING
▪ Common Work Area and Folder Sharing
▪ Document and Workflow Management
▪ Preview
▪ Record Content Annotation
▪ Electronic Record Management
▪ Institution-specific Taxonomy Tree
▪ User-specific Control Panel

EFFECTIVE AND FAST ACCESS TO ARCHIVE RECORDS
▪ Simple search
▪ Custom search
▪ Detailed search

E-SIGNATURE AND VIRTUAL NAVIGATION
▪ E-signature screen
▪ Virtual Navigation
▪ Detailed Search

SYSTEM MANAGEMENT
All system management configurations are performed on the system management page that can be accessed from the main page. Only the system administrators are authorized to use this feature. A few tasks that can be executed on this page:
▪ Users and Groups definition
▪ User Role and Authorization
▪ Record Type definition, Record Type metadata and Record Type group definition
▪ Repository definition
▪ System Settings and List

ARCHIVE MANAGEMENT SYSTEM THAT COMPLY WITH TSE STANDARDS
Records in paper form can be digitally recorded in the Electronic Record Management System (E-BELGEM) using fast and precision scanners. E-BELGEM provides advanced features such as metadata modifications and recent modifications on the records for operators.

DOCUMENT DIGITIZATION
▪ Drag and drop
▪ Microsoft Office and Email import integration
▪ Optical Character Recognition (OCR)
▪ Advanced precision and fast scanner integration

RECORD SHARING
▪ Common Work Area and Folder Sharing
▪ Document and Workflow Management
▪ Preview
▪ Record Content Annotation
▪ Electronic Record Management
▪ Institution-specific Taxonomy Tree
▪ User-specific Control Panel

EFFECTIVE AND FAST ACCESS TO ARCHIVE RECORDS
▪ Simple search
▪ Custom search
▪ Detailed search

E-SIGNATURE AND VIRTUAL NAVIGATION
▪ E-signature screen
▪ Virtual Navigation
▪ Detailed Search

SYSTEM MANAGEMENT
All system management configurations are performed on the system management page that can be accessed from the main page. Only the system administrators are authorized to use this feature. A few tasks that can be executed on this page:
▪ Users and Groups definition
▪ User Role and Authorization
▪ Record Type definition, Record Type metadata and Record Type group definition
▪ Repository definition
▪ System Settings and List
National Marker Control System is used to prevent distribution of the fuel oil which is obtained through unregistered production or smuggling. The system is developed to control the fuel market in the most efficient way and increase the tax revenues.

The system is consisted of MARKER XP National Marker Field Control Devices which are used in field controls to measure the marker concentration, MARKER K National Marker Laboratory Control Devices which are used to measure this concentration in the laboratories of fuel distribution companies, and Data Collection Center.

Marker measurement results are obtained in field or laboratory conditions through 3 different optical spectroscopy method in 400-1000 nm spectrum region. Then, these results are instantly encrypted and sent to the Data Collection Center through GSM-GPRS. Furthermore, a measurement report is taken from device’s printer. Measurement date, time, location, temperature, type of the fuel, serial number of the control device and registration number of the control personnel are indicated in this report. Statistical data mining transactions are carried out to the obtained results in the Data Collection Center.

The system is used by Police, Gendarmerie, Coast Guard, Undersecretariat of Customs, Ministry of Science, Industry and Technology, oil refineries, fuel stations, transportation tankers and storage fields to detect and control fuel smuggling.
The hyper spectrum measurements technology is employed for the first time in the next generation questioned documents examination devices which are developed and produced by TÜBİTAK BİLGEM. Hence, several cases about forgery of documents which could not be enlightened by the present technological devices were able to be solved.

Forensic XP-4010 D is developed to examine the originality of documents. Forensic XP-4010 D driven by the hyper spectrum measurements technology helps reveal of forgery of documents like money, cheques, documents and passport. Among the other important features of Forensic system one should note the non-destructive principles of examination, decision making based on objectively measured optical parameters of the document.

Forensic XP-4010 D is an advance spectrograph using hyper spectrum measurements.

**FEATURES**
- Hyperspectral imaging in 350-1100 nm spectrum range
- Revealing the presence of visually similar, but chemically different ink by original Spectral Enhancement Procedures
- Revealing invisibly embedded or deleted information
- UV activated security features examination
- Anti-Stokes features examination
- Pen pressure visualization and trace display using 3D technology
- Numerical imaging filter
- Passport machine readable zone and chip decoder
- Revealing passport hidden data

**MEASUREMENTS**
- Sensitive reflectance, absorbance and conductivity spectral measurements
- Color in any pixel FOV, XYZ, xy, Lab, Statistics
- Distance, Radius, Angle Y
- Rectangle area, any selected area Y
- Height (3D Shadowing)

**PRODUCT FEATURES**
- Nd: YAG Sensitivity
- High Speed and Accuracy
- Low Capacitance, High Breakdown Voltage
- Ultrafast Response
- Wide Dynamic Range
- High Responsiveness

**APPLICATIONS**
- Pulse Detectors
- Optical Communications
- Bar Code Readers
- Optical Remote Control
- Medical Equipment
- High Speed Photometry

**QUADRANT PHOTODETECTORS**
DDA-1 quadrantal photodetectors have four parallel PIN-diodes on the same silicon substrate. These detectors are optimized for high response at 1064 nm, the YAG laser light wavelength, and other higher responsiveness and wider dynamic range compared to similar products on the market. DDA-1 quadrantal photodetector technology is developed and produced entirely by TÜBİTAK BİLGEM.
GEZKIY / REAL-TIME IR TRACK PREDICTION AND MANAGEMENT SYSTEM

GEZKIY HARDWARE FEATURES
- Low and high temperature sensors
- Connection boxes
- GEZKIY main panel
- Panel computer
- Ethernet key and power unit

KEY SOFTWARE FEATURES
- Platform radiation images at desired frequencies
- 3-5 micron and 8-12 micron bad selection capability
- Suggestions for profile reduction
- System start/stop and test capability
- Warning in case of system failure

Key software features
- Showing of threat zones on polar screen
- Adding/deleting of threat models

REAL-TIME IR TRACK PREDICTION AND MANAGEMENT SYSTEM

FIBER OPTIC CABLE AUDIT SYSTEM

FKGS

SECURITY FEATURES
- User authentication with smart card and password
- Secure communication using SSL
- Integrated man/machine interface
- Flexible role-based access control
- Two step inventory change approval
- Contracting audit

FEATURES
- Inventory management of fiber optic cables, fibers, T connection boxes, buildings, manholes, poles, maintenance shares, cable segments, ODFs, links, fiber optic cable profiles, reference points
- Failure intervenes information management
- Detection of cable rupture, twist, aging, splice and connector losses
- Alarm generation according to the user defined thresholds and indication on geographical map
- Active and dark fiberoptic line tracking
- Alarm and incident reporting of measurements and alarms
- Forwarding of alarms by SNMP, e-mail and SMS
- Secure data change
- Support for warm stand-by management center
- High accuracy using 3D geographical coordinates
- Flexible configurable CBS base layers
- Inventory information gathering by field studies
- Internal messaging support between operators
- Auto updated web based user interface

GEZKIY

GEZKIY features
- Low and high temperature sensors
- Signal converters
- Connection boxes
- GVDS interface
- GEZKIY main panel
- Panel computer
- Ethernet key and power unit

KISY SOFTWARE FEATURES
- Platform radiation images at desired frequencies
- 3-5 micron and 8-12 micron bad selection capability
- Suggestions for profile reduction
- System start/stop and test capability
- Warning in case of system failure

KIKTY SOFTWARE FEATURES
- Showing of threat zones on polar screen
- Adding/deleting of threat models

FIBER OPTIC CABLE AUDIT SYSTEM

FKGS

Fiber optic wires' optical measurements are done by Remote Audit Units (UDB), which are controlled by Central Audit Unit (MDB) and detected actual and potential failures are reported to the user along with geographical coordinates.

FEATURES
- Inventory management of fiber optic cables, fibers, T connection boxes, buildings, manholes, poles, maintenance shares, cable segments, ODFs, links, fiber optic cable profiles, reference points
- Failure intervenes information management
- Integrated geographical information system
- Detection of cable rupture, twist, aging, splice and connector losses
- Alarm generation according to the user defined thresholds and indication on geographical map
- Active and dark fiberoptic line tracking
- Alarm and incident reporting of measurements and alarms
- Forwarding of alarms by SNMP, e-mail and SMS
- Secure data change
- Support for warm stand-by management center
- High accuracy using 3D geographical coordinates
- Flexible configurable CBS base layers
- Inventory information gathering by field studies
- Internal messaging support between operators
- Auto updated web based user interface
- Automatic updating of inventory information gathered by field studies
- Internal messaging support between operators

Passive threats against frigates platforms make use of the infrared radiation. GEZKIY system helps the commanding officer of the platform to see the platform itself by the eyes of the potential threats and to manage the platform accordingly. The system consists of thermal sensors mounted on various places and weather and sea water heat, wind speed and other meteorological information gathered from the ship data distribution system and calculates the infrared profile of the platform with the KISY software. KITY software then shows the potential threat areas of the platform to the commanding officer. GEZKIY system is being used on Heybeliada and Buyukada ships, which are produced within the MILGEM program.

GEZKIY has been developed to manage the fiber optic network including the geographical coordinates and audit the network against wear, rupture and eavesdropping events.
EMBC
ELECTRO-OPTICAL MODULATION DETECTION DEVICE

Light can be used as a data and voice transfer device. Therefore, there is a need to detect the undesired electro-optical transmitters in the critical fields. EMBC can detect these undesired electro-optical transmitters and reveal the features of these transmitters and transmitted signals by using VETESIS-Transmitter Detection Device (another device developed by TÜBİTAK BİLGEM). EMBC can be tested by EMBC-Test Device if required because of the operational conditions.

