Real-Time Industrial Automated Video Analytics System for Welding Defect Detection

Maksim Pavlov, Egor Rybin, Ivashnev Kirill, Aleksey Marakhtanov, Dmitry Korzun
Petrozavodsk State University (PetrSU)
Petrozavodsk, Russia
{mpavlov, rybin, ivashnev}@cs.petrsu.ru, marahtanov@petrsu.ru, dkorzun@cs.karelia.ru

***Abstract*—The control of quality is an obligatory stage of any welding work which makes problem of timely detection of welding defects is important for industry nowadays. Through digitisation it possible to solve this problem more efficiently and eliminate the human factor. This paper presents a real-time industrial automated video analytics system for weld defect detection. The system uses deep learning to analyze video images and detect weld defects in real-time. Experiments showed that the system can effectively detect weld defects with high accuracy and speed. A safety and trustworthiness analysis of the system showed that it can be reliable and safe for use in industrial manufacturing. The proposed solution has several key advantages for the industry: it allows for real-time data processinga and requires low computing power, making it an energy-efficient and cost-effective solution.**

I. Introduction

Inspection of the quality of welded joints is an obligatory stage of any welding work. Visual inspection is an obligatory stage of non-destructive testing and is often performed by the welder himself, which implies human factor and increases the risk of a missed defect. Despite its apparent simplicity, visual inspection of welded joints requires careful attention. The problem of quality assessment of welded joints is proposed to be effectively solved by automation of their assessment processes and use of artificial intelligence technologies. Software and hardware complex (automated system) of video analytics of welding defects control will allow timely detection of defects in the weld and their classification. The proposed solution can also be used for educational purposes, providing information on possible causes of defects, ways of their prevention and avoidance.

Modern existing solutions [1], [2] require a lot of resources to operate in real time and almost always requires the collection of its own dataset for the development of applied practical solutions [3], [4], which is rather labour-intensive and costly. These requirements limit their practical applicability, particularly in resource-constrained environments. Thus, the main contribution of our research is the development of a video analytics system capable of detecting welding defects in real time while operating on limited hardware and with small datasets.

To achieve this goal we have defined the following problems: collection and analysis of requirements for such industrial video analysis systems (software, hardware, subject area); development of a method for preparing and training a deep learning model on small amounts of data with the formation of data requirements; projecting and developing a video analytics system taking into consideration all the requirements; its security and trustworthiness analysis. The solution of these problems will allow to develop and create a modern video analytics system, which will be able to detect welding defects in real time with high accuracy and require small computing resources. The scientific novelty of this work lies in several key areas:

- Development of an efficient deep learning model: Unlike many existing approaches that require large datasets, our research focuses on the creation of a neural network capable of accurate detection and classification of welding defects with a limited number of training images. This approach addresses the challenge of dataset scarcity in industrial settings.
- Optimization for low-resource environments: We propose a system architecture optimized for real-time performance under limited hardware constraints, making it suitable for deployment in a wide range of industrial conditions.
- Trust and security in automated systems: We introduce a security and trustworthiness framework for automated video analytics in industrial environments, addressing safety concerns and ensuring reliability in defect detection processes.

Each finding may also be applied to another related R&D problems. We also aggregated the experience of our previous works in this study: the real-time underwater rainbow trout video surveillance system [5] and event driven image recognition [6].

The rest of the paper is organized as follows. Section II provides a literature review that forms the properties and requirements for state-of-the-art video analytics systems for welding defects. Section III presents a summary of the main welding defects of the study and the collected dataset. Section IV provides an analyses of the environmental and hardware constraints of the system. Section V shows our approach of real-time industrial automated video analytics system for welding defect detection. Section VII discusses safety issues associated with the use of automated systems in manufacturing. Section VII summarizes the key findings of this study.

II. Related Work

The development of automated video analysis systems, particularly for welding defect detection, has gained significant momentum in recent years by exploiting advances in neural networks and real-time detection technologies. Consider the related works in the context of our task's requirements (Table I)

Recent advancements in edge-centric video data analytics for industrial IoT systems, as explored in [7] and [8], highlight the shift towards local processing of video streams for real-time event detection and smart assistance services in manufacturing environments, demonstrating improved efficiency in equipment monitoring and contextual personnel recognition.

