In this literature review, I will be listing and expanding on the points which would be able to further understand how to improve working with faults in cyber physical systems (CPS). I will also be including the points from people that have actively worked on the research of cyber physical systems through articles that have been written.

The aim of this review is to find ways which could help people who are developing and using cyber physical systems to work with faults, increasing how robust and safe the systems are. This is an important sector to look at, cyber physical systems are becoming more apparent as technology is advancing so far that it can help people from all walks of life. This includes people working in offices to monitoring elderly people in care homes and hospitals. I will be displaying a few approaches which could be taken to aid cyber physical systems deal with faults effectively and maintain safety in order to keep systems working at an optimum rate.

Hardware

With the reliability of hardware in fault tolerance systems being a important factor, there are several possibilities which can come into play. The first being the condition of the hardware being used, this is a big point as the systems will be working for extremely long periods and sometimes without breaks. C.M. Krishna and I. Koren (2013) [2] argue that if a fault tolerance system was adaptive instead of a traditional system there would be less work load on the chips being used, this in turn will reduce the workload and heat being produced out of the chips. The way it will produce less of a workload is because there will be less task loading by reducing redundancy levels. By only making one copy instead of the default three in some cases the processors are less worked reducing heat and increasing long term reliability. This is useful in systems that cannot be repaired or are too expensive as they will not need as many backups.

L. Zhang (N/A) [4] also agrees with this, stating that the more hardware which is used in a system involves extra software support. The more software which is added increases the complexity of the system making it more susceptible to errors. This will then lead the software to re-execution or to resort to backups, with all of these also using more software. If the unessential hardware is removed then the system will be less prone to errors allowing the system to work with less strain.

A further study including K. Shin, E. Atkins C., M. Krishna, I. Koren and S. Wang (2016) [5] states and furthers the earlier study on adaptive fault systems by adding thermal cooling, helping the system even more. This thermal management system in the hardware of the cyber physical system will be used to regulate temperature using a run-time temperature estimation. Their research also came with these statistics in an automated highway system. ” These joint efforts in thermal management of CPS achieved 32% utilization improvement and 63% lifetime prolongation in vehicle ECUs and 13 % real-time performance improvement in mobile systems over state-of-the-art dynamic thermal management.” K. Shin, E. Atkins C., M. Krishna, I. Koren and S. Wang (2016) [5]

In my opinion the thermal cooling system is a very good idea to keep hardware at a better condition, therefore causing less errors. This will also means that repairs would be further apart allowing the system to be operational for more time. With improvements, it can be be especially helpful for systems which can’t be turned off like power plants. If there are less backups made then there will be less errors but my only concern is what happens if many errors come at once. If something was to happen, there is hardly any backups and the system needs to be re-executed then there might be a problem.

Detecting faults

Safety is a big responsibility with cyber physical systems, for example these systems are being used to monitor and track elderly people when in care homes. L. Sha (2008) [3] believes that before any of these systems are in place there needs to be a set of useful, coherent metrics and thresholds which can capture errors, failures, breaches of security and even uncertainty. This will make these systems more intelligent and less dependent on human watch. Doing this would be increasingly useful in hospitals, as if there is a fault with a certain piece of the system which could be monitoring patients the system would have identified the fault and alerted whoever was responsible. This will identify errors before something bad happens.

L. Sha (2008) [3] argues another way to increase reliability in cyber physical systems, by targeting intermittent errors which last milliseconds. L. Sha points out that the systems we use still rely on single computations which then might have intermittent errors, this could cascade an error throughout the system. If an algorithm can be used which would allow several computations to be taken over a set time to create a diverse system, it could render the errors safe as the system have several types of information.

A. Cardenas (2008) [1] thinks that a bigger problem is deception attacks and if a CPS could be able to detect an attack. This is because there is no detection algorithm which can identify deception attacks launched by compromised controllers. As most intrusion systems has a human in the loop, these systems don’t so an algorithm has to be made.

In my opinion I feel like both are useful when looking at these systems. This is because cyber physical systems are being used more often and in places which need to be protected from attacks, meaning if an algorithm is made or if someone is monitoring the system it would be useful for systems which need to be secured. On the other hand if it is at a high risk of breach then adding a set of standards to the systems where possible would be more efficient.

In conclusion working with fault tolerance is CPS is an inevitability as no software is perfect and errors will occur. This is why error prevention and detection of errors are the most important thing to a CPS as they are constantly in use. With the information that I have gathered I believe that keeping the hardware at the best condition is the best aid as it will help keep the system at an optimum efficacy for longer periods of time.

References

Cardenas, A., Amin, S. and Sastry, S. (2008). Secure Control: Towards Survivable Cyber-Physical Systems - IEEE Conference Publication. [online] Ieeexplore.ieee.org. Available at: https://ieeexplore.ieee.org/document/4577833/ [Accessed 18 Apr. 2018]. [1]

Krishna, C. and Koren, I. (2013). Adaptive fault-tolerance fault-tolerance for cyber-physical systems - IEEE Conference Publication. [online] Ieeexplore.ieee.org. Available at: https://ieeexplore.ieee.org/document/6504101/ [Accessed 18 Apr. 2018]. [2]

Sha, L., Gopalakrishnan, S. and Liu, X. (2008). Cyber-Physical Systems: A New Frontier - IEEE Conference Publication. [online] Ieeexplore.ieee.org. Available at: https://ieeexplore.ieee.org/document/4545732/ [Accessed 18 Apr. 2018]. [3]

Zhang, L., He, J. and Yu, W. (n.d.). Challenges and Solutions of Cyber-Physical Systems. [online] Pdfs.semanticscholar.org. Available at: https://pdfs.semanticscholar.org/5bd2/3a9db150316ef379ce3cc51e3a6ef4aada7e.pdf [Accessed 18 Apr. 2018]. [4]

G.Shin, K., Atkins, E., Krishna, C., Koren, I. and Wang, S. (2016). Thermal Management of Cyber Physical Systems. [online] Cps-vo.org. Available at: https://cps-vo.org/node/24791 [Accessed 20 Apr. 2018]. [5]