	تشریح پروژه واگذاری	شرکت توانیر
پژوهشگاه نیرو	TDF02-0	
	CoRFP20-9	

عنوان پروژه:	**اجرای آزمون نفوذ امنیت سایبری بر روی پایلوت آزمایشگاهی اتوماسیون توزیع با پروتکل ارتباطی DNP3**
عنوان طرح:	**آزمایشگاه‌های امنیتی سامانه‌های مبتنی بر ICT در صنعت برق**
واحد اجرایی:	**مرکز توسعه فناوری امنیت اطلاعات، ارتباطات و تجهیزات صنعت برق**

برآورد کلی مدت زمان اجرای پروژه: ۸ ماه

تبیین و تشریح پروژه همراه با ذکر مراحل کلی:

در شبکه توزیع برق، پست‌های توزیع زمینی و هوایی و مراکز پایش و کنترل، نیازمند زیرسیستم‌های مبتنی بر ICT جهت مقاصد پایش و کنترل هستند. در سال‌های اخیر، پروژه‌هایی در حوزه اتوماسیون شبکه توزیع در بسیاری از شرکت‌های توزیع مطرح شده و در حال توسعه است. با توجه به اینکه لازمه‌ی پیاده‌سازی اتوماسیون شبکه توزیع، استفاده از شبکه ارتباطی و اطلاعاتی می‌باشد در نتیجه تهدیدات سایبری در این شبکه نیز مطرح می‌باشد و نحوه ارتقاء امنیت در کنار حفظ عملکرد اصلی شبکه، یکی از دغدغه‌های بهره‌برداران این حوزه می‌باشد بنابراین استخراج آسیب‌پذیری‌های امنیتی و انجام آزمون‌های نفوذ به منظور شناسایی نقاط ضعف شبکه و رفع آنها، در دستیابی به قابلیت اطمینان بالاتر در شبکه توزیع، به صنعت برق کمک خواهد کرد. انجام این فعالیت‌ها، ابتدا بر روی سیستم اتوماسیون توزیع در شرایط فعلی مدنظر است، سپس راهکارهای امن‌سازی پیشنهاد می‌شود و پس از اجرای راهکارهای امن‌سازی و بکارگیری فناوری‌های امنیتی، مجدداً تست نفوذ صورت می‌پذیرد تا بتوان میزان تاثیر و کارآمد بودن روش‌های بکار گرفته شده جهت ارتقاء امنیت را مورد بررسی قرار داد. با توجه به اینکه برخی از این نوع ارزیابی‌ها در شرایط واقعی امکان‌پذیر نیستند؛ لذا «پیاده‌سازی پایلوت آزمایشگاهی سیستم‌های مبتنی بر ICT در اتوماسیون توزیع» در دستور کار «مرکز توسعه فناوری امنیت اطلاعات، ارتباطات و تجهیزات صنعت برق» پژوهشگاه نیرو قرار گرفته است.

پایلوت آزمایشگاهی اتوماسیون توزیع تحت آزمون در پروژه حاضر شامل شبیه‌ساز لایه فیلد و دستگاه‌های RTU با قابلیت اتصال به انواع محیط‌های مخابراتی باسیم (درگاه سریال و اترنت) و بی‌سیم (مودم رادیویی UHF) و تحت پروتکل DNP3 (سریال و TCP/IP) و همچنین اجزای یک مرکز کنترل اتوماسیون توزیع (تجهیزات و نرم‌افزارهای مورد نیاز آن) است و در محل پژوهشگاه نیرو مستقر می‌باشد.

مشخصات محصول نهایی(خروجی مورد انتظار):

- تعیین سناریوها و تهیه برنامه دقیق اجرای آزمون نفوذ (با توجه به اولویت آسیب‌پذیری‌ها)
- ارائه روش اجرایی انجام آزمون‌های نفوذ در کمیته فنی مربوطه، اخذ تایید این کمیته و انجام این آزمون‌ها بر روی پایلوت آزمایشگاهی در محل پژوهشگاه نیرو
- ارائه راهکارهایی جهت بهبود و ارتقاء امنیت پایلوت آزمایشگاهی
- پیاده‌سازی راهکارهای ارتقاء امنیت
- انجام مجدد آزمون‌های نفوذ به منظور مشخص نمودن میزان کارآمد بودن روش/ روش‌های انتخابی برای ارتقاء امنیت