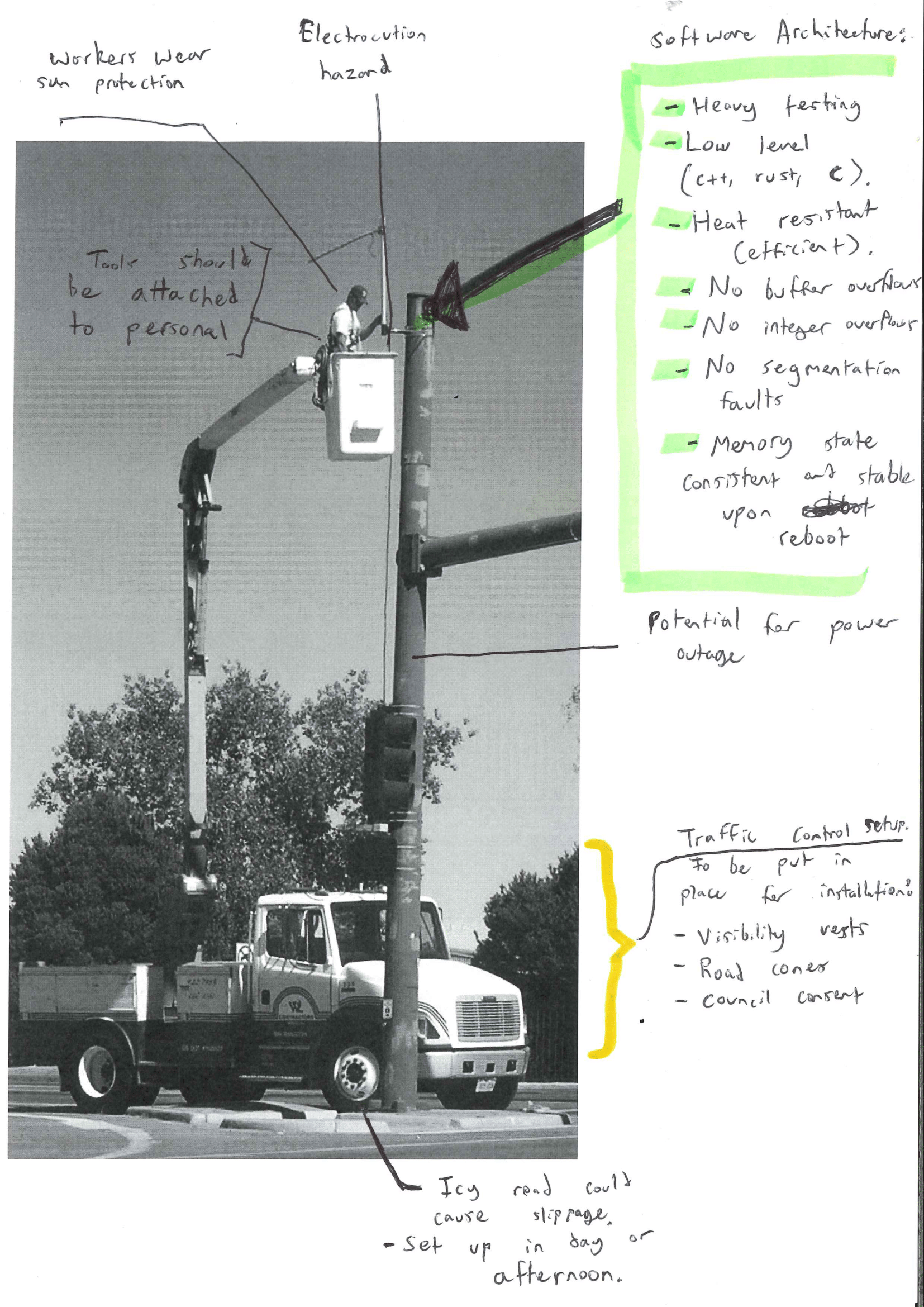
### Hazard assessment Template

|  |  |
| --- | --- |
| **Title** | Traffic light programming hazard analysis |
| **Author** | Oliver Garrett (oga20) |
| **Current state of technical system** | Traffic light software to be designed and deployed on a very busy intersection |