Recent research has focused on the use of convolutional neural networks (CNNs) for welding defect detection. For example, Manas Mehta presented a new CNN architecture that incorporates innovative modifications including ECA-Net integration for increased attention and [9] filtering. The addition of Bidirectional Feature Pyramid Network (BiFPN) association for bidirectional information flow and Adaptive Spatial Feature Fusion (ASFF) improved feature fusion at different scales. The results of the study showed a marked improvement in accuracy (6.5 %) and detection reliability compared to traditional method, but sacrificed runtime. In our solution, we propose to achieve high accuracy while keeping the speed of recognition by using a neural network based on YOLO architecture with a single pass over the image.

Real-time welding defect detection using video analytics has become a central theme in recent research. Almasoudi developed an advanced real-time defect detection system using a hybrid model combining CNNs and recurrent neural networks (RNNs), achieving impressive speed and efficiency in finding a defect in real-time without sacrificing accuracy [4]. Their results highlight the potential of combining different neural network architectures to improve performance in dynamic environments.

Table I. Summary table of project properties and existing solutions

Project property	Existing solutions	Proposed system
Analysis of welding defects in real time with a processing speed of at least 20 frames per second on an industrial panel computer	Implemented in part. Most solutions sacrifice runtime for accuracy [2]. Many of these also require more powerful hardware than a panel [4] industrial computer.	Executed in full. Keeping the speed of recognition by using a neural network with a single pass over the image and neural network quantization.
Detection and classification of undercuts, weld thickness, surface porosity, weld and product with an accuracy of at least 80 percent	Executed in full. However, requires datasets that require several tens of thousands of images [3].	Executed in full. This accuracy is achieved by careful preparation of the dataset and setting up the defect analysis model.

In summary, there are many techniques and mechanisms currently presented in research to improve the efficiency and accuracy of automated video analysis systems. Our work builds on this fundamental researches by focusing on integrating neural networks with robust video analysis techniques to develop a state-of-the-art welding defects detection system.

III. Dataset

The development of an automated video analytics system for controlling surfacing defects requires a requires dataset of images representing various types of defects. Before data collection, we formulated properties for such dataset to successfully solve the subsequent tasks (Table II). Following a thorough review of existing datasets, we selected a subset of defects most relevant to surfacing defects, specifically:

1) undercut;
2) weld thickness;
3) surface porosity.

Having these 3 classes is an important manufacturing need, because these defects were chosen due to their prevalence in welding processes and potential consequences for product quality and safety.

To collect and annotate the dataset, we relied on open-source repositories and online datasets. Unfortunately, we found only one publicly available dataset relevant to our research, which is based on the AtomicHack 2.0 dataset. This decision is related to the reason that practice shows to achieve good initial performance requires about a thousand images for each class of defects. Finally, our dataset consists of 2153 images of welding defects, annotated with the following classes:

1) adjacent defects (adj): splashes, arc burns, etc.
2) integrity defects (int): craters, slag, pores, etc.
3) geometry defects (geo): undercut, lack of fusion, overlap, etc. (class label: geo)

With regard to the requirements it's high important to us train the model to learn to distinguish and find each class as soon as possible. For this purpose, we selected the data so that the amount of defects in the images was as large as possible and obtained an average of 3.5 objects in each image.

Although our dataset is a good starting point, it has several limitations. Firstly, the dataset is relatively small, which may not be sufficient to train a robust machine learning model. Second, many of the images were taken from public sources, and the dataset was not originally specifically targeted at welding defects on our practice products, which may lead to reduced accuracy when performing real-world tests on images of our practice products.

Table II: Summary table of the welding defects dataset char-acteristics

Characteristic name	Value	Importance
Number of classes	3	High
Number of images	2153	Average
Number of annotations	7439	Average
Number of average annotations per image	3.5	High
Median image ratio	2160x2160 pixels	Small

Despite these limitations, the dataset can be used as a source of information for developing an automated video analysis

system for detecting cladding defects. It is planned to augment this dataset with additional images and annotations in order to increase its reliability and accuracy. The finalized version of the dataset will be more versatile than if we were to rely solely on our own images, as it will be based on a variety of data sources.

IV. Environmental and Hardware Requirements

A system of this nature must be able to withstand high temperatures, magnetic interference, vibration and noise while maintaining its accuracy and reliability. In addition, the system must be economically viable, requiring minimal investment in hardware and power consumption. Working with subject matter experts, we have extracted a number of requirements and constraints for the development of such a system.

