**SJEDIŠTE RIJEKA**
Kudeji 53
HR-51215 Kastav
rijeka@montelektro.hr
+ 385 51 54 58 10

**URED ZAGREB**
Marka Marulića 5
HR-10431 Sv. Nedelja
zagreb@montelektro.hr
+ 385 1 39 09 020

# White paper

## Process Control System - IT maintenance and security

**Revision history:**

| Date | Rev. | Description |
|---|---|---|
| 3.7.2019. | 1 | Initial release |

MONTELEKTRO

# TABLE OF CONTENTS

# 1. INTRODUCTION

Montelektro supplies a wide range of automation systems, ranging from simple machine automation to complex integrated plant automation. This document describes the basic IT principles and security strategies which should be applied to Process Control Systems (PCS) in general. Planned actions should be additionally checked and aligned with PCS vendor guidelines and recommendations.

Main PCS priority is to maintain production and process control, measures intended to prevent the spread of a security threat must not impair this aim. In other hand, to protect plants against cyber threats it's necessary to implement and continuously maintain state-of-art industrial security concept. When planning PCS security strategy, main goal is to find a balance between production continuity, system stability and security.

# 2. MICROSOFT UPDATES

Regular and prompt installation of software updates (patches) represents a vital element of a comprehensive security concept. Patches contribute toward stable system operation and/or eliminate known security vulnerabilities.

## 2.1. PCS RELEVANT UPDATES

Microsoft patches are classified as follows:

*Table 1 - Microsoft update classification and their relevance to PCS*

| Update classification | Description | PCS relevant |
|---|---|---|
| **Definition updates** | Updates provide pattern files for proprietary Microsoft security programs such as "Windows Defender". These are currently not approved for operation by most PCS vendors and it's recommended to use third party security products tested and approved by PCS vendor (Symantec, ESET etc.). | No |
| **Feature packs and Tools** | Updates usually introduce new functionalities. In many cases these cannot be used by PCS without compatibility check and vendor approval because PCS version upgrade might be required prior to the Feature pack or Tool installation. | No |
| **Update rollups** | Collections of previously published patches, could contain a patch not approved by PCS vendor. | No |
| **Drivers** | Latest hardware drivers. Drivers released and supplied by PCS vendor should always be used and should not be upgraded unless:<br>• system is facing errors fixed with new driver release<br>• new driver release is tested and approved by vendor | No |
| **Service Packs** | Service packs always result in major changes and are usually approved only with new PCS version – in order to deploy service pack, PCS software upgrade is mostly required | No |
| **Updates** | Updates eliminate minor flaws in a program. For this reason, only the critical updates and security updates are relevant to automation systems. PCS vendors and integrators usually run tests on these two classes of patches immediately after their release by Microsoft. | Critical and Security updates |

Many of the patches in these classifications are neither important nor essential for secure and stable plant operation. Feature packs and Service packs usually require PCS version upgrade which results in additional engineering and license costs thus such updates should be planned and budgeted in advance.

Critical and Security updates correct functionality errors and errors that can be used to attack the system. For this reason, it's important to deploy such updates on regular basis. Anyway, these two update classes are subjected to a compatibility test for specific versions by PCS vendors and should not be installed if not approved by vendor or at least tested in acceptance environment. In case there is no acceptance environment, last resort solution is to patch only a few production machines that are covered by disaster recovery scenario and can be reverted to the state prior to the patching.

## 2.2. PATCH PLANNING AND ADMINISTRATION

Patch plan must be planned thoughtfully, even in case when planned patches are approved by vendor or tested in acceptance environment there is a possibility of jeopardizing the production – patch may fail during installation or break PCS functionality which was not fully tested. It's recommended to consider following when creating a patch plan.

*Table 2 - Patch planning considerations and recommendations*

| Consideration | Recommendation |
|---|---|
| **Patching process can cause system malfunction** | • Plan production downtime during patch deployment<br>• Backup production data at backup destination outside of PCS<br>• Disaster recovery procedure must be in place and ready for execution in case of issues after patch installation<br>• Deploy patches in phases - If system consists of more machines of same role (Servers, Workstations, Engineering stations), in first phase patch only one machine of each role, test production for few days then patch other machines |
| **Avoid automatic Windows updates** | • Patching process must be planned and executed manually, automatic updates could install unwanted patches or restart production machines during production |
| **Deploy only PCS relevant updates** | • Don't select updates which require PCS version upgrade<br>• Don't' select updates which change OS version or add new functionality (Feature packs, Tools, Service packs)<br>• Check if selected updates are compatible with hardware and used operating systems<br>• Check if selected updates are blacklisted by PCS vendor<br>• Check if there are additional known issues after update installation |
| **Delay patch deployment** | • Don't plan deployment of patches immediately after patch release, wait for at least few weeks while Microsoft, vendor and community installs and test patches – sometimes patches bring additional issues and are withdrawn only few days after release |
| **Test updates before deploying to production** | • If there is a possibility to deploy patches in Acceptance environment, deploy and test them there first |
| **Don't patch functionalities you don't use, disable them** | • For example, if system doesn't require Remote Desktop Protocol disable RDP functionality and don't deploy patches targeting this functionality |
| **Prepare patch installation files** | • Use WSUS or prepare offline patch installers if WSUS is not available |

## 2.3. CONCLUSION

Patching a running and fully functional PCS is a challenging task. At the same time, we have responsibility to keep PCS secured and updated while there is no guarantee patch deployment won't cause system malfunction. That is the fact we must be aware of when planning the patching process and always take measures to avoid such scenario. System functionality and production continuation is our highest priority, PCS patching should never be done at any price – if we must choose between production and patching, system should probably be secured in some other way.

# 3. REFERENCES

ProLeiT AG. (2019, May 24). IT Security White paper, Plant iT V9.60.

Siemens AG. (2016, November). Security concept PCS 7 & WinCC (Basic).