Virtualization in Control Systems
Possibilities and Challenges
This presentation kick-starts the discussion by walking through pros and cons of virtualization in control systems as collected from various IT and SCADA related blogs and articles. It is a relatively new and hot topic, which is openly debated on the Internet.

Some attention is paid to cyber security issues before diving into the reality of today, finishing off with a quick look in the magic crystal ball about the future.

- Possibilities – what are the good things
- Challenges – why it may be a bad thing
- Cyber Security – more or less secure with VM
- What about reality – where are we now
- What about the future – where are we going
Why Virtualization?
In a control system environment

- **Lower number of physical servers**
  - Reduction of hardware maintenance and operational costs, significant for high-end SCADA/EMS environments with 50-100 servers.

- **Fast recovery from disasters**
  - Snapshots and clones shrink-wraps operational systems for fast and easy recovery from any kind of software induced failure

- **Simplified system deployment**
  - Virtual server templates facilitates system deployment by reduction of engineering efforts

- **Excellent development and quality assurance**
  - Again, snapshots and clones greatly enhance productivity and quality assurance in in release and production life cycles

- **Allows safe testing of security architectures**
  - Existing open source and show case VMs of security products and appliances ready for testing in you virtualized QA system

- **What else?**
Why Not Virtualization?
In a control system environment

- Difficulties in finding origin of problem
  - Vendors may be unwilling to support virtualized environments because of the fear of reported problems being related to the hypervisor of infrastructure rather than their applications. E.g. time synchronization

- Resilience (Availability)
  - The risk of losing 4 online systems by losing one server is evident.

- Increased attack surface
  - Although the surface of each guest remain the same, the hypervisor and infrastructure as such adds to the total.

- Potential problem with physical interfaces
  - USB, RS-232 etc may pose problems. Such problems can often be solved by additional, external hardware.

- Performance
  - Will a virtualized environment have the capacity to withstand a major disturbance in the process?

- What else?
Cyber Security Issues
In a virtualized environment

- Shared resources may act as an attack platform
  (http://www.infoworld.com/d/security-central/virtualizations-secret-security-threats-159)
  - "graphics cards and network cards today are really miniature computers that see everything in all the VMs."
  - Mitigations are developed on chip-level

- High Assurance Platform
  (http://www.internetnews.com/ent-news/article.php/3696996)
  - NSA are looking at using virtualization to solve the air-gap problem for personnel with multiple security clearances. Today, such personnel need to use separate workstations to access the information for each clearance level.
  - The HAP is developed with security in focus

- Relaxed posture regarding security in VM infrastructures
  - Almost 70% of all companies that have or are moving to virtualization do not plan to do anything regarding security in their virtualization infrastructures. All security is focused on the guests
  - Real-life incidents may be needed to change this posture
Cyber Security Issues
In a virtualized environment

- **Hypervisor kernel less vulnerable**
  - Optimized hypervisor kernels are less susceptible to malware than regular general purpose operating systems. However, they are still not impervious to attacks

- **Single hypervisor vulnerability**
  - If mission critical production systems are virtualized, redundancy and thereby availability may be inhibited if there is a single vulnerability in the hypervisor of choice that can be remotely exploited.

- **Conclusion**
  - Similar to the pros and cons regarding virtualization, the technology is yet to new to understand if the introduction of virtualization actually help provide better security for control systems, or if it introduce serious security vulnerabilities
  - There is a strong trend in securing control systems on host (guest) level at the moment. Introducing virtualization requires the same focus on hypervisor and infrastructure level! Perhaps even on chip-level as anticipated by NSA and AMD.
Reality of Yesterday
Example of SCADA/EMS of 2000 Years Model (excl. process comm.)

- SCADA/EMS production connected to office network
- SCADA/EMS consist of dual SCADA/EMS, dual Historian, dual data acquisition front-ends, one engineering station and multiple workstations
- Single solution for backup/recovery
- Total number of hosts often less than 20 servers for three sites and 20 - 40 workstations
Reality of Today
Example of SCADA/EMS of 2009 Years Model (excl. process comm.)

