SAND2019-13551PE

FY20 Kickoff for NA-241 Deep Learning Project using PredNet

Presenters:

Joshua Rutkowski (PI)

Michael R. Smith

SNL team (not present):

Michael Hamel

David Hannasch

Marcellus Smith (intern)

7 November 2019

Outline

Review FY19 task

- Data collected
- PredNet algorithm evaluation
- Image differencing

PWP Task 4 FY20 subtasks

- Data collection needs
- Streamline PredNet algorithm workflow
- Documentation and workflow design for IAEA
- ML/DL limitations awareness
- Assessment/findings report: PredNet for NGSS

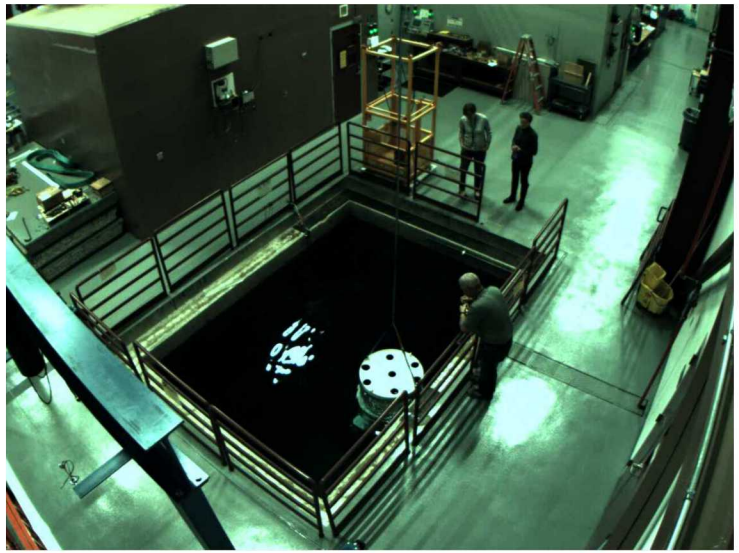
Data Collection at the Gamma Irradiation Facility

Developed a proxy use-case to transfer a large (approx. 5ft. tall by 3 ft. wide) container into and out of a floor vault

Deployed two NGSS cameras in the Gamma Irradiation Facility (GIF)

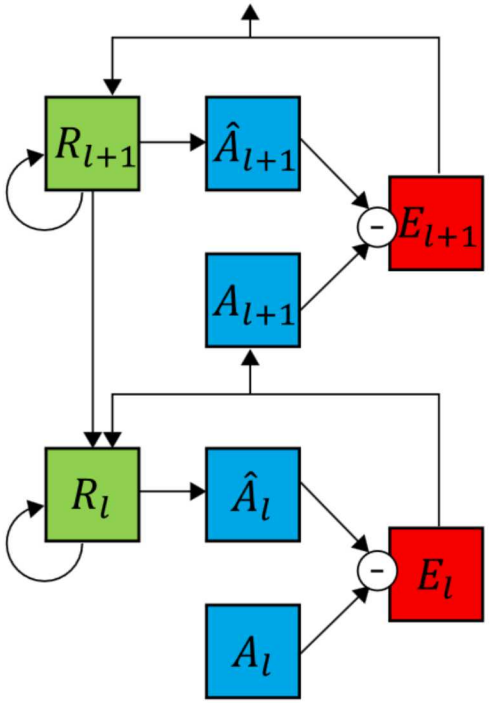
Collected down-time data and active scripted container movements over multiple days

Collections include both full (water) and empty floor vault scenarios



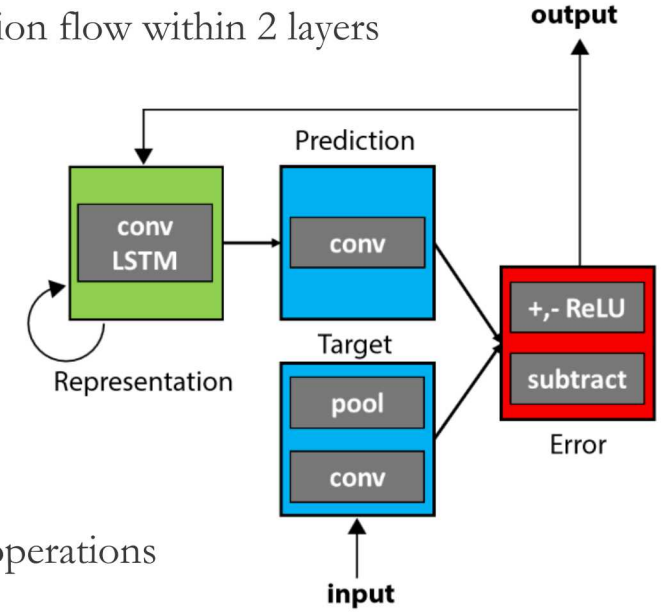
PredNet—predict the next frame in a video