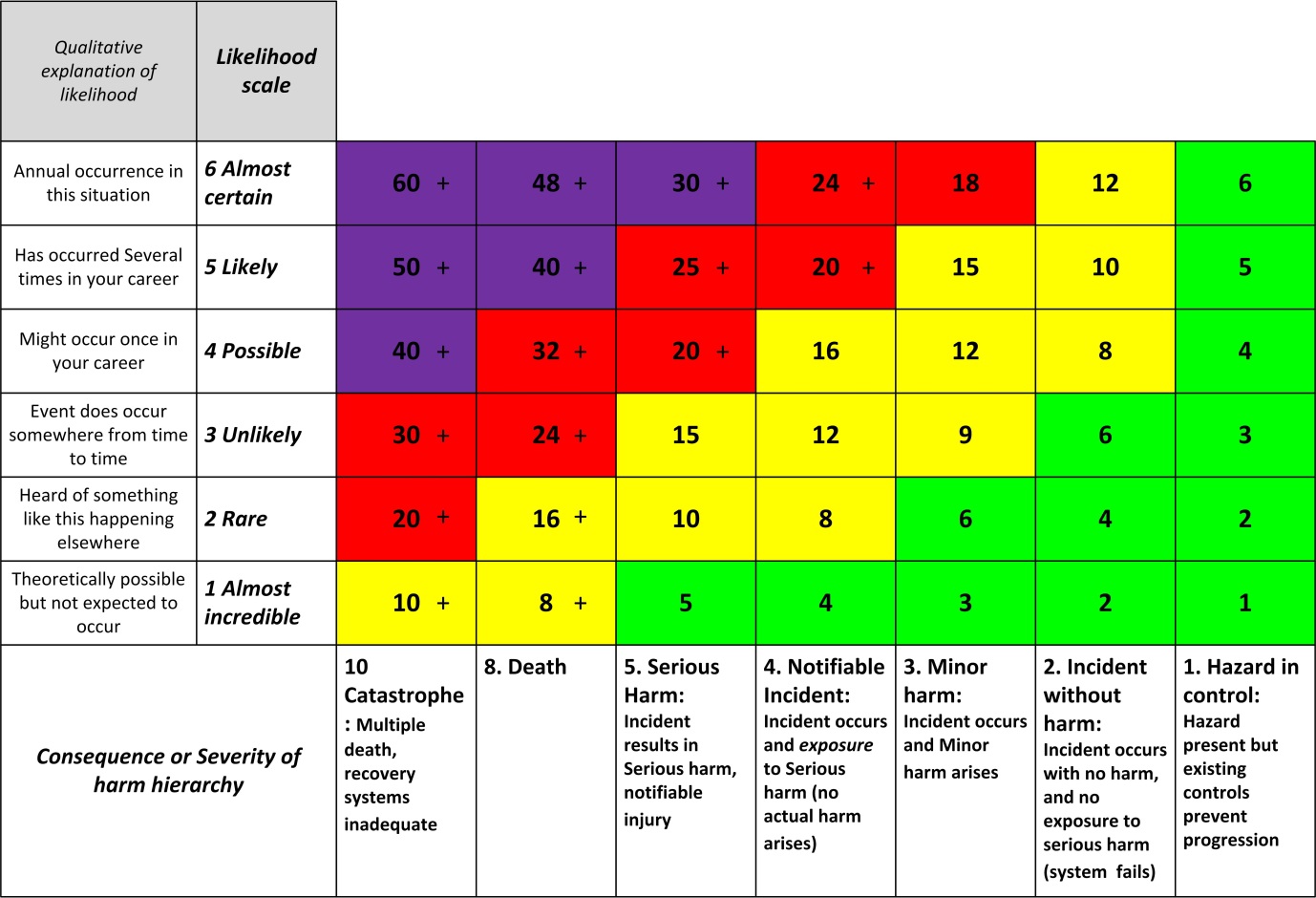
**Traffic light software for a busy intersection**

This report will go over the risks associated with creating and deploying traffic light software at a busy intersection. The main risks after deployment involve unprecedented faults in the software, such as segmentation faults, integer precision overflows, internal malloc data overwrites, and other errors that can cause undefined behaviour in the traffic lights after it has been deployed. The risks in deployment include fast moving cars, ice on the roads, unsafe tools, tool misuse by workers, falling objects from the ladder/crane, and other mundane risks such as sunburn.

The risk register table will document the risks, and describe the steps taken to mitigate them as best as possible.

1. **Architecture of the system**:

**2: Risk matrix and scales:**



**3: Risk register**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Risks of system in its CURRENT STATE, with its existing controls. | | | | | |  | Risks of system in its FUTURE STATE after these treatments. Insert any new threats caused by the treatments. | | | |
| Architecture level: Work-stream, project phase, hardware category, workstation | Specific hazard | Magnitude of consequence   * CC   c | Likelihood of consequence  j | Risk = (C x L) | Treatment? Consider Preventative and Recovery mechanisms.  30 or higher Unacceptable risk.  18 or higher Urgent treatment.  8 or higher Consider treatment  7 or less No intervention necessary. | Action required by who? Resources required? | Monitoring required of efficacy of treatment? |  | Treated Consequence (C\*) | Treated Likelihood (L\*) | Residual Risk  (C\* x L\*) | Is this acceptable? What further action is required? |
| Software System | Memory buffer overwrite changing unintended data and altering state of software unexpectedly, causing traffic lights to behave in an unintended manner. | 6 | 5 | 30 | Adequate testing should be done on the software to assure that it is impossible for this to happen. Programs like Valgrind, Dr Memory, or Address Sanitizer will also help for this. | Software engineering team, adequate planning and time required for testing | Automatic tests should be written and examined by multiple engineers to ensure correctness. |  | 6 | 1 | 6 | Risk minimalized. |
| Software system | Segmentation fault induces a crash, causing a traffic light fault | 7 | 2 | 14 | Adequate testing needs to be done to ensure that it is near impossible for something like this to happen. Segmentation faults are usually caught very easily due to the operating system catching illegal memory accesses at ring 0, so this risk is highly unlikely. | Software engineering team, adequate planning and time required for testing. Also, backup software should be written to run when the traffic light software detects it has crashed. | Automatic tests should be written and examined by multiple engineers to ensure correctness. The backup software should be testing religiously, as it has no crash backup program. |  | 7 | 1 | 7 | Risk minimalized. |
| Software system | Integer size overflow messes up traffic light timing in an unexpected manner. | 7 | 3 | 21 | Ensuring that all integers and floating-point data is taken the remainder of when running out of bits will ensure there is always enough bits to store the required data. | Software engineering team, adequate planning. Tests should utilize long time frames, I.e., simulating many years at a time to ensure that integers do not run out of precision. | All variables that keep track of the time should be examined in the long duration tests to ensure there is no overflow errors. |  | 7 | 1 | 7 | Risk minimalized |
| Software system | Bad code (I.e., bad Boolean algebra,) causes red light and green light at the same time. | 7 | 1 | 7 | The likelihood of this is extremely unlikely, as it would only happen with engineers who had absolutely no idea what they are doing. Ensure to get a competent engineering team. | Salaries for competent engineers | Ensure to get a competent engineering team. |  | 7 | 1 | 7 | This would only happen with highly incompetent engineers. |
| Setup stage | Pedestrians hit by falling tools upon setting up software. | 5 | 4 | 20 | Ensure installer’s tools are attached to all personal working on the traffic light | The firm that modifies software in traffic lights should be notified | Written confirmation by setup firm that tools will be attached |  | 1 | 1 | 1 | Attached tools cannot fall |
| Setup stage | Ice causing ladder or crane to slip. | 6 | 3 | 18 | Ensure that the setup is not enacted when it is icy outside | Setup firm needs to ensure that the procedure is carried out at a time where it is not icy. (If this is not possible, the crane or ladder should be equipped with ice grips.) | Written confirmation by setup firm that the change will not be during the morning, when it is icy |  | 1 | 1 | 1 | No ice means practically zero risk, and practically zero likelihood. |
| Structural | Lightning strike | 8 | 1 | 8 | Ensure fuses are emplaced to protect the CPU. | This risk is on the traffic light manufacturer | Plans from the engineering firm that creates the traffic lights |  | 4 | 1 | 4 | Fuses will prevent malfunction of software, and will cause a restart only |
| Electrical | Error in CPU manufacturer | 7 | 1 | 7 | CPU vendor delivers an error in the CPU instruction set. | Buy from a trusted CPU vendor | None |  | 1 | 1 | 1 | Trusted CPU vendors will never yield trivial errors due to human error |
| Setup stage | Sharp edges cut and hurt the setup personal | 3 | 4 | 12 | Wear appropriate clothing and gloves | Setup firm needs to ensure that the worker has the required equipment and buy it if needed. | Confirmation from the setup firm to confirm that the worker has the appropriate clothing. |  | 2 | 1 | 1 | Strong gloves won’t be cut badly |
| Setup stage | Rain permanently damaging electronics | 7 | 3 | 21 | Ensure that the setup is not done during the rain, or if it is, ensure that it is installed under a rain shelter. | Setup firm needs to confirm that hardware will not be damaged by rain upon insertion of new software. | Confirmation by setup firm to ensure that software will not be installed in the rain. |  | 1 | 1 | 1 | No rain ensures no consequences or likelihood. |
| Structural | Cars crashing into traffic pole, damaging software but leaving traffic light intact. | 7 | 1 | 7 | It is very unlikely that software will be damaged or altered by a physical impact before the structure itself is damaged beyond repair. | It is the job of the traffic light manufacturer to assure that the structure of the traffic light keeps the software safe upon a car collision. | No action needed- the software engineers cannot do anything and are not responsible for the safety of the structure itself. |  | 7 | 1 | 7 | This is unable to be mitigated by software engineers. |