Composition of the hardware-software part shall be as follows:

1) Hardware part should consist of a data acquisition device in the form of a video surveillance camera and a data processing and output device in the form of an industrial panel computer;
2) Software part realized on client-server architecture.

The use of high-tech equipment such as specialised cameras and sensors can be prohibitively expensive and impractical in many industrial environments.

The requirements for hardware in our case are as follows:

1) General requirements:
   a) Maximum operating temperature not less than +60°C;
   b) Protection against dust and moisture not less than protection class IP-50.
2) Requirements to the data acquisition device - CCTV cameras:
   a) The data source is a video camera or IP video camera;
   b) Receive video stream from IP-cameras via RTSP/RTMP protocol or directly;
   c) The image resolution of the video camera is not less than 1920x1080 pixels;
   d) Network stream bandwidth not less than 8192kbps;
   e) Support the transmission of at least 20 frames from the camera per second.
3) Requirements for data processing and output device in the form of industrial panel computer:
   a) Screen resolution not less than 1024x768 pixels;
   b) Processor not worse than a 4-core Intel Core i3-8145U of the 8th generation;
   c) At least 8 GB of RAM;
   d) Storage capacity of at least 256 GB;
   e) Processing speed of at least 20 frames per second for a frame with the image of a welded joint obtained from a video surveillance camera.

All these constraints must be carefully considered in the design and development of this type of system to ensure that it is practical and realisable in a real industrial environment. To address these challenges, we have selected the following hardware components for our system:

- CCTV cameras: our choice was HiWatch DS T215 C. This camera meets all our requirements and is equipped with a motorized pan-tilt-zoom mechanism, allowing it to rotate 360° and adjust its angle of view. This feature is particularly useful in industrial settings, where the camera may need to be adjusted to capture different areas of the production process.
- Industrial Panel Computer: we have selected a compact and rugged industrial panel computer RePC-PCS150T that is capable of withstanding high temperatures up to 85°C. Although it is not a high-performance computer, its processing power is sufficient for our system's requirements.

Welding defect detection must be able to run with real-time execution speed, to allow correction of found defects as soon as possible early in the manufacturing process, reducing costs and delays. By selecting these hardware components, we have ensured that our system can operate efficiently in an industrial environment while minimising cost and energy consumption. The choice of hardware components for the system must be carefully considered to ensure its practicality and feasibility in real industrial applications.

V. Video Analytics System

This section presents the architecture and developed prototype of the video analytics system for welding defects detection, including the procedure of defect detection and classification, and the results of our early experiments on training neural networks for this task. The performance of different neural network models and future research directions for developing similar systems are also discussed here.

A. System Architecture

The proposed our real-time industrial automated video analytics system for welding defects detecting is founded upon a client-server microservices architecture (Fig. 1), a paradigm that has garnered significant attention in recent years due to its scalability, flexibility, and maintainability. This architectural approach is particularly well-suited for complex industrial manufacturing environments, where the need for adaptability and fault tolerance is paramount. By decoupling the microservices approach allows us to decompose the system into smaller, independent services that can be developed, deployed, and scaled independently.

The following main microservices have been identified for our system:

- Camera connection module: responsible for connection and processing the video feed from camera.
- Image preprocessing module: image conversion to the size of the input layer of the neural network, image conversion to a vector format suitable for input to the neural network.
- Defect detection module: defect detection and classification, obtaining areas with probability of defects of certain

