Scada Industrial system controller hack

Wie heeft een belang bij een oplossing van he probleem

Welke instituties zijn er mee bezig?

Wie zijn de klanten?

Welke technologien (software/hardware/aanpak) zijn er in het kader van de opdracht

Wat houdt het probleem precies in?

<https://digitalguardian.com/blog/what-scada-security>

<https://www.reverecontrol.com/blogs/2019/08/20/scada-basics-cybersecurity/>

<https://nl.wikipedia.org/wiki/Supervisory_control_and_data_acquisition>

Welke organisaties en landen hebben vergelijkbare problemen?

<https://www.govinfo.gov/content/pkg/CHRG-109hhrg32242/html/CHRG-109hhrg32242.htm>

<https://www.scadafence.com/state-sponsored-hackers-target-big-pharmaceuticals/>

<https://it.slashdot.org/story/11/11/21/1357227/scada-hacker-water-district-used-3-character-password>

<https://www.dpstele.com/blog/major-scada-hacks.php>

Welke problemen zijn er te vinden via literatuurstudie

<https://electricenergyonline.com/energy/magazine/181/article/SCADA-System-Vulnerabilities-to-Cyber-Attack.htm>

<https://thehackernews.com/search/label/SCADA%20Hacking>

<https://www.ien.com/software/blog/21013133/security-threats-put-scada-on-thin-ice>

<https://www.cnet.com/news/expert-hacks-car-system-says-problems-reach-to-scada-systems/>

<https://www.securityweek.com/dam-hackers-rising-risks-ics-and-scada-environments>

<https://www.csoonline.com/article/2134949/scada-hacking-madness.html>

<https://www.gasystems.com.au/scada-devices-security-challenges/>

<https://www.richardvanhooijdonk.com/blog/en/terror-of-the-scada-and-iot-coordinated-attacks-on-critical-infrastructure>

<https://packetstormsecurity.com/news/tags/scada>

<https://krebsonsecurity.com/tag/scada/>

<https://www.technologyreview.com/2019/01/28/137704/industrial-control-systems-are-still-vulnerable-to-malicious-cyberattacks/>

<https://www.technologyreview.com/2012/08/14/184490/a-cyber-warhead-with-an-unknown-target/>

<https://www.technologyreview.com/2013/02/22/113965/cybersecurity-risk-high-in-industrial-control-systems/>

<https://www.technologyreview.com/2012/06/01/185876/how-obama-was-dangerously-naive-about-stuxnet-and-cyberwarfare/>

<https://www.helpnetsecurity.com/2018/07/26/scada-vulnerabilities-in-ics-architectures/>

<http://www.icare-cybersecurity.com/assets/icare-ics-white-paper-.pdf>

citrix servers

universiteit van maastricht

<https://conference.hitb.org/hitbsecconf2007kl/materials/D1T2%20-%20Raoul%20Chiesa%20and%20Mayhem%20-%20Hacking%20SCADA%20-%20How%20to%200wn%20Critical%20National%20Infrastructure.pdf>

<https://www.greentechmedia.com/articles/read/Maltese-Cybersecurity-Group-Claims-SCADA-System-Hacks>

<https://asmedigitalcollection.asme.org/memagazineselect/article/124/12/37/379167/SCADA-vs-the-HackersCan-Freebie-Software-and-a-Can>

<https://www.itnews.com.au/news/hackers-gain-full-control-of-critical-scada-systems-369200>

Welke bestaande oplossingen zijn er op de markt en waarom zijn deze niet goed genoeg? <https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2015/01/BID-Operationale-producten-025-ICS-SCADA-v1-0.pdf>

<https://www.energypact.org/wp-content/uploads/2018/03/SchubertJan.pdf>

<https://media.defense.gov/2017/Nov/20/2001846609/-1/-1/0/CPP0007_WEED_SCADA.PDF>

<http://processengineering.co.uk/article/2022738/control-systems-beating-the-hackers-with-better-security>

<https://www.ge.com/digital/sites/default/files/download_assets/Security%20in%20a%20Cyberphysical%20World.pdf>

<https://www.fortinet.com/blog/industry-trends/scada-ics-dangers---cybersecurity-strategies.html>

