University of BRISTOL
Bristol Cyber Security Group

connected everything.

Resilience in high value manufacturing units

Partha Das Chowdhury (partha.daschowdhury@bristol.ac.uk)
Joe Gardiner (joe.gardiner@bristol.ac.uk)

Connected Everything Workshop: 20 September 2022

1 Setting the scene

The workshop aimed to understand the meaning of resilience — in terms of system properties. We set the scene in which cyber-physical systems function — the uncertainty and noise of the real world. The engineering abstractions of powerful mathematical concepts are deterministic but the environment within which cyber-physical systems function are not deterministic. While we can evaluate determinism, timeliness, reliability and safety of a model of the system but how do we test them in an implemented system. These are important constituents of resilience. The broad themes of the workshop are summarized as:

- **What is resilience?** There is a lack of consensus on what resilience means for high-value manufacturing systems. Would we classify many near misses as resilience for such manufacturing units or not resilient? How do we enable external auditors to validate the resilience of IT and OT systems in manufacturing systems. These systems might use commodity operating systems, network protocols, hardware and applications stacks that build on top of one another. Is it possible to test protection mechanisms in the absence of the ability to simulate some of the dangerous attacks? How resilient would the system be in the event of a compromised IT system?
- **Resilience and business continuity.** Interruptions range from hours to days due to malicious and disruptive activities against the infrastructure. What would be the resilience essentials to keep the manufacturing unit functional against determined oppositions like nation-state actors as well as disorganised mal-actors. A related theme for business continuity would be the identification of locations where one should embed the safety/security defaults for such infrastructures. This will draw upon the insights/experience of the participants to debate the positioning of defaults either in the core or edge of any infrastructure or the advantages of spreading them between the core and the peripherals. We appreciate that this would differ across diverse industries, yet our goal would be to highlight the reasonable expectations from IT and OT systems. What is the extent to which we can evolve common building blocks and engineering abstractions that can be re-used across platform and administrative domains? How to prevent adversarial control of the defaults?
- **Effective measures of resilience.** The third theme of our workshop was to evolve a framework to measure resilience in infrastructures. This ties closely to theme 1 where we try to evolve the properties of resilience. An open question is on the foundations on which we can evolve the measures of resilience. This will lead to measures around IT and OT systems – revisiting the debates between security systems and safety systems.

2 Salient Points

The diverse understanding of resilience The discussants came up with the hierarchical nature of resilience — highlighting that it is not a system property which can be answered in binary. The NIS definition is broad, where as

real world operations need specific system properties that can be referred to with respect to defining resilience. An important reason for a diverse understanding of resilience is the risk appetite of individual organizations.

Evaluating resilience While there are models of the system which can be tested they do not operate within the uncertainty and noise of the real world. Related to this is the question on digital twins. Are digital twins an adequate model of the real world?

Resilience and duration While system properties are one component of defining resilience of a system the other element is time. As attacks progress they have an effect on the sustainability of protection mechanisms. Attacks will more often than not sustain for longer duration.

Contingency planning The participants discussed contingency planning involving subject matter experts and stakeholders. This means drawing-up the basic minimum operational requirements / continuity planning against worse case scenarios.

Business continuity Integral to the agreeing to semantics of resilience is defining exact system properties essential to continued operation. This will help evolve an understanding of the appropriate needs in terms of infrastructure — backups, power supply etc. A contextual resilience playbook with a series of steps for recovery was discussed as a potential research direction.

What do we measure There were diverse views on whether we measure near misses as resilience or the positive properties. There the difficulty lies in adequately testing the positive properties.

3 Attendance

- Total number - 20
- In-person / Virtual - 14:6
- M / F - 13:7
- Early Career Researchers - 7
- Postgraduate Researchers - 4

4 Materials generated

A full report on the meeting is currently under preparation and will be shared for further comment and consultation on the Bristol Cyber Security Group website. We anticipate that this will generate additional input from the community, from which we would hope to engage in discourse via future similar workshops or informal discussion.