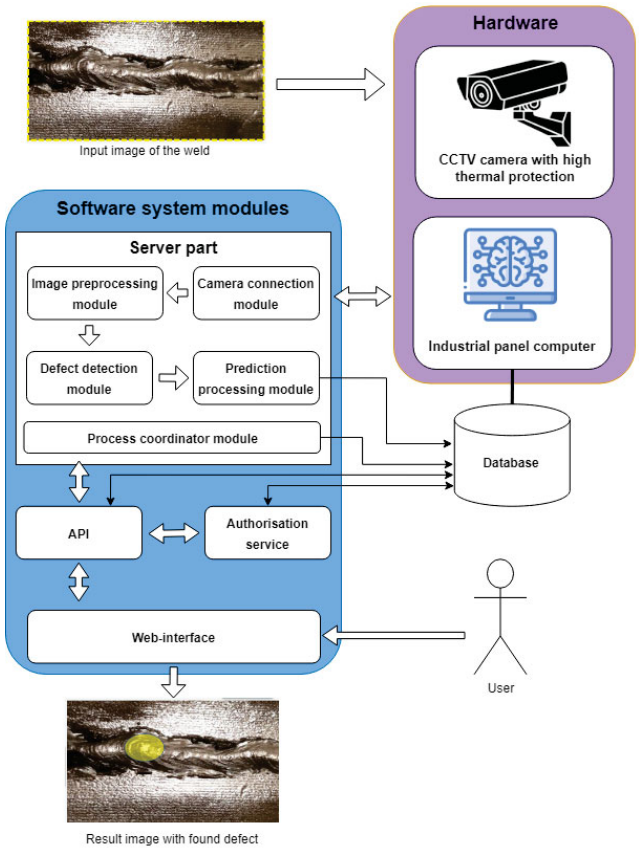

Fig. 1. Architecture of the hardware-software complex (automated system) of video analytics of surfacing defect monitoring

classes in them. Also filtering the results, discarding repetitive and significantly overlapping regions, discarding regions with low confidence of the neural network in the result.

- Prediction processing module: logging of defect detection events into the database, saving the image with the recognised defect.
- Process coordinator module: coordination of Camera connection module, Image preprocessing module, Defect detection module, Prediction processing module. Adjustment of module settings, tracking of their status and status, logging of system information.
- API: communication of the web interface with the software part of the system.
- Authorisation service: authorisation and verification of system users.
- Web-interface: interaction with the user, displaying the system results in a graphical interface.

The advantages of this architectural approach are multifaceted. Firstly, the scalability of our system is significantly enhanced, as each microservice can be scaled independently to meet the demands of the industrial manufacturing environment. Secondly, the flexibility of our system is improved, as we can leverage a diverse range of programming languages, frameworks, and databases to develop each microservice. Thirdly, the maintainability of our system is enhanced, as updates or replacements of individual services can be performed without affecting the overall system. Finally, the fault tolerance of our system is improved, as the failure of one microservice does not necessarily impact the operation of other services.

B. Defect Detection and Classification

The procedure of welding defect detection and classification is presented in Fig. 2. The following is a detailed description of the processing procedure.

1) Image Acquisition. At this stage, an initial image of the weld with a resolution of NxM pixels should be obtained from the camera. This could be done with ffmpeg program or OpenCV libraries over RTSP protocol, in case IP-camera over the internet, or Device driver, in case of USB cameras. receiving an image from the camera in RGB or Grayscale format.
2) Image preprocessing. The image is being converted into a format that can be accepted by the neural network. The image is resized to match the size of the input layer, which in our case with YOLO networks is 640 pixels. The image is then converted into a float 16 tensor.
3) Neural Network Application. This step involves using a neural network to detect and classify defects in the image from the previous step, as well as identify regions with probabilities of defect presence. The output is presents as the prediction matrix of each grid cell consisting of the coordinates of the defect areas in the format (x, y, w, h), the IoU metric and the probability of distribution of each class.
4) Post-processing. On this step we are using the non-max suppression method [10] to filter the predictions and select the most accurate areas with cladding defects, discarding repeated and overlapping regions, and discarding regions with low confidence. The output contains a list of predictions for each defect, including the coordinates of the defect area in the (x, y, w, h) format, and the IoU (intersection over union) metric value. It also includes the probability of the defect being present.
5) Saving and Displaying Results. Finally, the results of the image processing are saved to the database and displayed in the web-interface. This process involves saving the image and the coordinates of the bounding boxes around the detected defects, as well as logging information about the events that occurred during the processing, such as the timestamps, types, numbers, and coordinates of the defects. The process of displaying defects in the web interface involves representing them as a rectangular area and calculating their probability using methods from OpenCV and Pillow libraries. This process also includes notifications for the user.