SPECIFICATIONS
- Detectable Wavelength Range of the Light: 450-950 nm
- Detectable Modulation Frequency Range: 1 kHz-100 MHz
- Power Consumption: 720 mW
- Operating Time: > 1 hour
- Size: 198 mm x 57 mm x 51 mm (Portable)
- Operating Temperature: 0°C ~ 50°C
- Operating Humidity: %20 ~ %80
- TS EN 60529 IP23 Leak-proof Standard
- MIL-STD-810G Vibration Standard
- State of Charge Indication
- Ability to work with internal battery and charging kit

SPECIFICATIONS OF EMBC TEST DEVICE
- 780 nm Infrared Transmitter
- Adjustable Modulation Frequency: 10-200 kHz

* As a result of ongoing research and development, the specifications in this catalogue and its content may change without prior notice.
As a result of ongoing research and development, the specifications in this catalogue and its content may change without prior notice.

**STAMPS / CENTRALIZED CYBER THREAT SENSOR SYSTEM**

**FEATURES**

One of the biggest problems of corporate networks dispersed to multiple locations is monitoring and reacting to cyber threats in real-time from a single center. Cyber attacks targeting any node on the corporate network may be detected immediately with the Centralized Cyber Threat Detection System, which is developed for this specific purpose. Installing attack detection systems on the critical nodes of the corporate network lets you monitor the cyber attacks targeting the whole network from a single center. Installed attack detection systems may be configured/managed centrally. System may be customized due to requirements of corporations working on a distributed network architecture.

**CAPABILITIES**

- Distributed attack detection system infrastructure
- Monitoring all logs from a single point, featuring cyber-threat detection interface
- Scalable architecture
- Monitoring all logs from a single point with the underlying log fusion layer
- Detecting malicious activities in real-time with blacklist and cyber-threat intelligence support
- Creating new blacklists to define rules lists for filtering systems
- Advanced report module (PDF, HTML, XML, JSON)
- Centralized IDS configuration/management module
- Real-time monitoring of the logs
- Geographic awareness map that is being updated in real-time
- Integrated operation with Cyber Space Trap System (SORT)
Cyber attacks to various countries in the recent years is an indicator that Internet has become a battlefield. Cyber Threat Detection and Prevention System is based on detection of threats by systems implemented at critical network connection points and activating defense mechanisms on all systems to block the threats and is a major actor of the cyber defense. The system consists of distributed cyber traps, distributed attack detection systems, virtualization systems and central management system.

This system can be customized in accordance with the requirements and can be used by organizations which have distributed network architecture.

**CAPABILITIES**
- Capability to work with different trap systems supporting different network layers
- Distributed trap systems infrastructure
- Low cost trap systems router device usage
- Management of thousands of trap systems by Cyber Trap System Management Interface
- Rule management of all attack detection systems from a single point
- Scalable architecture
- Powerful virtualization infrastructure and management
- Classification of detected harmful software by Harmful Software Screening System
- Integrated Harmful Software Dynamic Analysis Environment
- Monitoring of all logs by powerful log collection infrastructure
- Detection of harmful software distributed via e-Mails by anti-spyware-Mail analysis
- Detection of harmful activities with blacklists
- Introduction of new rules to the filtering systems with the capability of generating new blacklists
- Advanced reporting system
- Centralized operation with Centralized Cyber Threat Sensor System

**FEATURES**
- Data Leakage Prevention System is being developed to protect corporate information and to prevent unauthorized leakage of this information from the organization. This system is one of the major security infrastructure requirements of both public and private organizations.

VKOS will trace network traffic at corporate gateways, tools information being processed at user terminals, audit whether information stored on servers is stored at proper locations and with proper policies and prevent data leakage at all locations.

This product, which currently supports Turkish language and text mining, distinguishes itself from competing systems with its performance. This system can be customized according to specific customer requirements and can be integrated with other security solutions at Cyber Security Institute.

**CAPABILITIES**
- Centralized web-based management
- Online and offline functioning capability of the agents
- Centralized discovery of information in MS, OLE, DDE, etc. media
- Controlled file transfer via FTP, TFTP, SMTP and FTP protocols
- Specific audits for MS, SQL and database servers
- Prevention of data leakage via screen capture devices
- Definition of sensitive data at file, process and expression levels
- Central management and reporting of data leakage incidents

**SUPERIORITY**
- Based on corporate software development practices
- Support for the language of customer and morphological analysis
- Detection of sensitive data using text mining
- Usage of sensitive data definitions specific to the required language
- Control of operating system drivers level
- Minimal performance reduction with acceptable levels of resource allocation
One of the important approaches to assuring the security of corporate IT systems and applications is moving the IT systems to a virtual environment. All sorts of attack and defense scenarios maybe executed and verified on that virtual environment. “SiberMeydan CTF” product includes scenarios featuring all kinds of vulnerabilities that may be found on network components, clients, servers and corporate services. Common exercises or team competitions maybe conducted on SiberMeydan CTF environment. Different types of competitions such as “Capture the Flag” or “Defend Yourself and Penetrate the Enemy” maybe applied. Several application interfaces are available to monitor the performance of plunders and general state of the competition. SiberMeydan CTF environment has been successfully field tried in National Cyber Exercise 2013, Cyber Security Summer School with restricted set of scenarios and in SiberMeydan UNİ 2013 with extended set of scenarios and all features.

**CAPABILITIES**

- Completely virtual simulation environment
- Around 120 related attack and defense scenarios.
- Simulation of ALL COMPONENTS of a common corporate network.
- Ability to work in the environment as a member of red or blue teams.
- Detailed documentation of scenarios and correlations among scenarios, including vector diagrams.

**SUPERIORTIES**

- Regular update of simulation environment and scenarios due to new experiences.
- Stable simulation environment.
- Generic content.
- Features designed for training.
- Covers qualifications related to multiple fields of expertise.

**CONSULTANCY FOR THE DEVELOPMENT OF SECURE SOFTWARE**

Security is not an add-on feature that could be added to a system or software. But instead, it should be evaluated as part of the development process. Implementation of security functions during the processes of development and installation is both easier and more effective.

SGE provides the following services to public and private organizations/institutions:

- Trainings for the secure software development
- Software source code analysis in order to detect vulnerabilities during the development of software
- Risk analysis and threat modeling with the purpose of making secure software development processes more efficient
- Search and implementation of new secure software development methods
- Conduct of workshops and conferences on the development of secure software

Within the scope of these services, SGE has added NATO many projects related to information system development. For the security accreditation of these system and software projects, the institute has presented consultancy regarding secure system design and the preparation of accreditation documents and also carried out the security tests of the developed systems. Within the scope of these services, SGE has aided NATO many projects related to information system development. For the security accreditation of these system and software projects, the institute has presented consultancy regarding secure system design and the preparation of accreditation documents and also carried out the security tests of the developed systems.

**IT PRODUCT SECURITY**

IT Product security-oriented studies are implemented within the IT Product Security Laboratory of the Cyber Security Institute. Security analysis of IT products is achieved through evaluating, testing and attacking weaknesses and vulnerabilities of the security functions. Risk analysis and penetration tests are carried out for smart card chips, operating systems, cryptographical memories, smart card readers, hardware security modules, network security products, security application software and secure environment modules.

IT Product Security Laboratory closely follows state of the art changes within the field, developing new attack techniques to detect security vulnerabilities.

IT Product Security Laboratory has proven to be at the same expertise level with its international counterparts, thanks to its active and passive side channel analyses and reverse engineering attacks especially on smart cards and smart crypto chips. The laboratory also provides technical aid to the Common Criteria Center (OKTEM) within TÜBİTAK BİLGEM in the work conducted pursuant to ISO/IEC 15408.
Cyber Security Services

Penetration Tests
Cyber Security Institute (SGE) conducts penetration tests and security audits both on state institutions/organizations and private sector companies. These penetration tests and security audits encompass all components of the information infrastructure. Upon the completion of these tests, detailed technical reports and executive summaries are established. Additionally, to increase awareness of the personnel on security, social engineering tests are implemented along with technical security tests.

In order to carry out tests that are supported by standards and efficiency, CSi researchers seek and develop new exploitation methods and tools.

Another emphasis within this scope is on information sharing. Apart from the above-said security tests, there are efforts to enhance the capacity of tests on information sharing. To this end, workshops are organized with the objective of determining the scope and depth of the tests, increasing the quality and objectivity of test results. Besides, joint projects are carried out with the organizer institutions.

Cyber Security Institute (SGE) conducts penetration tests and security audits both on state institutions/organizations and private sector companies. These penetration tests and security audits encompass all components of the information infrastructure. Upon the completion of these tests, detailed technical reports and executive summaries are established. Additionally, to increase awareness of the personnel on security, social engineering tests are implemented along with technical security tests.

In order to carry out tests that are supported by standards and efficiency, CSi researchers seek and develop new exploitation methods and tools.

Another emphasis within this scope is on information sharing. Apart from the above-said security tests, there are efforts to enhance the capacity of tests on information sharing. To this end, workshops are organized with the objective of determining the scope and depth of the tests, increasing the quality and objectivity of test results. Besides, joint projects are carried out with the organizer institutions.

Risk Analysis
Cyber Security Institute (SGE) provides information security risk analysis service to defence, public and private sectors. Both software and system level risk analysis projects are conducted. Corporate level risk analysis service is also provided in the scope of ISO 27001 certification.

In this scope, business processes are analysed, critical processes are identified, asset dependencies are determined and evaluated. In this phase, data flow charts are created as well. Afterwards, the probability and impact values of the potential risks acting on the assets are calculated and the identified risks are documented in detail in accordance with the project context. On hand of the derived risks, security requirements are identified from a list including the controls from ISO 27001 and NIST SP 800-53 standards and documented congruent with the project context. Security requirements and their maturity levels are discussed with the customer.