- Each layer in the neural network consists of:
  - R_l: representation neurons
  - $\hat{A}_l$: layer-specific predictions at each time step
  - A_l: layer-specific target
  - E_l: layer-specific error term
- Errors are propagated to the next layer



- Information flow within 2 layers

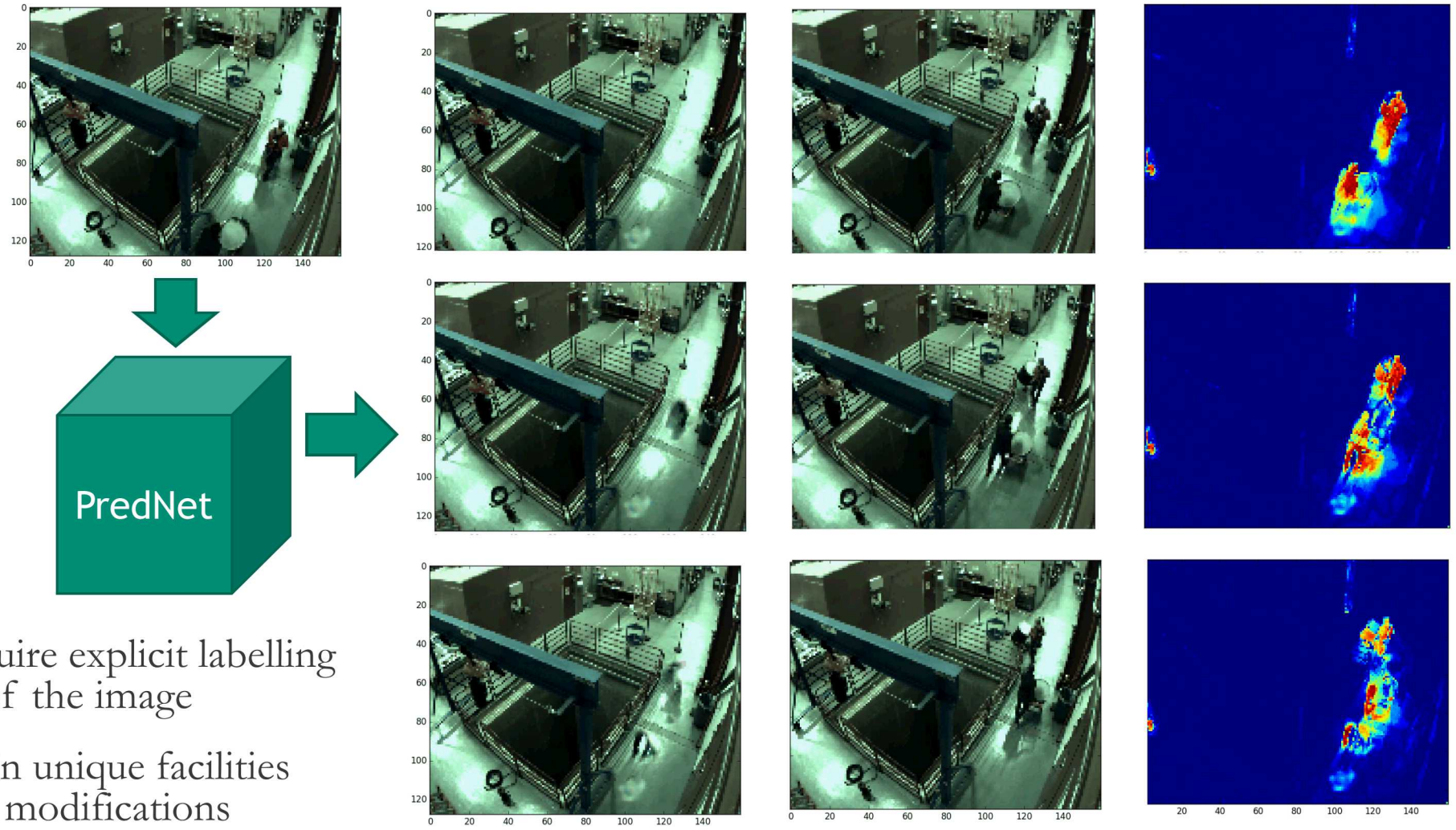
- PredNet Work:
  - Accept longer test sequences
  - Test the sensitivity to the length of test and training sequences
  - Build pipeline around PredNet for easier experimentation



