Minimizing the cost of securing a new ICS system
Lessons from implementation projects
Example of an avoidable cost

90 man-days of work * [vendor’s daily rate]

...for answering a question:
which firewall ports should be open for your SCADA application to work?
Examples of cost reductions per phase:

1. Scoping and requirements definition
2. Vendor selection and contracting
3. Building, implementing and handover to operations
1. Utilize available and cheap sources of knowledge
2. Move as much work as possible on the bidding vendors
3. Put security requirements in the Framework (Agreements)
Vendor selection and contracting

Patching

Typical contractual omissions, which translate into costs later:

Vendor will provide a list of qualified patches “regularly”

Patching ≠ Operating System

Application code ≠ Code developed by the vendor
# Vendor selection and contracting

## Hardening

**What if it doesn’t come out of the box?**

<table>
<thead>
<tr>
<th>Scenario 1</th>
<th>Impact analysis</th>
<th>Implementation and testing in batches</th>
</tr>
</thead>
</table>
| Hardening benchmark | Req 1: xxxxxxxx  
Req 2: xxxxxxxx  
Req 3: xxxxxxxx  
Req 4: xxxxxxxx  
Req X: xxxxxxxx |                                                  |
| Scenario 2 | Out-of-the-box Vulnerability analysis | Implementation and analysis of top priority items |
Management of Change
...can be a costly bottleneck.

Multiple approval layers

No SLA

Requirement to re-approve in case of in-flight change

Time and effort spent on red-tape
Building, implementing and handover to operations

System handover from Project to Operations

...can cause major delays.

<table>
<thead>
<tr>
<th>Initial approach</th>
<th>Implementation</th>
<th>Testing</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>App</td>
<td>DB</td>
</tr>
<tr>
<td></td>
<td>Fabric Manag.</td>
<td>OS Platform</td>
</tr>
<tr>
<td>Changed approach</td>
<td>App</td>
<td>DB</td>
</tr>
<tr>
<td></td>
<td>Hardware</td>
<td>Fabric Manag.</td>
</tr>
</tbody>
</table>

FAT
Takeaways’ recap

1. Don’t overdo security initial requirements - utilize existing standards.
2. Move workload to vendors/integrators during the bidding process, when it doesn’t cost you.
3. Don’t leave security loose ends in the contract.
4. Make sure Mock is not form over function.
Thank you for your attention!