Lastly, the residual risks left after applying the security measures are evaluated at the final step. The MAGERIT Version 2 methodology and the PILAR tool is utilized to realize the risk analysis.

Cyber Security Institute (SGE) conducts penetration tests and security audits both on state institutions/organizations and private sector companies. These penetration tests and security audits encompass all components of the information infrastructure. Upon the completion of these tests, detailed technical reports and executive summaries are established. Additionally, to increase awareness of the personnel on security, social engineering tests are implemented along with technical security tests.

In order to carry out tests that are supported by standards and efficiency, CSi researchers seek and develop new exploitation methods and tools.

Another emphasis within this scope is on information sharing. Apart from the above-said security tests, there are efforts to enhance the capacity of tests on information sharing. To this end, workshops are organized with the objective of determining the scope and depth of the tests, increasing the quality and objectivity of test results. Besides, joint projects are carried out with the organizer institutions.

Risk Analysis
Cyber Security Institute (SGE) provides information security risk analysis service to defence, public and private sectors. Both software and system level risk analysis projects are conducted. Corporate level risk analysis service is also provided in the scope of ISO 27001 certification.

In this scope, business processes are analysed, critical processes are identified, asset dependencies are determined and evaluated. In this phase, data flow charts are created as well. Afterwards, the probability and impact values of the potential risks acting on the assets are calculated and the identified risks are documented in detail in accordance with the project context. On hand of the derived risks, security requirements are identified from a list including the controls from ISO 27001 and NIST SP 800-53 standards and documented congruent with the project context. Security requirements and their maturity levels are discussed with the customer.

Lastly, the residual risks left after applying the security measures are evaluated at the final step. The MAGERIT Version 2 methodology and the PILAR tool is utilized to realize the risk analysis.
MALWARE ANALYSIS

Among the most widely seen cyber-security threats at the level of end users are viruses, trojan horses, backdoors and worms. Nowadays, malicious software is not only used for financial fraud, but also for obtaining confidential information and damaging information accessibility. Developed countries that have a good grasp of the importance of the issue, make significant investments in keeping their protection mechanisms updated. In this direction, the Cyber Security Institute Malware Analysis Unit closely follows the current malware trends and analyzes the malware which may pose a huge threat to Turkey’s infrastructure and services that are of critical importance. Results and counter measures deriving from these analyses are shared with relevant institutions via information sharing platforms.

Especially in today’s world, malicious software could pose a huge threat when used for cyber espionage under the name of Advanced Persistent Threat (APT). Countries may use malware either to negatively influence the critical infrastructure of other countries or to acquire their sensitive information. Upon demands from critical public institutions or private corporations, CSI conducts investigations to detect and deal with such threats.

UNDERWATER DEFENSE SYSTEMS
DABIS
SUBMARINE BATTERY MONITORING SYSTEM

DABIS is a monitoring and recording system for submarines. It measures, displays and records voltages of 480 batteries, temperatures of 24 pilot batteries, currents of 4 battery groups. Battery capacity is calculated from these measurements. Fault thresholds can be set by the user. In case of any failure, the system warns the user by audio and visual feedback while failure is logged. DABIS system is currently being used in 10 submarines.
**DATAS**

**SUBMARINE TACTICAL SIMULATOR**

DATAS is a tactical and operational training simulator for submarine commanders and combat teams. The system generates different training scenarios for search, engagement, attack and avoidance.

**USAGE**

DATAS is located on shore and consists of three physical sections.

- **Training Control Room**: In this room trainers control the simulation system, prepare and run training scenarios.
- **Central Room**: Room where the trainees take tactical and operational decisions and perform the training.
- **Debriefing Room**: Room for the evaluation of training results with the assistance of debriefing tools.

**GENERAL CAPABILITIES**

- Submarine Control Rooms Systems and Consoles Simulation
- Cylindrical Array Sonar
- Flank Array Sonar
- Passive Ranging Sonar
- Velocir Passive sonar
- Active sonar
- Radar and ESM (Electronic Support Measures)
- LINK/ROL-11
- Torpedo and guided missile
- Fire Control and Target Motion Analysis (TMA)
- Submarine navigation and diving simulation
- Dead Reckoning Table simulation
- Underwater environment modeling
- Platforms and embitter noise modeling
- Acoustic propagation modeling (Normal Mode and Ray Trace)
- Autonomous reacting target modeling
- Application of Unit Submarine Warfare (USW) Tactics

**SEDAVER**

**SCENARIO BASED SUBMARINE DATA PACKAGE GENERATOR**

SEDAVER is the software for generation of data packages of command and control, launcher, firing station, etc. systems in accordance with actual communication protocols.

**GENERAL CAPABILITIES**

- Adaptation to different submarine classes
- Editing threat status as scenario
- Two dimensional scenario realization
- Online scenario update
- Scenario based submarine data package generation
- Submarine navigation data
- Submerged environment measurement data
- Submarine information distribution system compatible data package generation
- Data package transmission over RD-232/RS-422/Ethernet

**LAUNCHER SYSTEM SIMULATION**

- Launcher data package generation
- Launching data package
- Programming of decoys and jammers in casings
- Decoy and jammer launched orders
- Built-in Test (BIT)

**FIRESTATION SIMULATION**

- Firing station data package generation
- Programming of decoys and jammers at firing station
- Firing station self status information query
- Internal test
DAKA / BTBM

ACOUSTIC DECOY DEVELOPMENT FOR SUBMARINE / QUEST OF ACOUSTIC REACTIONS FOR ANTI-TORPEDO

DAKA / BTBM is the modeling and simulation tool for decoy and jammer release and evasive maneuvers for submerged platforms and surface vessels under torpedo threat.

SIMULATION CAPABILITIES

▪ Defining Torpedo tactics
  ▪ Avoidance maneuver
  ▪ Defining torpedo guidance modes and release sequence
  ▪ Defining threat situation as scenario
  ▪ Defining Sound speed profile
  ▪ Defining sea bottom type and profile
  ▪ Defining Torpedo threat
    ▪ Heavy/light torpedo selection
  ▪ Defining Torpedo guidance behavior and sonar
  ▪ Defining Acoustic decoy and jammer
  ▪ Defining submerged platforms/surface vessels and sonar payloads

ANALYSIS CAPABILITIES

▪ Torpedo/platform/decoy/jammer dynamical analysis
  ▪ Torpedo phase change analysis
  ▪ Torpedo and platform sonar data analysis
  ▪ Acoustic decoy/jammer data analysis
  ▪ Successful/failed tactics analysis
  ▪ Most successful tactic selection
  ▪ Tactic comparison
  ▪ Forward/reverse replay on time axis
  ▪ Analysis report generation
  ▪ Data transfer to Microsoft Excel
  ▪ Defining RUN by scenario and tactics
    ▪ Single run: Two dimensional animation and pre-analysis
    ▪ Multiple run: Statistical analysis
  ▪ Display of online data of the simulation run
  ▪ Replay at various speeds

MODELING CAPABILITIES

▪ A world of Degrees of Freedom (DoF): dynamic modeling
  ▪ Underwater acoustic propagation modeling (Ray Tracing)
  ▪ Sonar and movement modeling in accordance with torpedo phase
  ▪ Modeling of torpedo detection, evasion and decoying behavior of decoys
  ▪ Modeling of noise emission behavior of jammers

SONOBOY

FLOATING PLATFORM POSITIONING DEVICE

Sonobuoys are important devices of anti-submarine warfare. They are used for positioning submarines. Sonobuoys are dropped from ship, aircraft or helicopter after selection of operating time, depth and channel.

Sonobuoys use acoustic sensors to convert underwater sounds to electrical signals. The electrical signals from acoustic sensors are transmitted to aircraft or to ship which has sonobouy receiver.

SPECIFICATIONS

▪ Type: Passive and directional (DIFAR)
  ▪ Frequency range: 5-2400 Hz
  ▪ Operational depth: 30-100 m
  ▪ Operational time: 1, 2, 4 and 8 hour
  ▪ Deployment altitude: 30,000 ft (max)

USER INTERFACE

▪ 2 button operation, 7-segment and LED displays

ELECTRICAL SPECIFICATIONS

▪ Replaceable batteries
  ▪ Sea battery (Mg-CuI)
  ▪ Control battery (Li)

MECHANICAL DESIGN

1-Omni Sensor
2-Vectoral Receiver
3-Inert Mass

ACOUSTIC SENSOR
**DRT TABLE**

**DIGITAL DEAD RECKONING TABLE**

The DRT (Dead Reckoning Table) is a PC-based plotting table for navigational and tactical data used in the Combat Information Center (CIC).

**NUMERICAL PLOTTING TABLE**

The DRT displays the ship's position, speed and heading information on its 40” display using data gathered from various navigational sensors. Also, plot information received from navigation radar can be seen on display. Therefore, own ship and targets related navigational information is to be displayed, monitored and plotted on digital map. S-57 and S-63 digital map formats are used and all information coming from sensors are displayed in real-time.

**PHYSICAL CHARACTERISTICS**

- 40” FULL-HD LCD Display
- Keyboard and Touch-ball for user input
- NMEA 0183 compliant sensor interface
- COTS hardware design
- Ergonomic design
- Easy access to internal parts
- System status indicators
- Dimensions: 1210 mm x 1200 mm x 1100 mm
- Weight: < 250 kg
GIS REAL-TIME OPERATING SYSTEM

GIS

GIS is the first and only hard real-time operating system (RTOS) developed in Turkey. GIS is intended to improve current avionics system design and integration capabilities, which is part of safety critical systems. GIS aims to fill the technological gap in RTOS industry for Turkey. It is developed to be used in a wide range of applications. It is flexible and scalable for working on different platforms. GIS consists of several architectural modules which enable it to easily modify and integrate to various platforms including military and civil embedded system applications.