| Setup stage | Car hits setup personal while on ladder or crane | 7 | 4 | 28 | Ensure that high vis markers and road cones are placed around the busy intersection upon setup. Also ensure that the speed limit is set to 30 km/h or lower, and that there are personal controlling the traffic flow. | Setup firm needs to acquire road cones, signs, and government consent. | Road cones, road signs, truck to move cones and signs, extra setup personal, and traffic flow personal. |  | 4 | 2 | 8 | With traffic control procedures enacted, chance of collision is extremely low. Lower speeds also yield safer consequences. |
| Electrical/Software system | Software overheats and stops running, causing traffic light malfunction | 7 | 4 | 28 | Check with the traffic light manufacturer that cooling methods are in place. Also design software so that it is heat efficient. | Traffic light manufacturer must put cooling methods in place, or at least provide sufficient heat flow, to ensure no overheating. The software engineers should run tests on the traffic light hardware and document heat levels. | Plans from the traffic light manufacturer, hardware from the traffic light manufacturer, time to test. |  | 7 | 1 | 7 | Risk likelihood is mitigated with appropriate cooling. |
| Software system | Power outage messes up memory state, causing traffic light malfunction upon reset | 7 | 2 | 14 | Firstly, traffic lights should be connected to external generators to be online 24/7, however in the case that it is not, rebooting the traffic light software should fully reset the state of it. | The software engineers should be aware of the software reboot process and how it affects the internal memory state. | Time to test the software rebooting, and money to pay the salaries of software engineers. |  | 1 | 2 | 2 | Although a reset of state is very unlikely anyway, ensuring memory is configured afterwards ensures no risk. |
| Setup stage | Tool malfunction injures worker or bystander | 2 | 4 | 8 | Use tools from a trusted seller. | The setup firm is responsible for providing workers with safe and trusted tools. | Safe tools or adequate funding to get them. |  | 2 | 2 | 4 | Safer tools will cause less harm |
| Setup stage | Tool misuse by worker injures worker or bystander | 3 | 4 | 12 | Ensure the setup workers are trained appropriately and are aware of the safety measures to be taken. | The setup firm is responsible for hiring workers that know what they are doing. | Adequate funding to hire the workers, plus a potential background check to ensure competence. |  | 2 | 2 | 4 | Workers that are responsible and knowledgeable will be less likely to misuse, and less likely to cause serious harm. |
| Setup stage | Car crash due to lights being temporarily disabled | 6 | 5 | 30 | Traffic control personal should be deployed to control the flow of traffic until the light software is functional again. | The setup firm should hire extra personal and road cones, signs, etc. | Money to hire individuals and gear, an extra truck to bring the gear to the intersection |  | 2 | 2 | 4 | With a speed limit and traffic control, a car crash will be unlikely and not cause much harm. |
| Setup stage | Setup personal getting sunburned | 3 | 4 | 12 | Under New Zealand law, companies can be held liable for not providing workers with sun protection. Sunscreen, hats, and appropriate clothing should be available to workers. Sunburn is also the prime cause of skin cancer. | Setup firm should provide workers with sunscreen, hats, and clothing to protect from the sun. | The firm should already have these, but if not- sunscreen, hats, wrap-around sunglasses, and long sleeve work shirts are required |  | 3 | 2 | 6 | After providing workers with sun protection, it is the worker’s responsibility to ensure it is used. |
| Setup stage | Car driver unable to see setup personal, and hits them whilst controlling traffic | 7 | 4 | 28 | Provide setup workers with high visibility clothing and set a speed limit for the intersection whilst the software is being installed. | Setup firm should provide all workers with high-vis vests, and high-vis helmets. A speed limit should also be set with consent from the council. | High-visibility vests, high-visibility helmets, and speed signs. Consent from the local council to set a speed limit will also be required. |  | 2 | 2 | 4 | Cars move slower and workers are more visible. Much less likely, and risk minimized. |
| Setup stage | Electric shock on worker from handling software | 8 | 4 | 32 | Give main setup worker thick insulative gloves and insulative boots. Also ensure main setup worker has the required training to replace the software. | Setup firm should provide this and ensure the personal in charge of replacement is trained. | Thick rubber gloves, and insulative rubber boots or overalls. Confirmation of the personal’s training or competence should also be required. |  | 4 | 2 | 8 | Risk minimized as much as possible. Electric shocks can still be harmful through rubber. |

To conclude, the biggest risks are also the risks that require some of the most expensive/time consuming mitigation. For the software side, the most important aspect is just to test the software extensively. A team should be dedicated towards testing the software in all environments, both to assume it is efficient enough not to blow a fuse, and to ensure that any faults in the software are caught before deployment. For the setup side of things, the setup firm is primarily responsible for the safety of the workers during installation, however it also becomes the engineer’s job to ensure that the listed safety precautions are being followed by the firm itself.

The hazard assessment table contains steps to mitigate all the risks identified.