The engineered system provides a robust and efficient solution for automated video analytics control of surfacing defects. The use of a neural network enables the system to learn from data and improve its performance over time. The

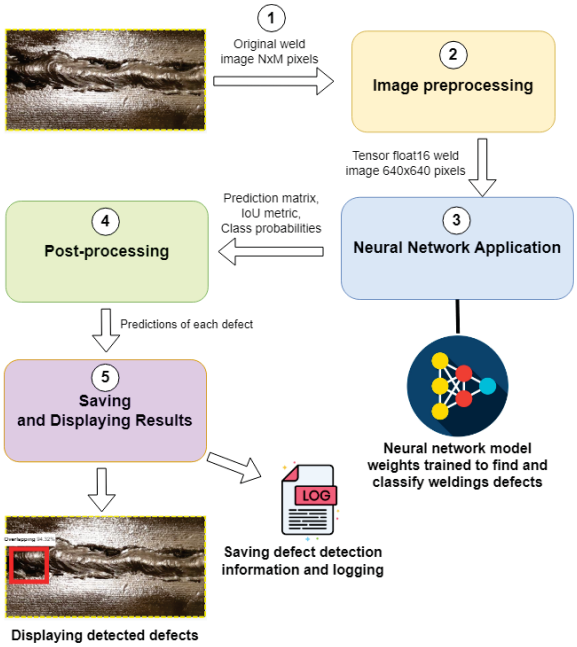

Fig. 2. Procedure of detecting surfacing defects and their classification

system's architecture is designed to be scalable, flexible, and easy to maintain, making it suitable for industrial settings. The use of a microservices approach and deep learning algorithms enables the system to provide high accuracy and robustness in defect detection and classification. The system's ability to detect and classify defects in real-time enables prompt action to be taken to prevent defects from affecting product quality.

C. Training & Early Experiments

Recently, numerous solutions exist to the task of object detection. And deep learning-based methods show one of the best results. Among these methods, YOLO (You Only Look Once) models have gained significant attention due to their high accuracy and speed [11], [12]. One of the main criteria for selecting the solution should be the ability to train the neural network on your specific class of objects and a set of points. It should also be possible to use your own dataset for training and convert annotations to the required format.

- The size and number of parameters and the number of layers directly affect the speed of inference. Modern computer vision tasks often require the ability to work in real time.
- Sufficient accuracy. In many tasks, even a slight error of a couple of pixels can be crucial. For example, it is important for determining the defect dimensions so that they can also be corrected automatically in the future.
- Having weights pretrained on the dataset with additional object classes can lead to better performance.

Neural networks YoLov8, YoLov9, YoLov10, in tiny and medium variants, were trained as early experiments for the task of welding defects. The models were trained for 300 epochs with a batch size of 16. The learning rate was set to 0.001, and the momentum was set to 0.9.

Table III. NEURAL NETWORK SPEED AND ACCURACY RESULTS

Neural network model	Inference, ms	Accuracy (mAP50)			
		Overall	Weld seam	Defect	Detail
Yolo8 nano	**0.7**	**0.84**	**0.97**	**0.57**	**0.99**
Yolo8 medium	2.7	0.83	0.97	0.53	0.99
Yolo9 tiny	0.8	0.67	0.91	0.12	0.98
Yolo9 medium	2.9	0.73	0.97	0.21	0.99
Yolo10 tiny	0.8	0.77	0.95	0.37	0.95
Yolo10 medium	3.2	0.79	0.96	0.42	0.96

Precise localization of defects bounding box is less important than correctly classifying defects in this case, because fix up requires manual intervention of human worker that will locate exact position and boundaries of defect themselves knowing position from system. Therefore mAP50 metric was chosen. For situations where defect detection and correction preformed autonomously mAP50-95 metric could be explored in the future work.

The results of the experiments are presented in Table III. As can be seen from the table, the YoLov8 medium model achieved the highest accuracy. Results shows that neural network learned to detect detail itself on the image with high accuracy and also weld seam relatively well, but the accuracy for defect detection is quite low. This could be attributed to the fact that welding defects in training dataset are rather different from each other as many of them were taken from public sources but weld seam being always clearly visible and well defined. These experiments show that the developed prototype is already fully operational and shows sufficient results of accuracy and speed in detecting defects for solving applied problems. For future research it is recommended to improve dataset quality with regard weld defects.

VI. IMPROVEMENT OF THE SYSTEM SECURITY

This section discusses security concerns related to the use of automated systems in production, as well as general security concerns associated with neural networks. It also proposes solutions to enhance the security of the system under development.

A. Industrial Safety Considerations

When using deep neural networks, it is important to take into account the security issues of their use. In the case of the problem of detecting defects in an industrial environment, the main safety criterion is a high level of trust in the video analysis system. Therefore, we assume that the trust and security of the system modules should be inextricably linked.