"MEETS THE REQUIREMENTS OF SAFETY CRITICAL SYSTEMS"

GIS is developed from ground-up according to the guidelines of DO-178B Level A. GIS can be used both in ARINC-653 mode which supports safety critical application interfaces, and also in PSE-51, PSE-52 or PSE-53 modes defined by POSIX. GIS comes with an integrated development environment called TGO. TGO is an Eclipse based integrated development environment which provides system integrators with features like application development, mode selection, debugging, event analysis and simulation.

"INTEGRATION TO DIFFERENT ARCHITECTURES"

GIS has a modular design with Architecture Support Package (ASP) and Board Support Package (BSP) layers, which enable it to easily be ported to run on different micro-processor families or different boards. It also has a safety critical graphics library, OPENGL SC, to meet the needs of graphic based applications.

"COMPATIBILITY WITH ARINC 653 AND POSIX STANDARDS"

ARINC 653 and POSIX compliances are tested with a wide range of applications and test suites. The system tests included cooperation with other real time operating systems running on other boards. These tests confirmed the compliance of standards. GIS will become prevalent by replacing other real time operating systems running safety critical systems.

"IT REDUCES FOREIGN DEPENDENCY FOR DEFENSE AND PRIVATE SECTOR"

GIS prevents critical data theft in secret projects and provides being hundred percent national for embedded systems. Since, GIS reduces the costs, Turkish industry will reach a competitive level in the international rival and new SME companies would be established as well.

ETMTS-2 HAND-HELD MINE DETECTION SYSTEM

ETMTS-2 is a new generation dual sensor hand-held mine detection system containing both Metal Detector (EMI) and Ground Penetrating Radar (GPR). The system is capable of operating in challenging military conditions.

ETMTS-2 device runs on two main modes, which are detection and identification. Audio warnings about the detection of targeted targets are given to the operator by headphone or external speaker, and visual warnings are shown on LCD screen. Therefore, user may create his own identification decision through the audio-visual information produced by the system. The device is a "black box" (BT) both in start up and during operation, which provides reliability. Data from the sensors, system warnings and battery level status are displayed on the screen. The system can communicate with the outer World through an Ethernet port if needed.

The operator can detect and localize both metallic and non-metallic buried mines and IEDs along a scanning path and can visualize suspicious territory and generate a prediction about the type of the buried objects utilizing automatic classification software.

The system is compatible with the military standards MIL-STD 810G and MIL-STD 461F. Underground visualization can be obtained with high gain planar antenna structure and metals can be detected with high sensitivity via optimally designed search coil.

SENSORS

▪ EMI (Electromagnetic Induction) Sensor
▪ GPR (Ground Penetrating Radar) Sensor

CAPABILITIES

▪ Detection of metallic mines
▪ Detection of non-metallic mines
▪ Detection of IEDs
▪ Detection of metal objects
▪ Precise target containing by audio-visual warnings.
▪ Self-training capability to the operator.
TAKSIS
TACTICAL TRAINING SYSTEM

TAKSIS (Tactical Training System) is an embodiment simulation system intended for the urbanized area training of SWAT forces.

TAKSIS:
Special suits with hit detection capability, weapons generating laser beam and having realistic blow-back mechanism, high accuracy positioning system, hand grenade and blast bomb, bready traps, powerfull sound systems and smart camera system forming and room training are the main components of the system. Personal, team and tactics based performance evaluation can be executed by using the real-time data acquired during the operation and the results can be extracted as detailed reports. It is also possible to carry out debriefing for a more detailed analysis by simultaneously replaying the video streams and animation displayed on tactical area layout.

SPECIFICATIONS

- High level of similarity to real operational area
- Mutual combat with moving targets
- Laser beam weapons with realistic blow-back mechanism
- Specially designed training suits with hit detection capability
- Emulative hand-grenades, blast bombs and bready traps
- Powerful sound system playing high intensity explosion sounds of weapons and ammunitions
- Reusable training materials
- 2D indoor and outdoor positioning system
- Operation monitoring via video stream and simultaneous replay
- Screens for scenario creation, tactics definition, operation tracking on tactical area layout
- Individual, team and tactics based performance evaluation and analysis

HIGH LEVEL OF SIMILARITY TO REAL OPERATIONAL AREA

Equipment is same as the originals in appearance and weights such as hand-grenade, blast bombs and bready traps enable trainees to battle in a training area same as the real ones. Realistic sounds of bombs and weapons make up challenging battle medium for trainees. Weapons equipped with a blow-back mechanism and generating intensive explosive sounds make trainees gain realistic experience.
SiMA is a simulation modeling and execution framework that aims to significantly reduce the development time of simulation applications. SiMA provides both an abstraction for system modeling and a protocol for executing and synchronizing the simulation of the modeled system, which provides a well-defined approach for constructing scalable and hierarchical models of complex systems. SiMA is primarily written in .NET environments but can interface to pure C++ simulation models. In addition, SiMA includes a Distributed Simulator Module that can act as an adapter to various external distributed simulation infrastructures such as HLA.

**GENERAL CAPABILITIES**

- Discrete Event System Specification (DEVS) Formalism
- Re-usable model development
- Flexibility to develop different simulations with different model compositions
- Development of models in C++, and .NET Environments
- Fast model development processes with code generation tools
- Recording of simulation inputs and outputs
- Distributed Simulation Development support
- Interaction with HLA/RTI adapted simulations
MARSsys / MANAGEMENT AND ANALYSIS OF RADIO SPECTRUM SYSTEM

MARSsys is the unique solution satisfying both military and civil operational requirements through its integration into a wide range of spectrum management capabilities at national and international levels. By having a full support for NATO SMADE-XML data exchange standard thus giving an international coordination capability in spectrum management, MARSsys is considered as one of the most advanced software in spectrum management field. MARSsys offers access control with role based authorization and security levels on a hierarchical organization structure. Frequency assignment process, frequency request and interference messaging process, interference analysis and clear frequency assignment, coverage and interferences analysis for various system types and frequency bands are some key functional features of MARSsys.

SMAS (TECHNICAL ANALYSIS MODULE) CAPABILITIES

▪ ITU-R compatible propagation models for LF/MF-HF-V/UHF-Radar-Radio Link bands (3KHz- 52 GHz)
▪ User-friendly, flexible, and customizable user interface
▪ Stand alone operation
▪ Database query interface
▪ Batch analysis for multiple systems
▪ GE-based Interactive Map Interface
▪ OMDR/OMDRS/SOM DES data usage
▪ Support for various vector and raster map formats
▪ Layered display of maps and analysis results
▪ Powerful report and print-out capabilities

FIMS (DATABASE SERVICES MODULE) CAPABILITIES

▪ Multi - user database
▪ Association / Alliance / Assignment databases
▪ Joint Restricted Frequency List (JRFIL)
▪ Frequency Assignment Wizard
▪ Inventory Database
▪ Advanced query interface
▪ Risk based user access and operation control
▪ Interactive Map Interface
▪ Powerful data exchange capabilities: Import / Export interfaces including NATO SMADE-XML format

IRDMAS / INFRARED MEASUREMENTS DATA BASE MANAGEMENT AND ANALYSIS SOFTWARE

IRData Management and Analysis Software (IR-DMAS) addresses well known issues of IR data recording, management and analysis and provides a unique solution satisfying both operational and engineering level military requirements through the integration of planning, measurement, analysis and reporting phases of IR signature measurement campaigns. IR-DMAS can be customized in accordance with user requirements. Different language options are available on user demand.
REDAY
RADAR & ELECTRONIC SUPPORT SYSTEMS PERFORMANCE ANALYSIS SYSTEM

REDAY is an integrated software dealing with performance analyses of Radar and Electronic Support (ES) systems including earth environment conditions. The effects of earth and atmosphere to the electromagnetic energy scattered from the electronic warfare (EW) systems are modeled with numerous empirical and deterministic methods. By the use of these methods, performance analyses and tactical behavior of EW systems can be tested with different scenarios.

GENERAL CAPABILITIES
▪ Radar coverage analyses
▪ Radar systems detectability analyses
▪ Electronic Support Systems detectability analyses
▪ Empirical and deterministic (Fourier Split Step) analysis
▪ Inventory of systems
▪ AREPS Software and Database compatibility
▪ Batch analysis for multiple systems
▪ User defined study area
▪ GIS-based Interactive Map Interface
▪ DTED 0/1/2 height data usage
▪ Support for various vector and raster map formats
▪ Layered display of maps and analysis results
▪ Technical analysis include antenna pattern effects, refraction profiles of the atmosphere

RASES
RADAR CROSS SECTION COMPUTATION

RASES is a high-frequency electromagnetic simulation software which is capable of calculating Radar Cross Section (RCS) of complex targets. The computation methods that are implemented within the software are Physical Optics (PO), Shooting and Bouncing Ray (SBR) and Physical Theory of Diffraction (PTD).

▪ RADAR CROSS SECTION COMPUTATION
Monostatic and bistatic RCS computations can be performed for different frequencies, materials, incidence and observation angles within the simulation environment. Statistical information of the evaluated RCS values can also be investigated. The variation of the RCS values of a target due to any specific maneuver can be analyzed. RASES provides reliable RCS results which have been verified by analytical solutions, numerical methods and experimental results.

▪ EVALUATION OF RANGE PROFILES AND ISAR IMAGES
Within the RASES software, 1-D (Range Profile), 2-D and 3-D (ISAR) images of the targets can be constructed by using the estimated RCS values. By using Inverse Synthetic Aperture Radar (ISAR) images, dominant scattering regions on a platform could be determined.

▪ DETERMINATION OF SCATTERING CENTERS
Positions and amplitudes of the scattering centers that can be extracted from 1-D, 2-D and 3-D (ISAR) images of high importance for the RCS reduction studies of the targets. Extraction of the scattering centers is performed via the CLEAN algorithm.

