



انجمن رمز ایران  
Iranian Society of Cryptology



## امنیت پروتکل‌های ارتباطی در سیستم‌های کنترل صنعتی

در چند سال اخیر، اهمیت امنیت سیستم‌های کنترل صنعتی بر همگان روشن شده است. امروزه بسیاری از سیستم‌های کنترل صنعتی از پروتکل‌های ارتباطی قدیمی استفاده نموده که دارای آسیب‌پذیری‌های فراوانی هستند. بسیاری از این آسیب‌پذیری‌ها مربوط به ذات پروتکل بوده و امکان رفع آن‌ها به سادگی میسر نیست. در این کارگاه، نقاط ضعف و آسیب‌پذیری‌های پروتکل‌های ارتباطی ModBus، DNP3، OPC، ات‌نت صنعتی و ... مورد بررسی قرار گرفته و راه حل پیشنهادی برای رفع آن‌ها ارائه خواهد شد.

### **Industrial Control Systems (ICS) – Communication protocols security**

In recent years, everybody knows the importance of Industrial Control Systems (ICSs) security. Nowadays, most of ICSs use old communication protocols that have many vulnerabilities. Most of these vulnerabilities arising from the protocol design and cannot be repaired easily.

In this workshop, Modbus, DNP3, OPC, Industrial Ethernet and etc. protocols and their vulnerabilities will be reviewed and suitable workaround and mitigation will be determined.