From the perspective of the manufacturer, it is essential that the system integrates into the production environment in a safe manner. To ensure this, the system should meet the following criteria:

- Accurate and reliable detection of welding defects.
- A minimum number of false positive and false negative detection.

- Access to the system should be limited to authorized users, and all actions within the system must be authorized.
- The system should continue functioning in case of a module failure.

B. Security Issues of Neural Networks

The use of neural network algorithms gives rise to a number of potential risks. The key issue with artificial neural networks lies in the fact that humans do not fully comprehend the mechanism of their operation. At its essence, a neural network represents a ”black box”, allowing for the insertion of ”backdoors” in its code, enabling remote control over the functioning of the model [13]. These vulnerabilities can remain undetected until triggered, making them difficult to identify. ”Backdoors” can be introduced into the model during its training by the developer. Additionally, there exists a technique known as ”Trojan attack”, which allows for the selection of triggers to activate specific neurons within the neural network without requiring access to training data [14].

Additionally, there is the issue of adversarial attacks, which involves manipulating input data to compromise the outputs of neural networks. This type of threat is particularly relevant for detection and classification algorithms. Data distortion occurs when an invisible disturbance is superimposed on the input image, which is then fed into the neural network’s input [15]. This interference can lead to inaccurate classification or detection of objects. The problem takes place when the attacker has access to the data source feeding the model.

Another type of threat to machine learning models is data poisoning. In this scenario, malicious data is intentionally introduced into the training dataset, leading to the incorrect training of the model [16]. This issue is particularly prevalent in situations where the data originates from untrustworthy sources.

In addition to deliberate security threats, there are also unintentional hazards associated with the intricacies of neural network training. A phenomenon known as ”overfitting” arises when a neural network fails to generalize data effectively and generates erroneous predictions [17]. This issue can have severe repercussions when deploying neural networks in production environments.

C. Cyber Immune Approach to System Development

In order to enhance the level of confidence in the deployment of neural network algorithms in industrial settings, it is prudent to adopt a cyber immune approach. This is a methodology based on the MILLS [18] and FLASK [19] technologies, proposed by Kaspersky Lab [20]. Rather than pursuing a comprehensive search for all possible sources of vulnerability, this approach focuses on identifying trusted and untrusted elements within the system architecture. This strategy enables the maintenance of a robust and trustworthy system operation in the face of potential threats by leveraging components that bolster data integrity and effectively prevent compromised information from infiltrating other system modules.

The main stage preceding the development of an architecture, according to the cyber immune approach, is the definition of security goals and assumptions. In our case, the main security goal is to adequately detect surfacing defects. We do not allow the case when a defect is not handled by the defect detection module. More precise security goals can be defined by specifying the values that need to be protected during the system’s operation. An example for our system is given in Table IV. It presents possible negative scenarios, consequences, and threat levels for each value of the system.

Table IV. RISK AND SECURITY VALUES OF THE SYSTEM

Risk	**Vulnerability**	**Consequences**	**Risk Level**	**Mitigation Measures**
Loss of video analytics data	Equipment failure, property damage	Missed defects, downtime, financial losses	High	Regular data backups, monitoring systems for equipment status
False positives from the system	Low quality of analysis algorithm	Resource overuse, reduced trust in the system	Medium	Improve analysis algorithms, train the model on more data
Incorrect calibration of equipment	Configuration errors	Incorrect data interpretation, welding quality	High	Regular checks and calibration of equipment, operator training
Software failures	Vulnerabilities in software	System downtime, data loss	High	Update software, vulnerability testing

The security assumptions include the following:

1) The camera used is reliable and trustworthy.
2) The employees interacting with the system are qualified, trustworthy, and authorized to use the system.
3) Camera connection module, image processing module, prediction processing module and web-interface are trustworthy and reliable.
4) The dataset is prepared by reliable and trusted members of the research team.

Thus, in the first iteration of development, we focus on the surface defect detection module as the main untrusted entity. As can be observed from the Table IV, the primary risks are associated with this component of the system. In further iterations, the architecture policy may change due to the clarification of security assumptions during testing. Adversarial attacks and data poisoning are not typical for our case, due to the security assumption number 4. The main potential source of threat is the presence of ”backdoors” in the selected neural network model. The problem of retraining is also likely, but it is usually identified at the stage of preparing the model for implementation.