New additions:
- Security Zones
- Replicas
- Quality Assurance
- Configuration Mgt
- Security Mgt

- 50 – 100 Servers
- 25 – 50 PC:s
Reality of Today
As seen from a vendor perspective

- Massive increase in number of servers in tenders since last year, mainly inspired from NERC-CIP (security and quality assurance)

- With the increase in number of servers, there are always discussions regarding virtualization.
  - A couple of customers are considering virtualization of their existing production systems, possibly waiving parts of the support agreements.
  - One contract includes virtualized quality assurance systems
  - Two major tenders includes virtualized environments for development and quality assurance

- Vendors offering virtualized environment will also have to face to music. Warranty and support agreements must include the virtualized solutions.
  - Readiness for such responsibilities are made by fully virtualized (to some extent including virtual security appliances) release acceptance environments in addition to physical ones. Currently, applications that interact with physical interfaces not natively supported by the VM are excluded, typically data acquisition hosts.
Real Life Experiences
Internal Acceptance Tests conducted on virtualized systems

- Internal Acceptance Tests
  - System verification and validation are conducted on virtualized systems, including virtual appliances, in addition to the physical environments. This facilitates better test coverage since multiple configurations can be tested for each release with significantly less deployment efforts.
  - Penetration and vulnerability tests are conducted on virtual environments but are currently excluding the hypervisors and virtualization infrastructures

- Development merge verification and validation
  - Virtual environments are used to verify and validate that development tracks are merged into the baseline correctly.
Real Life Experiences
Miscellaneous applications of virtualized environments

- SCADA images produced for critical roles for development and test:
  - SCADA/EMS/Historian application servers in one image
  - Domain Controller, Engineering and HMI in another
  - VMs produced for use in local workstations. Being replaced by centralized lab automation solution

- ESXi leverage excellent test and demo possibilities
  - A $1000 PC can now run an almost full configuration with reasonable performance, making the virtualization technology very inexpensive and commonly available

- Introduction of lab automation system
  - Excellent workbench for core configuration tests (dual SCADA, dual Historian, ICCP partners, Security Management etc)
  - Multiple developers can test core configurations at the same time by checking out a specific build, conduct tests and then drop it. Checking out such a configuration is a matter minutes. A system of 5-6 hosts is up and running within five minutes.
  - Unsuitable for testing components that interact with physical interfaces like data acquisition.
Real Life Experiences
Lab automation as development and test platform, from beta tests

- Screenshot from lab automation configuration overview, showing system with dual SCADA/Historian servers and combined Domain Controller, Engineering and HMI
Real Life Experiences
Lab automation as development and test platform

- Screenshot from lab automation configuration overview, showing system from a network perspective
Real Life Experiences
Lab automation as development and test platform, console view
Real Life Experiences
Lab automation as development and test platform, HMI console view
What awaits us in the future
Regarding virtualization in control systems

- Personally, at the time of writing
  - Virtualization will be the most common solution for non-critical systems, like development, test and quality assurance
  - Production environments will be partly virtualized, but not fully.
  - There will be security incidents where hypervisors are compromised
  - New mitigation techniques and strategies will be developed to make hypervisors extremely difficult to compromise
  - Overall quality of control system over the full life-cycle will increase

- Stratos Technologies thinks:
  - True utility computing enables resource sharing and dynamic resource allocation based on user-specified criteria, such as time of day and incremental capacity needs.
What awaits us in the future
Regarding virtualization in control systems

- **Stratos Technologies thinks (contd.):**
  - Utility computing is the focus
  - Simpler deployment, use will make benefits more broadly accessible
  - Management and monitoring come of age
    - Self-management
    - Policy making can be automated
  - Virtualization standards will increase ease of deployment, reduce risk
  - Single point of failure at virtualization layer is overcome by deploying in a fault-tolerant environment
  - Robust fault-tolerant hardware eliminates single points of failure on the virtualization server platform

- Finally; what do you think?