▪ DESIGN PROPOSALS FOR RCS REDUCTION
The RCS value of a platform can be reduced via structural modifications on a platform or the usage of radar absorbing materials (RAM). By using the built-in coating material types of RASES and by including the electrical specifications of new material types in the material library of RASES, the effects of the RAM application can be investigated in various RCS conditions. The structural modifications that can be performed by using several commercial CAD software, can also be imported RASES in order to investigate and design platforms with low RCS values.
**ELECTRONIC WARFARE SYSTEMS DESIGN & DEVELOPMENT**

Within İLTAREN (Advanced Technology Research Institute), studies are carried out to develop terms for the systems of advanced EW technologies. Prototype and term representation systems are being promoted. Within this context, prototypes of various electronic attack and electronic support systems have been successfully developed by qualified groups of engineers.

**ELECTRONIC ATTACK TECHNOLOGIES**

A term representation system (TRS) developed with the intention of analyzing the efficiency of various electronic attack techniques enables electronic attack applications which are resistant to electronic jamming and deception and quite effective against modern search and tracking radars. Among the main features of the TRS are:

- Narrow-band, high-powered electronic attack capacity
- Capability of applying electronic attack to any side thanks to the sealed beam dish antennas
- DRFM-based advanced technical generator
- Very low time lag
- Capacity of finding the direction of threats and polarization
- Target monitoring with a camera
- Capacity for changing polarization within receiving and transmitting antennas
- Capacity of being stationed both at land and air platforms
- Capacity of applying integrated techniques via various jamming and deception techniques

**ELECTRONIC SUPPORT TECHNOLOGIES**

A prototype system including various electronic support system features has been developed. Apart from comprising the features of a typical electronic aid and ELINT systems, this prototype includes the following as well:

- Operator-specific analysis screens
- High-driven missile detection under intense operations
- Center and operator-specific data access possibility to emitter identification
- Instant matching of contact record specifications with GPS and gyro
- Capacity of creating contact files for analysis

**ELECTRONIC WARFARE SYSTEMS DESIGN & DEVELOPMENT**

In order to scientifically reinforce the electronic warfare system development, analysis activities are carried out within İLTAREN (Advanced Technology Research Institute). İLTAREN maintains these tasks by having various measurement, testing and evaluation infrastructures whether operating at open field or in laboratories. Additionally, studies for detecting radar, infrared systems and other platforms under different conditions. Thanks to the experience and expertise in acquisition activities, various consultancy and engineering support services are also being presented.

**HARDWARE IN-THE-LOOP LABORATORY**

Hardware In-The-Loop Laboratories are established with the purpose of analyzing how various systems operating on RF and infrared bands perform under different conditions and scenarios. Studies to develop more reliable and loyal models via open field testing and measurement activities and to conduct analyses on system behaviors are conducted as well.

**RF & INFRARED MEASUREMENT SYSTEMS**

A system to measure infrared traces of decoys such as air and land platforms and heat shells have been developed. Two different recording system is put for RF and infrared bands. Recording and playing back the signals on RF, IF and video bands is possible. Both of these systems are placed in a Panel van-type minibus whose components have been specifically designed for mobile usage.

**ENGINEERING SUPPORT SERVICES**

İLAREN gives engineering support services to the Turkish Armed Forces, by using the infrastructure gained from electronic warfare systems projects that are conducted by the Turkish Undersecretariat for Defence Industries. These services include development of electronic warfare techniques and tactics, upgraining of the electronic warfare systems in a way that will meet the operational requirements, maintaining the experience and knowledge of the personnel dealing with electronic warfare, testing, evaluating and system engineering.
Numerous studies have been conducted on the basic building blocks of high-power/high-frequency electromagnetic generators (TWT, Magnetron, FEL, and Vircators):

▪ Thermionic cathodes
▪ Oxide cathodes
▪ Dispersed cathodes
▪ Reservoir cathodes
▪ Hollow cathodes
▪ Photocathodes

These products are being developed specifically for projects.

FEATURES
- Current density range: 1 - 50 A/cm²
- Surface Coating: Osmium/Ruthenium/Molybdenum/Cesium
- Relative porosity: 50%-90%
- Diameter range: 1-50 mm
- Fast Heating
- Oxide emitter fillers (Al₂O₃/BaO)

* As a result of ongoing research and development, the specifications in this catalogue and its content may change without prior notice.
TRAVELING WAVE-TUBE TECHNOLOGIES

TWT design and prototype development for radar, electronic warfare, and satellite communications applications

- Radar TWT (High power, wideband, S-band, X-band, Ku-band, Ka-band, Pulse and CW modes)
- Electronic Warfare TWT (High Power, X-band, Ku-band, Ka-band, Pulse and CW modes)
- Satellite Systems (X-band, Ku-band, Ka-band, efficiency over 60%, Pulse and CW modes)

FEATURES
- Helix, Coupled-Cavity TWT
- Multi-stage collectors
- TWTs with fast warm-up cathodes
- TWTs with 2, 3 stage power, absorber coated, ceramic support rods

MAGNETRON TECHNOLOGIES

Magnetron design and prototype development for radar and microwave heating systems applications

- Radar Magnetron (High Power, K-band, S-band, X-band, Pulse and CW modes)
- Microwave Heating Systems (set to material resonance frequency, Pulse and CW modes)

FEATURES
- Hole and Slot Magnetron
- Vane Magnetron
- Rising Sun Magnetron

These products are being developed specifically for projects.
CLOUD COMPUTING SOLUTIONS
DAMLA is the National Search Engine Prototype for searching over internet content, developed by domestic resources. With Turkish grammar specific features taken into account, the search engine can analyze internet contents to determine whether they are in Turkish or not. Therefore the search engine can provide the capability of filtering Turkish contents during indexing and searching activities for fast and efficient browsing.

DAMLA can provide:

▪ auto-complete
▪ auto-suggestion
▪ query correction
▪ stemming and stem-based searching, being Turkish grammar aware during all search processes.

FEATURES

▪ Identification and classification by content categories (News, Sports, Health, etc)
▪ Search within selected categories only
▪ Safe search for eliminating adult content
▪ Searching within content or specified time intervals
▪ Searching inside files and by file types (Pdf, Docx, Xls, etc)
▪ Advanced ranking and prioritization algorithms
▪ Image search
▪ Searching images with specified file size ranges
▪ Searching images by location information, if available
▪ Horizontally scalable, Cloud-compatible system architecture

* As a result of ongoing research and development, the specifications in this catalogue and its content may change without prior notice.
## SAFIR PRODUCT FAMILY

### SAFIR INFRASTRUCTURE

- **Safir Infrastructure** is an "Infrastructure as a Service" solution provided by Cloud Computing and Big Data Research Laboratory (B3LAB). Support of multi-tenancy, resource management, security and privacy are provided in "Infrastructure as a Service" layer of cloud computing. Safir Infrastructure presents a secure virtual information technology environment with virtual servers, storages and network devices.

### SAFIR STORAGE

- **Safir Storage** is a secure centralized cloud storage solution for accessing and storing objects like documents, papers, audios and videos distributively. Safir Storage is a virtual object storage under Openstack Swift infrastructure, and compatible with Amazon AWS S3 platform. It provides high speed writing, reading and deleting functions to the integrated systems. It scales in vertical with both running nodes and disk capacity. The system distributes each object added to the storage among the nodes with 3 duplicate copies. Thus, damage on one of the disks or servers does not affect the reliability of the system.

### SAFIR IDENTITY

- **Safir Identity** provides an authentication mechanism to the cloud components with SSO (Single Sign On) support. It also provides single sign on and authentication with smart cards.

### SAFIR LIBRARY

- **Safir Library** provides a platform independent Application Programming Interface (API) to access and use the functionalities of all of the cloud services.

## BIG DATA ANALYTICS SOLUTIONS

The amount of created, inspected and analyzed data is increasing every day, and the term “digital world” surrounds the reality of daily life. In fact, every form of data has its own importance. “Big Data Analytics Solutions” developed by Cloud Computing and Big Data Research Laboratory (B3LAB) can analyze big data and turn this bulk data into information.

### FEATURES

- Safir Infrastructure (OpenStack Controller, Neutron, Compute infrastructure)
- Safir Storage (OpenStack Swift Infrastructure)
- Safir Identity (Role based secure access layer)
- Safir Library (REST/JSON API support)
- Easy cloud usage with client scripts

### Big Data Analytics Solutions include:

- Hadoop cluster setup and consultancy
- NoSQL database setup, configuration and optimization
- Big data file systems' configuration and optimization
- Configuration and optimization of Linux based operating systems used for big data solutions
- Designing, building and implementing network architectures for big data solutions
- Implementing big data code (e.g. Map Reduce code)
- Turnkey solutions for big data problems
- Optimization of big data code
- Hadoop cluster optimization
- Big data training
TÜBİTAK BİLGEM TECHNOLOGY AND SOLUTION CATALOGUE

TÜBİTAK BİLGEM TECHNOLOGY AND SOLUTION CATALOGUE

As a result of ongoing research and development, the specifications in this catalogue and its content may change without prior notice.

e-GOVERNMENT PLANNING SERVICES
With the aim of having policies and actions, which are identified with a focus on e-Government, developed, implemented and improved:

- supporting the preparation of medium & long-term plans,
- supporting activities on the amendment of law and regulation,
- providing technical consultancy and process guidance,
- carrying out activities with the intent to identify current status, generate alternative solutions and implement the established solutions,
- researching and developing the methods towards enhancing the effectiveness and efficiency of e-government projects, incorporating the knowledge acquired in this scope into guidelines and carry out the activities such as training for the extensification of these.
INSTITUTIONAL INFORMATION AND COMMUNICATIONS TECHNOLOGIES (ICT) CAPACITY ANALYSIS AND IT STRATEGY FORMULATION

In scope of this service, the analysis reports designated to serve as a reference in the IT infrastructure-related budget proposals, which will be submitted by Ministry of Development, are prepared.

