Think Automation and beyond...

安全注意事项

随着当今互联网社会的高速发展，确保网络安全的重要性日益凸显。因此，在使用本公司产品时，务必注意以下安全防范措施。请您在使用我们的产品前了解这些注意事项。

安全注意事项

一般来说，在未采取适当安全措施的情况下构建网络，可能会引发以下问题：

- ✓ 由于外部网络的非法入侵，可能导致系统中断或非法操作、机密信息被利用、数据被篡改或破坏、恶意软件被植入
- ✓ 以植入恶意软件为跳板，从受害者转为加害者去攻击其他网络设备
- ✓ 网络服务许可导致意想不到的信息泄漏或溢出
- ✓ 通过行骗进行非法操作
- ✓ 上述问题可能引发二次损害，比如伤害、损害赔偿、声誉受损、机会丧失等

为了防止上述问题，请参考后述的安全措施实例，适当设置本公司产品、同一网络内的其他设备及其所支持的安全功能后，再将本公司产品连接到网络。必要时，为了避免可能发生的安全风险，还应采取其他措施。

本公司产品不能直接连接到电信运营商的通信线路（移动通信公司、固网通信公司、互联网供应商等）或者公共无线局域网。将本公司产品连接到互联网时，请务必通过路由器或者类似设备。

非法访问手段和控制系统的漏洞不断被发现，无论采取多少安全措施，安全风险仍然存在。我们强烈建议您了解网络连接始终存在风险，请随时获取最新信息并采取安全措施。

请注意，对于因非法访问而直接或间接产生的损失、损害及其他费用，本公司不承担任何责任。

安全措施实例

构建封闭网络和加密

如果您将我们的产品所在的局域网连接到外部网络，请使用专用网络或 VPN 等封闭网络。并尽可能采取加密（SSL/TLS）等措施。即使使用封闭网络，安全也可能因特殊方法而被破坏，此风险应予以考虑。

密码

请参考以下内容设置密码。有关本公司产品的密码设置方法，请参阅对象产品的手册。

- ✓ 更改初始密码
- ✓ 设置为不容易破解的密码。密码应包含大小写英文和数字等，长度应较长
- ✓ 定期更改密码，严格管理

访问限制

请参考以下内容，对网络连接的设备设置访问限制。有关如何配置我们的产品，请参阅对象产品的手册。

- ✓ 关闭不必要的网络服务和端口
- ✓ 仅允许来自特定访问源的连接
- ✓ 限制每个帐户的访问权限

其他参考信息

国内外已发布各种安全指南，请根据这些指南构建和运行网络。