پژوهشگاه نیرو	**فرم تشریح پروژه** **CoRFP20-2**	شرکت توانیر

عنوان پروژه:	**طراحی و ساخت نمونه نیمه صنعتی رمزنگار داده، متناسب با کاربردهای اسکادا**
عنوان طرح:	**طرح توسعه فناوری‌های امنیتی در صنعت برق**
واحد اجرایی:	**مرکز توسعه فناوری امنیت اطلاعات، ارتباطات و تجهیزات صنعت برق**

برآورد کلی مدت زمان اجرای پروژه: 12 ماه

تبیین و تشریح پروژه همراه با ذکر مراحل کلی:

یکی از جنبه‌های امنیت، محرمانگی (Privacy) است که می‌تواند با استفاده از انواع روش‌های رمزنگاری به صورت تعبیه شده در سیستم و یا با استفاده از رمزنگارهای مجزا (Stand alone) تحقق یابد. از آنجا که در سیستم‌های مخابراتی و اسکادای موجود در صنعت برق این ویژگی امنیتی لحاظ نشده است، لذا استفاده از رمزنگارهای مجزا (Stand alone) تنها راه‌حل موجود برای حفظ محرمانگی داده می‌باشد.

با توجه به اینکه رمزنگار متناسب با کاربردهای صنعت برق باید علاوه بر قدرت رمزنگاری و امنیت فیزیکی رمزنگار، ملاحظات خاص دیگری را نیز مورد توجه قرار دهد، لذا استفاده از محصولات رمزنگار عمومی موجود در کشور به این منظور مناسب نمی‌باشد. همچنین اگرچه نمونه این محصولات در شرکت‌های خارجی طراحی و ساخته شده‌اند ولی به دلیل آنکه الگوریتم رمزنگاری این سیستم‌ها در اختیار آن شرکت‌ها می‌باشد، استفاده از این محصولات در ارتباطات استراتژیک صنایع کشور قابل اطمینان نیست. لذا ساخت رمزنگار داده در کشور می‌تواند در جهت ارتقای سطح امنیت ارتباطات در صنایع کشور موثر واقع شود که در این تعریف پروژه به آن پرداخته می‌شود.

در این تعریف پروژه با توجه به توضیحات مطرح شده به دو مورد توجه است. مورد اول سطح امنیت رمزنگار می‌باشد. سطوح امنیتی مختلفی برای انواع رمزنگارها وجود دارد. استاندارد FIPS 140 سطوح امنیتی ماژول‌های رمزنگاری را مشخص می‌کند که در واقع تعیین‌کننده قدرت رمزنگار در مقابله با انواع حملات سایبری و فیزیکی می‌باشد. به طور مثال در این سطوح امنیتی به استفاده از یک الگوریتم اثبات شده مانند AES و مکانیزم‌های امنیت فیزیکی Tamper-Evident و اقداماتی برای جلوگیری از دسترسی افراد مزاحم به پارامترهای امنیتی حساس که در ماژول‌های رمزنگاری نگه داشته می‌شوند اشاره شده است. مورد دوم ملاحظات خاص موجود در کاربردهای صنعت برق می‌باشد. همانطور که ذکر شد در طراحی رمزنگار متناسب با کاربردهای صنعت برق باید علاوه بر قدرت رمزنگاری و امنیت فیزیکی رمزنگار، ملاحظات خاص دیگری را نیز مورد توجه قرار داد. از جمله این ملاحظات می‌توان به پشتیبانی از پیغام‌های تکراری، پشتیبانی از پیغام‌های بلادرنگ مد نظر در دیسپاچینگ، عدم تداخل با مکانیزم‌های تشخیص خطا در سیستم کنترلی صنعت برق، پشتیبانی از نرخ بیت پایین داده متناسب با کاربردهای دیسپاچینگ و ... اشاره نمود.

با توجه به توضیحات فوق فعالیت‌های اصلی اجرای این پروژه شامل موارد زیر است:

- انجام مطالعات به منظور استخراج استانداردها، ملاحظات رمزنگار داده متناسب با کاربردهای دیسپاچینگ
- طراحی الگوریتم رمزنگاری متناسب برای کاربرد دیسپاچینگ و شبیه‌سازی آن
- انتخاب و پیاده‌سازی سخت‌افزار مناسب
- پیاده‌سازی نرم‌افزار الگوریتم طراحی شده
- طراحی بخش حفاظت فیزیکی سیستم
- انجام تست‌های استاندارد امنیتی (فیزیکی و اطلاعاتی) مطابق مطالعات انجام شده

پژوهشگاه نیرو	**فرم تشریح پروژه** **CoRFP20-2**	شرکت توانیر

عنوان پروژه:	**طراحی و ساخت نمونه نیمه صنعتی رمزنگار داده، متناسب با کاربردهای اسکادا**
عنوان طرح:	**طرح توسعه فناوری‌های امنیتی در صنعت برق**
واحد اجرایی:	**مرکز توسعه فناوری امنیت اطلاعات، ارتباطات و تجهیزات صنعت برق**

برآورد کلی مدت زمان اجرای پروژه: 12 ماه

مشخصات محصول نهایی(خروجی مورد انتظار) :

- رمزنگار داده متناسب با کاربردهای دیسپاچینگ به صورت Stand alone با قابلیت‌های زیر:
- دارای سطح امنیتی 2 استاندارد FIPS 140 و تطابق با استاندارد AGA-12
- دارای الگوریتم‌های رمزنگاری AES 128bit، RSA 1024/2048 و HMAC SHA 256
- دارای قابلیت پشتیبانی از پروتکل‌های صنعتی DNP3، Modbus، IEC 60870-101/104
- دارای واسط ارتباطی سریال RS232 با کانکتور DB-9 و Ethernet-TCP/IP (10/100 Base)
- دارای واسط مدیریت سریال RS232 با کانکتور DB-9 و Ethernet-TCP/IP (10/100 Base)
- پشتیبانی از پیغام‌های تکراری
- پشتیبانی از پیغام‌های بلادرنگ (عملیات رمزنگاری دارای تاخیر ذاتی می‌باشد)
- عدم تداخل با مکانیزم‌های تشخیص خطا در سیستم دیسپاچینگ
- پشتیبانی از نرخ بیت‌های پایین داده متناسب با نیازهای دیسپاچینگ
- پشتیبانی از نرخ بیت کانال‌های مخابراتی موجود از نرخ 300bps تا 115.2kbps
- دارای مکانیزم کنترل دسترسی و سیستم مدیریت کلید مناسب
-