



# 工业控制系统安全保护

给欧洲和成员国的建议

2011年12月9日发布



# 目录

- 1 执行摘要
- 2 介绍
  - 2.1 工业控制系统的进化史
  - 2.2 ICS 的网络安全
  - 2.3 开展 ICS 安全研究的需要
- 3 本项研究的目的和范围
  - 3.1 研究的目的
  - 3.2 研究的范围
- 4 适用对象
- 5 方法
- 6 关键发现
  - 6.1 ICS 安全的最大挑战
  - 6.2 标准、指南和法规
  - 6.3 标准、指南和法规的接受和使用
  - 6.4 在运营商/基础设施层面制定安全计划的必要性
  - 6.5 对信息共享和其他协作方案的态度
  - 6.6 公共私营合作伙伴关系
  - 6.7 通用测试平台
  - 6.8 宣传和意识教育方案
  - 6.9 ICS-计算机应急响应能力或同等备选方案的益处
  - 6.10 技术威胁和解决方案的现状
  - 6.11 与旧系统相关的风险
  - 6.12 ICT 与 ICS 融合的问题
  - 6.13 其他技术问题
  - 6.14 当前和未来的研究
  - 6.15 有关 ICS 安全和其他相关问题的悬而未决争议
- 7 建议
  - 7.1 建议 1: 制定泛欧和国家层面 ICS 安全战略
  - 7.2 建议 2: 拟定一部 ICS 良好安全规范指南
  - 7.3 建议 3: 创建 ICS 安全计划模板
  - 7.4 建议 4: 推动意识教育和培训
  - 7.5 建议 5: 创建一个通用测试平台或一个 ICS 安全认证框架
  - 7.6 建议 6: 建立国家 ICS-计算机应急响应能力
  - 7.7 建议 7: 借助现有研究方案推动 ICS 安全研究
- 8 结论
- 9 参考文献
- 10 缩略语
- 附录 I 文案研究结果
- 附录 II 调查和走访分析
- 附录 III 与 ICS 安全相关的标准、指南和政策文件
- 附录 IV 与 ICS 安全相关的方案

附录 V	关键发现
附录 VI	研讨会会议纪要