- Module operations

PredNet—predict the next frame in a video

Directly addresses the need of identifying anomalous activity in video



Does not require explicit labelling of portions of the image

Can be used in unique facilities with minimal modifications

PredNet Results Analysis

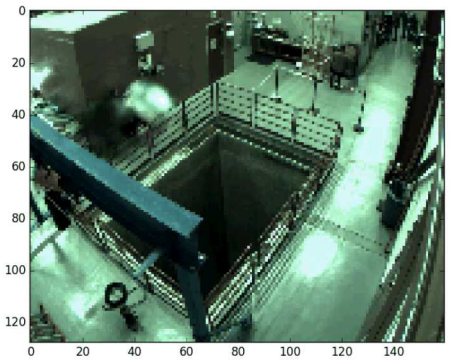
Compare **Predicted Image** to **Actual Image**

1. Convert both images to grayscale
2. Calculate Squared Error, E, for each pixel i

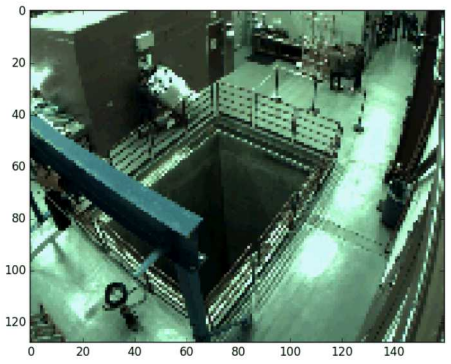
$$P = Predicted\ Image \qquad A = Actual\ Image$$

$$E_i = (P_i - A_i)^2$$

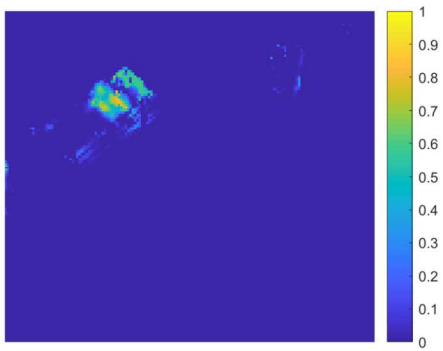
Predicted Image



Actual Image



Squared Error Image



FY20 PWP task 4

4	Develop PredNet algorithm	Milestone	Complete optimization of PredNet	SNL	08/31/2020
		Deliverable	Guidance on implementing PredNet	SNL	09/30/2020

Task 4. Develop PredNet algorithm (Lead Lab: SNL)

In FY19, some initial ways to quantify the anomalies were created, but they were not optimized for safeguards relevance. This task will investigate the best suited calculations for the image differencing based on the benefit to detecting safeguards-relevant activities. After the calculations are made, inspectors will want to receive notifications about anomalies in a clear and useful mechanism. This task will provide the IAEA with guidance on implementing PredNet, calculating image differences and setting thresholds that are relevant to safeguards activities.

Milestone: Complete optimization of PredNet for safeguards relevance by Aug. 31, 2020.

Deliverable: Guidance on implementing PredNet by Sept. 30, 2020.

FY20 PWP task 4

4	Develop PredNet algorithm	Milestone	Complete optimization of PredNet	SNL	08/31/2020
		Deliverable	Guidance on implementing PredNet	SNL	09/30/2020

Task 4. Develop PredNet algorithm (Lead Lab: SNL)

In FY19, some initial ways to quantify the anomalies were created, but they were not optimized for safeguards relevance. This task will investigate the best suited calculations for the image differencing based on the benefit to detecting safeguards-relevant activities. After the calculations are made, inspectors will want to receive notifications about anomalies in a clear and useful mechanism. This task will provide the IAEA with guidance on implementing PredNet, calculating image differences and setting thresholds that are relevant to safeguards activities.