<https://www.yokogawa.com/library/resources/media-publications/cyber-security-for-pipelines-other-scada-systems/>

<https://www.sofcontraining.com/how-to-protect-industrial-automation-control-systems-from-hacking.html/9517167917>

<https://hackernoon.com/scada-cyber-security-threats-and-countermeasures-ultimate-checklist-f236f56938cd>

<https://www.trendmicro.com/vinfo/nz/security/news/vulnerabilities-and-exploits/white-hat-hackers-break-industrial-control-system-security-in-pwn2own-2020>

<https://medium.com/insinia/hacking-scada-how-we-attacked-a-company-and-lost-them-1-6m-with-only-4-lines-of-code-1c4389bf3145>

<https://www.tiga.us/blog/how-to-ensure-your-scada-system-is-secure>

<https://www.computerweekly.com/news/252439658/Next-generation-of-SCADA-industrial-controls-will-protect-against-cyber-attack>

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf>

<https://download.schneider-electric.com/files?p_Doc_Ref=998-2095-04-09-12AR0_EN>

Hoe wordt een cyber-physical attack uitgevoerd?

<https://www.blackhat.com/docs/asia-17/materials/asia-17-Krotofil-Man-In-The-SCADA-Anatomy-Of-Data-Integrity-Attacks-In-Industrial-Control-Systems.pdf>

<https://pgjonline.com/magazine/2009/november-2009-vol-236-no-11/features/hacking-the-industrial-scada-network>

<https://www.ptsecurity.com/ww-en/analytics/ics-attacks-2018/>

<https://scadahacker.com/howto.html>

<https://www.hackers-arise.com/scada-hacking>

<https://www.hackers-arise.com/post/2016/08/01/scada-hacking-dosing-a-scada-site>

<https://null-byte.wonderhowto.com/news/hacking-scada-0162095/>

Een scada hack

<https://www.hackers-arise.com/post/2016/08/05/scada-hacking-hacking-the-schneider-automated-building-system>

<http://78.218.196.95/Portal/Portal.mwsl?PriNav=Diag&ts&ts&ThrNav=DiagTable2>

<https://www.hackers-arise.com/post/2016/08/01/scada-hacking-dosing-a-scada-site>

<https://www.hackers-arise.com/post/2016/07/07/hacking-scada-finding-and-enumerating-scada-sites-with-nmap-and-nmap-scripts>

<https://www.hackers-arise.com/post/2016/07/05/scada-hacking-finding-vulnerable-scada-systems-using-google-hacking>

<https://www.hackers-arise.com/post/2017/03/28/scada-hacking-hacking-the-schneider-electric-tm221-modicon-plc-using-modbus-cli>

<https://www.hackers-arise.com/post/2016/07/22/scada-hacking-monitoring-scada-sites-with-splunk>

<https://www.hackers-arise.com/scada-hacking>

<https://www.shodan.io/search?query=%22Schneider+Electric%22+automation>

inurl:/Portal/Portal.mwsl

<https://www.hackers-arise.com/post/2016/08/01/scada-hacking-dosing-a-scada-site>

Analyse

Wat zijn de verschilllende aspecten en deelproblemen en welk onderscheid wordt daarbij gemaakt?

Waar kan benodigde informatie worden verzameld over achtergronden en oorzaken

Welke verbanden zijn er tussen de verzamelde ideen

Kan het relatieve belang van de elementen/uitkomsten worden beperkt?

Wat zijn de oorzaken van de uitkomsten

Welke adequate oplossingen kunnen er worden bedacht op zijn in producie?

Helikopteriew

Wat zijn de groten lijen als je het oog voor detail van vraagstuk/gegvens of object gerelateerd aan SCADA controlsystemen meeneemt?

Als je van een afstand bekkijk, bijvoorbeeld als leek hoe is dan de stand van zaken te overzien?

Is het mogelijk om de problematiek rondom controlesystemen zoals SCADA het tekort van techniek in de 21e eeuw te verklaren?

Welke trends en ontwikkelingen binnen de sector, lokale en landelijke overheden of internationaal kunnen worden geinterpreteerd en vertaald worden naar de lokale situatie?