▪ INFORMATION AND COMMUNICATIONS TECHNOLOGIES AUTHORITY IT MANAGEMENT SYSTEM CONSULTANCY SERVICE PROJECT
  More efficient implementation of regulation and supervision processes through IT management system in conformity with international standards, improving sectional data analysis and reporting infrastructures and conducting an analysis on the current status with the aim of providing assistance to the decision support processes, preparing technical solution offer and identifying a roadmap with a view to ensure that the software is supplied in line with analysis results.

▪ MINISTRY OF TRANSPORT, MARITIME AFFAIRS AND COMMUNICATIONS SYSTEM ROOM MODERNIZATION PROJECT
  Examination of the physical, system and network infrastructure of the system rooms which accommodate the IT services of Ministry of Transport, Maritime Affairs and Communications, submitting solution offers in these matters and establishing the prospective (1-5 years) capacity plan of the institution.

▪ PRESIDENCY FOR TURKS ABROAD AND RELATIVE COMMUNITIES SYSTEM ROOM MODERNIZATION PROJECT
  Examination of the physical, system and network infrastructure of the system rooms which accommodate the IT services of Presidency for Turks Abroad and Relative Communities, submitting solution offers in these matters and establishing the prospective (1-5 years) capacity plan of the institution, preparing template technical specifications accordingly.

GOVERNMENT PLANNING SERVICES

CURRENT STATUS ANALYSIS AND ROADMAP DEVELOPMENT

▪ STATE SUPPLY OFFICE (DMO) E-CONVERSION ANALYSIS PROJECT
  Creating a roadmap which includes high-level solution offers towards meeting the needs for enhancing the efficiency of the supply process of the institution through the analysis of the current status of DMO, reducing the administrative burden of procurement process, ensure the interoperability among DMO, suppliers and public institutions, revising / improving the relevant business processes of DMO through the use of IT, boosting service quality and identifying mechanisms that will serve as a basis for the decision-support functions.
DEVELOPING TECHNICAL SPECIFICATIONS

▪ İL-CAS PROJECT

▪ MINISTRY OF CUSTOMS AND TRADE (GTB) PERCEPTION, AWARENESS AND SATISFACTION MEASUREMENT SYSTEM PROJECT
Development of a model proposal which would allow the perception, awareness and satisfaction levels of GTB service receivers in terms of the services offered to customs and trade to be measured periodically and to be compared based on years.

▪ PUBLIC WEBSITES GUIDE (KAMİS) PROJECT
Raise awareness of institutions that provide public service so that they have more usable and accessible websites, providing guidance to the public institutions for the theoretical and practical implementations of usability provisions in the governmental ecosystem, conducting research activities on the usability and accessibility of public websites and guiding to render public websites in conformity to usability and accessibility standards.

▪ DEVELOPMENT OF PROVINCIAL INVENTORY SYSTEM AND DECISION SUPPORT SYSTEM
Establishing a system which provides direct data communication with the information systems of ministry with the aim of meeting up-to-date information needs, providing a basis for planning activities, providing entrepreneurs who will make investments with data, monitoring the investment status of Province, District and Villages on computer, evaluating business and procedures of Planning and Coordination Directorates in the provinces on computer, providing information to researchers in universities, press and media in order to provide efficiency in the decision making process of central regulations of Ministry and Public institutions and agencies, mayors, district governors, municipality mayors, provincial and district directors, investors and researchers.

▪ IMPROVEMENT OF PROPOSAL PREPARATION PROCESS IN PUBLIC ICT PROJECTS (KABİT) PROJECT
Defining Project Evaluation Methodology for the evaluation of ICT Projects to be proposed to Development of Ministry by public institutions and agencies, identifying Public ICT Project categories and updating Public ICT Projects Preparation Manual and related forms so that these offer more structural, concrete and guiding information based on determined project categories.
Software process improvement activities based on international models and standards as well as best practices are carried out for organizations that develop software solutions. Solutions are generated in the areas of training, monitoring, process implementation and quantitative management required in order to support process management activities, and render these sustainable and permanent.

In this scope, activities are carried out for providing the training and process implementation support required with the aim of identifying strengths and weaknesses of organizations by conducting analysis of current status through methodological approaches, identifying / improving, monitoring, analyzing, evaluating processes and intensifying these.
For the R&D related e-Government projects with strategic and critical significance that support the realization of key actions on the e-Government oriented national agenda:

- conducting analysis on current status,
- describing the targeted system,
- determining and prioritizing business packages,
- establishing software requirements in the light of the findings from current status analysis,
- configuring architectural, high-level and detailed software designs,
- realizing the activities of coding, code reviewing and testing,
- installing developed software systems,
- delivering practical user trainings on computer for extensification,
- preparing training materials in line with the needs and expectations of target audience and providing required user support.
INVESTMENT, INCENTIVE AND SUPPORT MANAGEMENT SYSTEMS

Central and integrated management information systems which ensure efficiency, transparency and accountability of the activities and resource use by institutions and agencies as well as ensuring the monitoring and evaluation of financial and technical supports, and investment support activities in place.

▪ DEVELOPMENT AGENCIES MANAGEMENT SYSTEM (KAYS) PROJECT
Ensuring transparency, accountability, harmony and coordination in financial management of Development Agencies, enhance the transparency, efficiency and accountability of evaluations through common independent Auditor pool Turkey-wide through the development of an integrated central information system that will improve efficiency and efficacy of major service processes, management, instant monitoring and reporting of Agency support in an efficient, transparent and reliable way so as to provide decision makers with guiding information.

▪ PROVINCIAL COORDINATION AND MONITORING SYSTEM (İKİS) PROJECT
Institutional capacity building in the local level, reinforcing the communication between central and local areas, developing decision support system and rendering regional and local development policies effective and ensure that these are monitored.

SECTORIAL SUPERVISING AND MONITORING MANAGEMENT SYSTEMS

Information systems which aims for increasing the monitorability and supervisability of the market for regulatory and supervisory institutions and agencies, developing e-Government infrastructure for relevant institutions and agencies that have a corner on the market, and saving from labor force and time through carrying out processes electronically.

▪ PRODUCT TRACKING SYSTEM (ÜTS) PROJECT
Establishing infrastructure in order to ensure the end-to-end tracking of all (domestic and imported) medical devices and cosmetic products and to have supervision services and clinical engineering processes carried out in a healthy and effective manner, preventing circulation of counterfeit and smuggled products in medical device and cosmetic sector by developing national and original Product Tracking and Monitoring System, providing easy access to singular product in the recall of defective products from the market, ensuring the accuracy in the calibration, maintenance and repair of medical devices and accessing extensive up-to-date statistical data.

▪ ENERGY MARKET REGULATORY AUTHORITY IT SYSTEM DEVELOPMENT PROJECT
Considering the security needs of energy market (electricity, natural gas, petrol and LPG), development of an information system which ensures central management in line with the needs of Energy Market Regulatory Authority.
SOCIAL RELIEF AND SERVICES MANAGEMENT SYSTEMS

Information systems which provide an infrastructure for providing decision-makers with social relief and service information through the integration of data sources regarding all social relief and services provided by institutions and agencies for more equitable source distribution.

▪ INTEGRATED SOCIAL ASSISTANCE SERVICES PROJECT

Centralizing information on the entire social relief provided by government, developing an information system to ensure more equitable resource distribution, making social relief decisions efficient through integrative management of social relief information, accelerating the processes of application, evaluation and decision (integration with 16 institutions has been completed), realizing General Health Insurance by means of Income Tests via the system, ensuring monitorability and supervisability of social relief services.

▪ DEVELOPING A SCORING FORMULA FOR DETERMINING SOCIAL ASSISTANCE BENEFICIARIES PROJECT

Developing a scoring formula for determining the poor who will benefit from social relief according to objective criteria and provide decision-makers with guidance through this formula.

GEOGRAPHICAL INFORMATION SYSTEMS

The organization comprising of hardware, software, personnel, data and method components which integratively fulfill the functions of collecting spatial and non-spatial data from various sources, storing, processing, analyzing and delivering these so as to meet the needs of researchers, planners, implementers, investors and decision-making bodies in respect to their business and procedures regarding spatial matters.

▪ Basin Monitoring and Evaluation Information System Project

Developing Basin Monitoring and Evaluation System with the aim of providing infrastructure for the establishment of integrative policies through the collective assessment of interactive themes such as Desertification, Erosion, Flood, High Water Basin in the effective management of natural resources.
e-GOVERNMENT POLICY MONITORING AND EVALUATION SERVICES
**e-GOVERNMENT POLICY MONITORING AND EVALUATION SERVICES**

**e-GOVERNMENT POLICY MONITORING AND EVALUATION SERVICES**

With the aim of providing the quality assurance and improvement of the performance and quality of actions carried out in scope of e-Government policies:

- supporting policy researches,
- conducting tendency and problem analyses,
- supporting the activities of performance management, evaluation or valorization,
- supporting the implementation of required improvement activities.

**2015-2019 NATIONAL E-GOVERNMENT STRATEGY AND ACTION PLAN PROJECT**


In this scope, it is aimed that a contribution will be made into making services delivered by public institutions faster, more reliable, efficient, effective, transparent, accountable, saving from time, money, paper and energy through successful e-Government practices and raising awareness for effectively and efficiently maintaining e-Government practices.