Milestone: Complete optimization of PredNet for safeguards relevance by Aug. 31, 2020.

Deliverable: Guidance on implementing PredNet by Sept. 30, 2020.

…investigate the best suited calculations for the image differencing based on the benefit to detecting safeguards-relevant activities.

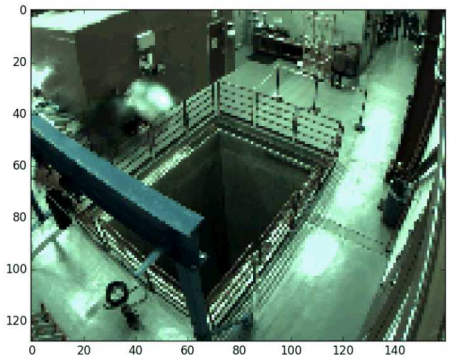
Compare **Predicted Image** to **Actual Image**

1. Convert both images to grayscale
2. Calculate Squared Error, E, for each pixel i

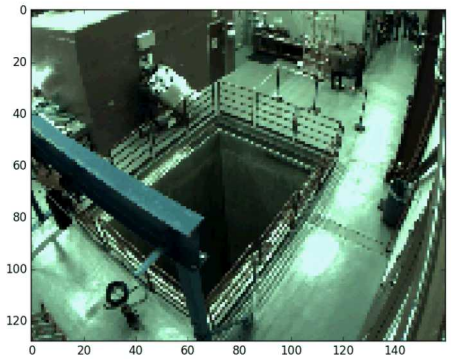
$P = Predicted\ Image$ $A = Actual\ Image$