D. Development of a Cyber Immune System Architecture

In order to prevent security threats in an implemented system, a cyber immune architecture for the project was developed. The diagram can be seen in Fig. 3. The diagram depicts the trusted computing base of the surface defect control system, highlighting the security domains. Additionally, there is a qualitative assessment of these domains based on the complexity and size of the code within each module. Developing a cyber immune architecture presents a challenge in ensuring the reliability of complex and XL-class domains, as it requires substantial time and resources.

Fig. 3. Cyber immune system architecture

Let us take a closer look at the principles of marking security domains in this particular example.

- We consider the camera module to be trusted, since it is assumed that its configuration and connection will be performed by the staff of the research group. The camera communicates via the network interface only with the host on which the defect detection module is deployed, which eliminates the possibility of remote connection and compromise of its operation. Thus, the output of the camera can be considered high-integrity data.
- The camera connection module and image preprocessing module are also considered trusted domains, since its programming is handled by staff.
- At the level of the defect detection module, a YOLO neural network architecture is used, which, according to the issues described above, makes it difficult to consider it a trusted entity. Therefore, we assume that the defect detection module generates low-integrity data that must be verified and processed at the prediction processing module level.
- The quantitative analysis of the module reveals a high level of complexity in the code, but it also has a medium volume, making it possible to use a cyber immune approach. Thus, the prediction processing module is considered a domain that increases integrity and provides high-integrity output data in the Web interface that the user interacts with.

The above method is just the first step towards developing a cyber immune system that meets security requirements. Other stages of developing a cyber immune architecture policy include modeling negative work scenarios, unit testing and clarifying the trusted computing base. In the future, we will continue to develop more detailed security measures for specific domains in order to enhance data integrity. The main areas that need to be addressed in order to increase the reliability of neural networks in industrial settings include the use of explainable AI techniques, the implementation of feedback loops, regularization, and standardization of industrial AI usage. Additionally, there are other possible solutions that may be explored in further research.

VII. Conclusion

This paper introduces an industrial automated real-time video analysis system for welding defect detection that builds on the foundation laid by the previous researchers in this field. In contrast to existing solutions, which often require significant computational resources and large datasets, our system is engineered to operate in real-time with low hardware requirements. Using a deep learning approach and a client-server microservices architecture, our system achieves high accuracy and reliability in welding defect detection, making it a valuable tool for quality control and process optimization in industrial manufacturing environments.

The problem solving process resulted in environmental constraints and hardware requirements based on real industry demands. For example, these requirements allow the camera and computer to be placed in an intensive welding area. Based on the experience gained, a system architecture is developed to detect welding defects using artificial intelligence and computer vision technologies in real time. The neural network trained on a welding defect dataset demonstrates an overall accuracy of 0.84 (mAP50 metric) with an inference time of 0.7ms. The obtained results may also be applied to other related R&D problems. Key finding of this study:

- Hardware requirements for harsh environmental condition near welding operations;
- Hardware requirements for minimal required processing power;
- Dataset quality and quantity requirements;
- Comparison of different neural networks for task of welding defect recognition;
- System architecture for software realization;
- Cyber Immunity approach for ensuring security of proposed system;

With Industry 4.0 developing, the demand for intelligent and autonomous quality control systems will only grow. Future

R&D directions may include exploring the possibility of applying such systems to other industrial processes, integrating it with new technologies such as IoT and edge computing, developing more advanced algorithms to further predictive analytics for defect occurrence and improve detection accuracy and efficiency. In addition, the development of more robust and secure systems will be critical to ensuring widespread adoption of automated video analytics in industrial manufacturing. By pushing the boundaries of what is possible with automated video analytics, we can unlock new levels of productivity, efficiency and innovation in the manufacturing sector.

ACKNOWLEDGMENT

The research described in this publication was made possible in part by R&D Support Program for undergraduate and graduate students and postdoctoral researcher of PetrSU, funded by the Government of the Republic of Karelia.

REFERENCES

[1] Y. Zuo, J. Wang, and J. Song, "Application of yolo object detection network in weld surface defect detection," *2021 IEEE 11th Annual International Conference on CYBER Technology in Automation, Control, and Intelligent Systems (CYBER)*, pp. 704–710, 2021.