In this scope, it is aimed that a contribution will be made into making services delivered by public institutions faster, more reliable, efficient, effective, transparent, accountable, saving from time, money, paper and energy through successful e-Government practices and raising awareness for effectively and efficiently maintaining e-Government practices.
In scope of e-Government oriented institutional architectural activities:

- supporting the activities of establishing relationship, co-operability and integration,
- establishing a basis for the e-Government service providers by carrying out the activities of process, implementation, technology and data management, integration and sharing, and delivering guidance and training services for extensification purposes,
- conducting analyses on the public information which has an integrated management, sharing the obtained statistical data and analytic results with e-Government service providers and beneficiaries.
ATAM is a research center where R&D, design and production activities are carried out regarding electromagnetics, microwaves and antennas. In parallel to these activities, the center provides consultancy to public administrations and agencies, Turkish Armed Forces, universities and the private sector.

**Planar and Cylindrical Near Field Measurement System**

<table>
<thead>
<tr>
<th>Dimension</th>
<th>Maximum Weight</th>
<th>Frequency Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test Room Dimensions</td>
<td>17 x 18 x 14 m (L x W x H)</td>
<td>0.75 GHz – 40 GHz</td>
</tr>
<tr>
<td>Maximum Dimension of Test Antenna</td>
<td>6 x 6 x 6 m</td>
<td></td>
</tr>
<tr>
<td>Maximum Weight of Test Antenna</td>
<td>4000 Kg</td>
<td></td>
</tr>
<tr>
<td>Scanning Plane</td>
<td>9 x 9 meters</td>
<td></td>
</tr>
</tbody>
</table>

**Compact Range Measurement System**

<table>
<thead>
<tr>
<th>Dimension</th>
<th>Maximum Weight</th>
<th>Frequency Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test Room Dimensions</td>
<td>37 x 13 x 12 m (L x W x H)</td>
<td>0.8 GHz – 40 GHz</td>
</tr>
<tr>
<td>Test Area Dimensions</td>
<td>3.48 x 2.44 x 3.66 m (L x W x H)</td>
<td></td>
</tr>
<tr>
<td>Maximum Weight of Test Antenna</td>
<td>500 Kg</td>
<td></td>
</tr>
</tbody>
</table>

**Spherical Near Field Measurement System**

<table>
<thead>
<tr>
<th>Dimension</th>
<th>Maximum Weight</th>
<th>Frequency Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test Room Dimensions</td>
<td>7.5 x 4.7 x 3.30 m (L x W x H)</td>
<td>0.8 GHz – 20 GHz</td>
</tr>
<tr>
<td>Maximum Dimension of Test Antenna</td>
<td>1.4 m</td>
<td></td>
</tr>
<tr>
<td>Maximum Weight of Test Antenna</td>
<td>75 Kg</td>
<td></td>
</tr>
<tr>
<td>Scanning Plane</td>
<td>Full Spherical</td>
<td></td>
</tr>
<tr>
<td>Frequency Range</td>
<td>0.8 GHz – 20 GHz</td>
<td></td>
</tr>
</tbody>
</table>
INFORMATION SECURITY RISK ANALYSIS

Information Security Risk Analysis Unit, reporting to the Vice Presidency for Testing and Evaluation (TDBY), was established with the purpose of conducting security risk analysis of information and communication systems.

Within the scope of the risk analysis, assets that are important for information security and business continuity and the threats against these assets are determined. The effects of these threats are assessed and risk treatment options are provided.

The aim of the risk analysis is to help:

▪ Identification of the secure and non-secure elements of the system
▪ More effective project cost calculation and scope determination
▪ Cost-effective secure design
▪ Identification of security operational procedures
▪ Better definition of business processes and data flows

* TDBY: TÜBİTAK BİLGEM Vice Presidency for Testing and Evaluation

COMMUNICATIONS SECURITY LABORATORY

Communications Security (COMSEC) Laboratory conducts testing to assess whether information security products processing classified information are compatible with the COMSEC criteria. Services provided by the COMSEC laboratory, including consultancy and training, are of utmost importance especially for the information security products to be used by the military.

▪ COMSEC TEST
  Within the scope of the COMSEC product tests, it is aimed to test whether products' design and implementation method is in conformance with the COMSEC criteria. As a result of the COMSEC testing, how information security products will respond to and show protection against threats, such as "tampering, fault attack, side-channel analysis and protocol attacks", is assessed.

▪ COMSEC CONSULTANCY
  Consultancy given for COMSEC information security products mainly focuses on specific details about the design and implementation of a product in accordance with its confidentiality level. Main objective of this consultancy is to ensure that COMSEC criteria are taken into account during the design and implementation phase.

▪ COMSEC TRAINING
  Within the scope of the COMSEC training, information is given about COMSEC criteria and against what sort of attacks these criteria maintain protection.
KDTM
SPEECH & LANGUAGE TECHNOLOGIES LABORATORY

Studies and Tasks
ISO and NATO certified semi-anechoic acoustic recording and test rooms are Turkey’s first and only “Voice and Speech Technology Evaluation” infrastructure. This infrastructure comprises two specially insulated semi-anechoic acoustic recording rooms (20 and 18 m² area) and a specially insulated listener test room (91 m² area). In the test room, 16 subjects can actively participate in the assessment simultaneously.

Various audio technologies developed for military and civilian purposes can be evaluated in this infrastructure with the help of simulated versions of various acoustic environments. The listener room can also be used as a “Human Factors Laboratory” thanks to its silent terminals and touch screen monitors.

Applications
- Intelligibility tests
- Communications efficiency and quality of service tests
- Evaluation of civilian and military voice encoder equipment and systems
- Acoustic and digital embedding (concert, tank, aircraft, helicopter, restaurant, concert, outdoors etc.)
- Acoustic database construction and recording for language-dependent and language-independent technologies

Optical Systems Laboratory

Electro-optics and Laser Systems Laboratory is established inline with the mission of TÜBİTAK BİLGEM to perform R&D activities in laser and laser systems involving critical technologies for the nation, to develop systems and to ensure the continuity, to improve the quality of laser-optic products, and to become one of world’s leading nations in this field.

Capabilities
- To obtain the existing laser technologies and to develop new ones
- To develop high power laser systems
- R&D studies in free space optical communication systems
- R&D studies in fiberoptic communication systems
- Quantum cryptography and related R&D studies
- R&D studies in optical systems based on radiation sources other than laser
- Activities related to adaptive optical systems
The laboratory is established in 2011 to carry out studies in genetic data security and bioinformatics that are critically and strategically important for Turkey. The key asset of laboratory is its interdisciplinary approach, encompassing the disciplines of computer science, mathematics, bioinformatics, and biotechnology. In addition to this, well-educated human resource, national and foreign consultants and partners enable the laboratory to perform several studies in a product and future oriented manner.

SERVICES
- Full Genome Sequencing
- Full Exome Sequencing
- Standard Analysis
  - Sequence alignment
  - SNP calls and small insertion/deletion finding
  - Gene and variance annotation
- Detailed Analysis
  - Selection of variances as per requested filters
  - Association of variances with Mendelian genetic diseases

DEVELOPED DEVICES AND SYSTEMS
MiSens™: is a mobile, fully automated biosensor device, that can be used in vehicles or on a desk. Can be controlled from the remote control app on a tablet PC or it's on-device touchscreen with minimal training of the user. Includes easy-to-use biochips (patent application No. 2014/3992 PT).

BiSens™: is a handheld, on-site biosensor equipment, which allows the detection of analytes without any necessity of an expert user or a laboratory owing to its single use cartridge system.

SOBE™: is an optical, handheld, transcutaneous bilirubin measurement device which helps in the diagnosis of jaundice seen in the newborn babies (design patent application No. 2015/01029).

BIOLOGICAL AGENT DIAGNOSTIC SYSTEMS
The detection and identification of biologically threatening microorganisms, such as viruses and bacteria, from soil, surface, air and liquid samples is known as Biological Agent Diagnostic Systems (BADS). In this context, B&D is carried out for reliable, precise, uninterupted mobile or stationary early warning detection systems.
Cathode and Microwave Vacuum Tube Research Labs aim is to design and develop cathodes for microwave vacuum tubes (Magnetrons, TWTs, etc.) for various applications like satellite communications, electronic warfare systems, high power radar systems and medical systems.

**RESEARCH INFRASTRUCTURE AND TECHNICAL CAPABILITIES**
- Hydrogen, Argon and Nitrogen sintering technology up to 2500°C degrees
- Brazing technology in high temperature and vacuum environment
- Cathode coating technology with metallic films
- Material characterization technology
- Pneumatic and Isostatic pressing technology
- Cathode and E-Gun test and characterization technology in vacuum tube environment
- Microwave vacuum tube (Magnetron, TWT) infrastructure development technology
- Thermionic Cathode, Magnetron and TWT prototype infrastructure development technology

**FACILITIES**
- 4500 m² indoor area
- 2500 m² laboratory area
- 500 m² cleanroom area
- Electromechanics Laboratory
- Chemistry Laboratory
- Numerical Electromagnetics Computing Laboratory
- Cathode Prototype and Test Laboratory
- Sintering (in Hydrogen Atmosphere) Laboratory

Cryptanalysis Laboratory carries out the cryptanalysis activities under Vice Presidency for Test and Evaluation (TDBY). In Cryptanalysis Laboratory, cryptographic security of information security solutions for military, public and private institutions/organizations are being studied by expert cryptographers since 1995.

Cryptanalysis Laboratory performs its activities in two major fields: "cryptographic algorithm analysis" and "cryptographic architecture analysis". During these activities the cryptographic security of a cryptographic algorithm or an architecture against open literature attacks or original attacks is determined.

Cryptanalysis of cryptographic algorithms comprises following activities:
- Cryptanalysis and evaluation of cryptographic primitives, such as cryptographic encryption/decryption algorithms, cryptographic hash algorithms, message authentication codes, etc. in cryptographic systems. Security conditions of these cryptographic primitives are also determined.
- Analysis of random number/key generators (RNGs), which are the sensitive parts of cryptographic systems. Besides the cryptanalysis of cryptographic primitives in RNGs, an original statistical test package developed by Cryptanalysis Laboratory is applied on the data provided by RNGs.