$$E_i = (P_i - A_i)^2$$

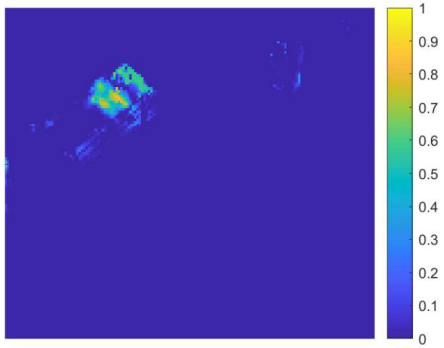
Predicted Image



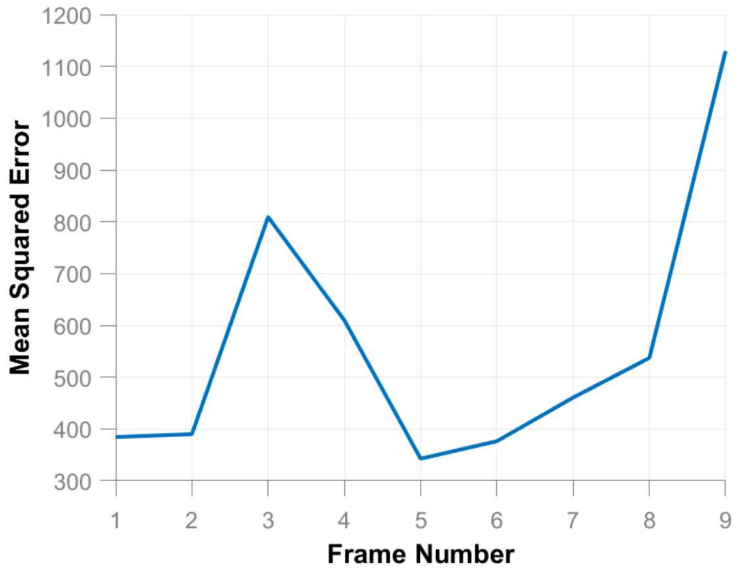
Actual Image



Squared Error Image



receive notifications about anomalies in a clear and useful mechanism

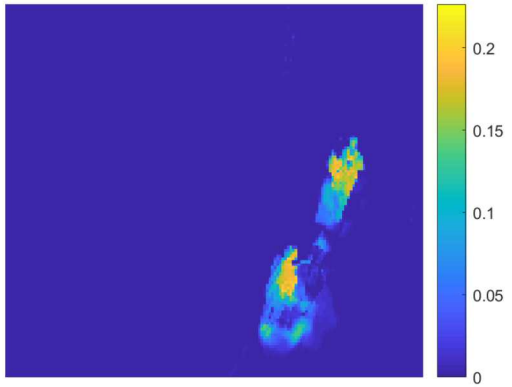


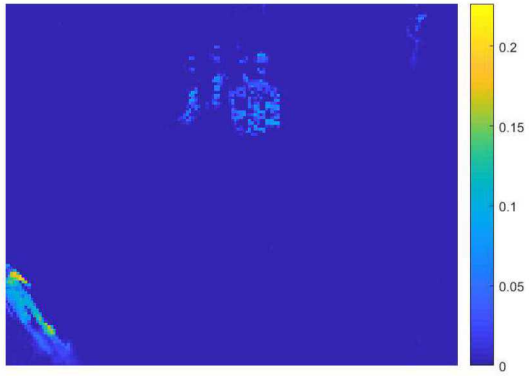
Frame 8

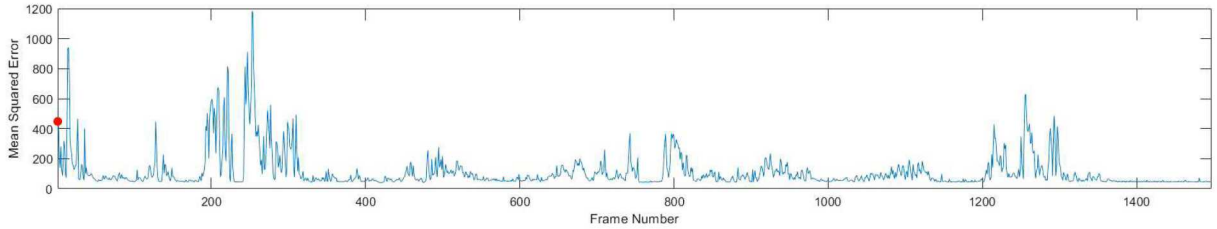
Frame 9 Prediction

Frame 9 Actual

Predicted vs. Actual Difference




0.2
0.15
0.1
0.05
0


Mean Squared Error
1200
1000
800
600
400
200
0
200
400
600
800
1000
1200
1400
Frame Number

provide the IAEA with guidance on implementing PredNet…setting thresholds that are relevant to safeguards activities

Deliverables

- Code and documentation
- Sample input videos and the output they should produce
- Code install and workflow guidance documents
- DL limitations awareness statement
- Findings report

Code and Code Documentation

Python package installable via pip (standard)

Deliverable to isolated system as .tar.gz (like any Python package)

Invoke with python -m (like python -m pytest)

Tentative plan for interface: python -m ModelNAME (path to videos) [--save-model at_location] [--load-model model_file]

Uses TensorFlow as the machine learning engine, so requires an NVIDIA GPU

No licensed code, no license server (no MatLab)

Documentation in Sphinx (as standard for Python packages)

Per-function docstrings both aid IAEA code review and get incorporated into HTML API reference

As much sample data as possible; pytest --pyargs ModelNAME to check that everything appears to be running correctly on your computer and GPU.

Sample data

We need as much data as possible!

The good news: we don't need labeled data, just videos

We need training and testing datasets for the IAEA so they can evaluate code

Need to define requirements for BNL testbed scenarios

Delivering 2 or more sample datasets to IAEA could be helpful

Code install and workflow guidance documents

Workflow documents explaining how to install dependencies and code

Machine setup/implementation

Sample datasets

Image difference calculation description

DL limitations awareness statement

Essay on the limitations associated with using deep learning

Essay should highlight safeguards-related scenarios:

- Facility operators undermining through consistent behavior
- Code manipulations
- Taking advantage of code 'blind spots'
- Privacy

Key point: this only looks for activity in the video that is out of the ordinary. If they do the same thing every day for a year, no matter what that is, it won't be flagged.

Security of data: models derived from videos should be protected at the same level as the original videos. A model that encodes what is "normal" at the facility naturally allows anyone who has it to reproduce (roughly) the video footage. Sharing models across facilities is potentially valuable but might not be permissible in all the IAEA's use-cases.

Mitigations to these issues are known and will be documented.

Summary

- Code and Code documentation
- Sample data
- Code install and workflow guidance documents
- DL limitations awareness statement
- Findings report

Timeline:

Milestone: Complete optimization of PredNet for safeguards relevance by Aug. 31, 2020

Deliverable: Guidance on implementing PredNet by Sept. 30, 2020