[2] P. K. Ravichandiran, D. Ramachandran, and R. Jegadeeshwaran, "Welding defect identification with machine vision system using machine learning," *Journal of Physics: Conference Series*, vol. 1716, 12 2020.

[3] P. Sassi, P. Tripicchio, and C. A. Avizzano, "A smart monitoring system for automatic welding defect detection," *IEEE Transactions on Industrial Electronics*, vol. 66, no. 12, pp. 9641–9650, 2019.

[4] F. M. Almasoudi, "Enhancing power grid resilience through real-time fault detection and remediation using advanced hybrid machine learning models," *Sustainability*, vol. 15, p. 8348, 2023.

[5] M. P. Pavlov, V. V. Perminov, and A. G. Marakhtanov, "Real-time system for detection hidden and visible keypoints of rainbow trout," *2023 International Conference on Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS)*, pp. 161–165, 2023.

[6] B. Nikita, R. Egor, and K. Dmitry, "An Event-Driven Approach to the Recognition Problem in Video Surveillance System Development," in *2022 32nd Conference of Open Innovations Association (FRUCT)*. Tampere, Finland: IEEE, 2022, pp. 65–74.

[13] A. B. Menisov, A. G. Lomako, and A. S. Dudkin, "Method for protecting neural networks from computer backdoor attacks based on identifying bookmark triggers," *Scientific and Technical Bulletin of Information Technologies, Mechanics and Optics*, vol. 22, no. 4, pp. 742–750, 2022.

[7] N. Bazhenov and D. Korzun, "Event-driven video services for monitoring in edge-centric internet of things environments," in *2019 25th Conference of Open Innovations Association (FRUCT)*. IEEE, 2019, pp. 47–56.

[8] N. Bazhenov, A. Harkovchuk, and D. Korzun, "Edge-centric video data analytics for smart assistance services in industrial systems," in *Proc. 14th Int'l Conf. on Mobile Ubiquitous Computing, Systems, Services and Technologies (UBICOMM)*, 2020.

[9] M. Mehta, "Aff-yolo: A real-time industrial defect detection method based on attention mechanism and feature fusion," 2022, pREPRINT (Version 1) available at Research Square.

[10] A. Mrutyunjay, P. Kondrakunta, and H. Rallapalli, "Non-max suppression for real-time human localization in long wavelength infrared region," *Springer International Publishing*, pp. 166–174, 2020.

[11] P. Jiang, D. Ergu, F. Liu, Y. Cai, and B. Ma, "A review of yolo algorithm developments," *The 8th International Conference on Information Technology and Quantitative Management (ITQM 2020 & 2021): Developing Global Digital Economy after COVID-19*, vol. 199, pp. 1066–1073, 2022.

[12] V. Viswanatha, R. K. Chandana, and A. C. Ramachandra, "Real time object detection system with yolo and cnn models: A review," *arXiv*, 2022.

[14] Y. Liu, S. Ma, Y. Aafer, W.-C. Lee, J. Zhai, W. Wang, and X. Zhang, "Trojaning attack on neural networks," in *25th Annual Network And Distributed System Security Symposium (NDSS 2018)*. Internet Soc, 2018.

[15] E. A. Chekhonina and V. V. Kostyumov, "Overview of advanced attacks and defense methods for object detectors," *International Journal of Open Information Technologies*, vol. 11, no. 7, pp. 11–20, 2023.

[16] F. A. Yerlikaya and Şerif Bahtiyar, "Data poisoning attacks against machine learning algorithms," *Expert Systems with Applications*, vol. 208, p. 118101, 2022.

[17] H. Li, J. Li, X. Guan, B. Liang, Y. Lai, and X. Luo, "Research on overfitting of deep learning," in *2019 15th international conference on computational intelligence and security (CIS)*. IEEE, 2019, pp. 78–81.

[18] R. J. DeLong and E. Rudina, "Mils architectural approach supporting trustworthiness of the iiot solutions," *IIC whitepaper. Boston, Industrial Internet Consortium*, 2021.

[19] R. Spencer, S. Smalley, P. Loscocco, M. Hibler, D. Andersen, and J. Lepreau, "The flask security architecture: System support for diverse security policies," in *8th USENIX Security Symposium (USENIX Security 99)*, 1999.

[20] S. P. Sobolev, "Cyber immune development approach. microservices based illustration," *Bulletin of the St. Petersburg University. Applied mathematics. Computer science. Management processes*, 2024.