Cryptanalysis of cryptographic architectures comprises following activities:
- Analysis of cryptographic aspects of key management plan, synchronization of cryptographic parameters, authentication, access control, authorization, confidentiality, integrity, signature, source verification mechanisms, etc. in cryptographic systems and their mutual interactions.
- Determination of cryptographic management rules that are vital for the security and maintenance of cryptographic systems.
SPHERICAL NEAR FIELD MEASUREMENT SYSTEM LABORATORY

Parametric measurements of antennas (up to 1.8 m) up to 20 GHz frequency band are performed in the Spherical Near Field Measurement System Lab. Also their 3D radiation patterns are obtained.

OKTEM (Common Criteria Test Center), established in 2001, conducts tests of and provides consultancy and training for Information Technology (IT) products. OKTEM guarantees the security of an IT product by evaluating it according to an international standard known as Common Criteria (CC) or ISO/IEC 15408. This standard not only determines the security requirements of the IT product, but also guides the vendors to implement these requirements on the products/systems. It is a principal method for security evaluation of the products/systems.

Product vendors choose having Common Criteria evaluations in order to increase the security quality of their products and to gain assurance that the claimed security features are valid and have been independently tested against recognized criteria. Additionally, security evaluations of some IT products, which are of critical importance for national and military domains, are carried out within the Center.

OKTEM conducts Common Criteria security evaluations for a wide range of products including firewalls, smart card integrated circuits, software security applications and secure flash drives. The evaluation results are reported in an Evaluation Technical Report (ETR) to the Turkish Standards Institute (TSE), which is the CC Certification Body of Turkey. The final step of the evaluation process is the certification of the product by TSE. The CC Certification Bodies in each country, including USA, Canada, Australia, Japan and many European countries, who have signed the Common Criteria Recognition Agreement.

Besides the Common Criteria evaluations of IT products, OKTEM offers consultancy to specify the security requirements of critical products and develops Protection Profiles that are compatible with the international standards. Additionally, crypto module conformity tests in accordance with the Security Requirements for Cryptographic Modules (ISO/IEC 19790) are also being conducted.

Quality of the evaluations conducted by OKTEM is accredited by the Turkish Accreditation Agency (TÜRKAK) within the scope of the ISO 17025.

ACTIVITIES
- Common Criteria Product Evaluation
- Common Criteria Protection Profile Evaluation
- Common Criteria Consultancy
- Common Criteria Training
- Crypto Module Conformity Test
CAPABILITIES

▪ Radar Systems Engineering
  Coverage Area Analysis
  Analysis and Design
  Antenna and Software Development
  Target Detection
  Doppler processing
  Micro-Doppler processing
  clutter Reduction
  3D target Tracking
  Data Association
  Target Classification
  Communications layer for Distributed and Embedded systems
  Multilayered software architecture
  Multi-Operating Systems Support (Linux & Windows)
  Radar Database Management
  EUROCONTROL ASTERIX coding
  Built-in test (BIT) Management
  Radar PPI, PPI Map etc. interface development
  Web Statistical Analysis with web access

▪ Signal Processing Hardware
  FPGA-based Signal Processing
  Analog-digital (Analog) design
  VME/VPX multi-core high speed digital system design
  High speed baseband signal generation and processing
  BIP = (Enhanced small form-factor plugable) data transmission
  Radar Verification and Validation
  Target Signal & Environment Simulation
  Performance Evaluation
  Laboratory testing
  Field Tests

Advanced radar signal processing research and development, radar systems integration and validation/verification studies are carried out in the Radar Research and Development Laboratory. Current research areas are basically pulse-Doppler, PARM and phased-array radars.

RADAR PERFORMANCE AND SIGNATURE ANALYSIS CENTER

RAPSIM (Radar Performance and Signature Analysis Center) has been founded with the aim of examining the deteriorating effects of WFs on the performance of electronic systems with civilian and military purposes. Within the scope of RAPSIM, it is possible to model many different kinds of radar, navigation and communications systems by also considering the real world geographical positions and the operating parameters and to simulate the overall system performance. The simulation environment that has been based on high reliability system modeling is also supported by high level graphical interfaces and an automated report generation tool.

Wind energy, which is one of the most environmentally friendly (so called “green”) and efficient types of renewable energy, has recently attracted great attention throughout the world. This great demand that currently exist on the wind energy production clearly indicates the increasing future investments in this technology. However, the wind farms (WFs) that might consist of even hundreds of wind turbines are known to have a great potential to degrade the performance of systems propagating electromagnetic energy due to the time-invariant scatterings of the masts and the time-varying scattering characteristics of the rotating blades.

RAPSIM (Radar Performance and Signature Analysis Center) has been founded with the aim of examining the deteriorating effects of WFs on the performance of electronic systems with civilian and military purposes. Within the scope of RAPSIM, it is possible to model many different kinds of radar, navigation and communications systems by also considering the real world geographical positions and the operating parameters and to simulate the overall system performance. The simulation environment that has been based on high reliability system modeling is also supported by high level graphical interfaces and an automated report generation tool.
RF RESEARCH & DEVELOPMENT LABORATORY

RF R&D Laboratory consists of personnel and infrastructure capable of research and development up to 110 GHz frequency band. There exists an evaluation and test/measurement RF/microwave infrastructure up to 40 GHz. Millimeter waveband designs can be implemented in "Chip On Board" technology-based MCMs (Multi-chip Modules) using the facilities of Gebze Campus.

RF DESIGN PRODUCTS
▪ S-band very high power (16 kW) solid-state power amplifiers
▪ X-band medium power (< 1 kW) solid-state power amplifiers
▪ Frequency up-down converters (X-, Ka-, K-band)
▪ Passive RF Components (filters, diplexers, combiners, couplers, etc.)
▪ Very low phase noise DDS-based frequency synthesizers
▪ Very low noise amplifiers
▪ Radio link systems in UHF -0.8-GHz frequency bands up to 25 GHz

TEMPEST TEST LABORATORY

TEMPEST Test Laboratory conducts tests of equipment, systems and platforms processing classified data in accordance with the NATO standard SDEP 2011 “NATO TEMPEST Requirements and Evaluation Procedures”.

Equipment and system tests are carried out using Fully Anechoic Chambers while platform tests are conducted on site.

EQUIPMENT/SYSTEM LEVEL TESTS
▪ All types of cryptographic communication devices
▪ TEMPEST-protected devices, such as PCs, scanners, fax, printers
▪ Satellite cryptographic communication equipment (e.g. GOES-9)

PLATFORM TESTS
▪ Mobile military platforms, including aircraft, ships, etc. (e.g. MILGEM-2 Büyükada)
YITAL was established for conducting research in the fields of semiconductor technology in 1983. YITAL currently uses the 0.7 μm CMOS technology and has been developing the 0.25 μm 5-metal CMOS and SiGeC HBT BULK processes. YITAL, which develops its original production processes, has reached present position by developing BIPOLAR technology, 3 μm and 1.3 μm CMOS technologies and producing low-voltage military standard integrated circuits (IC).

YITAL has the infrastructure enabling to implement IC design, mask production, wafer processing, wafer probing, packaging, circuit test and aging processes. Having 800 m² of clean room space YITAL is the unique laboratory in Turkey which produces ICs in semiconductor technologies.

For the first time in 1989, the ICs containing national crypto algorithms used TUBITAK UEKA’s cryptographic devices are designed and manufactured with YITAL CMOS processes. From this date, the institute’s crypto ICs are designed and manufactured at YITAL.

YITAL team has designed Turkey’s first National Smart Card IC with the use of combined power coming from extensive experience in IC design and the knowledge of secure circuit design captured through 6th Framework Programme. These ICs are currently in use.

For the first time in 1999, the ICs containing national crypto algorithms used TUBITAK UEKA’s cryptographic devices are designed and manufactured with YITAL CMOS processes. From this date, the institute’s crypto ICs are designed and manufactured at YITAL.

Parallel PLUTO/E (Parallel Tactical Data System) Interface Communication Cards is implemented with the use of YITAL’s ICs. These ICs are manufactured with high voltage 24 V CMOS process which is specially developed for this work. Additionally, radon gas and photodiode production processes are developed. Detectors produced with these processes are widely used with success in applications oriented towards Turkey’s needs.

YITAL, parallel to Turkey’s objectives in the field of space, is conducting research space-grade IC manufacturing technology. Within this scope, there is an ongoing effort to develop 0.13 μm CMOS processes.

YITAL is in collaboration with various universities providing support to master’s and doctoral programs which will benefit of Turkey’s semiconductor technology and electronic design capability.

Developing advanced semiconductor manufacturing processes and having military-standard products used in Turkey’s critical applications manufactured with this processes, YITAL has the capability of converting a design on paper to a packaged and tested IC with national resources.
Wireless Telecommunication Technologies Research Laboratory (KİTAL), which has been established at TÜBİTAK BİLGEM under the sponsorship of Ministry of Development, aims at providing an infrastructure that will support industry-leading efforts in this critical area. KİTAL, which will significantly increase the R&D capabilities of Turkey in the area of wireless telecommunication technologies, provides a laboratory infrastructure for experimenting different aspects of heterogeneous networks. It will include equipment for R&D activities of both 3rd and 4th generation technologies (3G, LTE, etc.) and 5th generation technologies (5G, LTE-A, 802.11ad, etc.) whose standardization has been going on. KİTAL will also provide infrastructure for R&D of next generation tactical wireless telecommunication technologies towards enabling “Network Centric Warfare”. KİTAL infrastructure will be made open to universities and companies to support wireless telecommunication R&D activities in Turkey.

Several ongoing projects within KİTAL framework concentrate on different aspects of wireless communications research.

▪ OFDM based 4G mobile broadband wireless system project
▪ Outdoor wireless mobile mesh network project
▪ Detailed real-time emulation of heterogeneous wireless systems project