Vulnerability Assessments of Induction Machine-Based Multistage Rolling Mill System Under Sensor Integrity Attacks

Kun Hu, *Member, IEEE*, Jin Ye, *Senior Member, IEEE*, and Wenzhan Song, *Senior Member, IEEE*

***Abstract*—In this article, we provide vulnerability assessments for a multistage rolling mill system under various sensor integrity attacks in response to the increasing cyber-attack threats in manufacturing systems. We first present detailed modeling of the whole system. Then, five typical integrity attacks are designed to simulate the possible cyber threats to the thickness sensor, speed sensor, and looper angle sensor. To comprehensively evaluate the impact, we propose a vulnerability assessment framework that includes 1) five device-level evaluation metrics to assess the manufacturing quality, operation safety and milling productivity, and 2) system-level indices to reflect the comprehensive impact on the multistage system. To verify the effectiveness of the proposed evaluation methods, simulations of different sensor attack scenarios in a five-stage rolling mill system are conducted in MATLAB/Simulink. The proposed metrics successfully assess the impact caused by different attack cases and show the possibility of applying the proposed indices for attack detection and mitigation in the future.**

***Index Terms*—Manufacturing cyber-physical security, sensor integrity attacks, vulnerability assessment.**

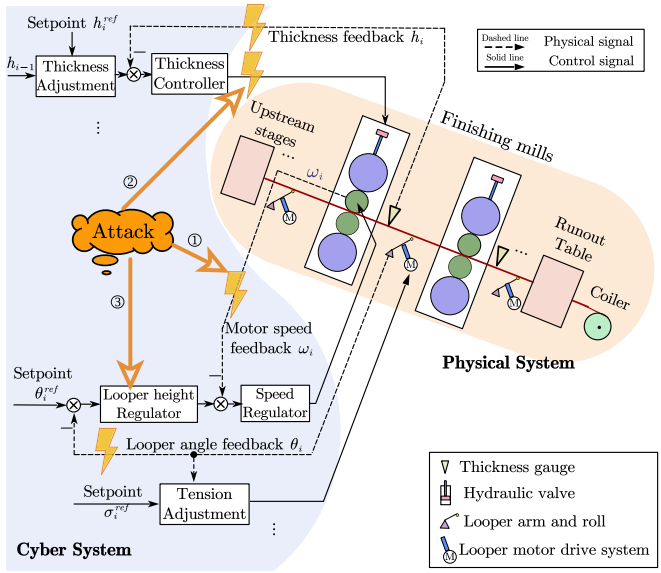

Fig. 1. Simplified layout of multistage rolling mill system.

I. Introduction

A. Motivation and Incitement

HOT/COLD rolling mill in metallurgical has played and is still playing a vital role in the industrial fields due to a huge quantity of metal production each year, such as steel plate, cold-drawn bars, seamless pipes, rails, etc [1]. To produce high-quality products, improve production efficiency, and maintain secure manufacturing, advanced communication and networking technologies are introduced in the rolling and milling process. A simplified layout of a multistage rolling mill system is shown in Fig. 1. Typically, the finishing rolling mill system cascades with five to seven stages. The thickness of the raw material is reduced progressively after the plate is extruded from one stage by another with the cooperation of three subsystems, namely, the hydraulic milling system, the looper tension control system, and the motor drive system. Therefore, the multistage rolling mill system is an assembly of sensors, physical actuators, controllers, and monitor/alarm systems [1], [2].

Apparently, the adoption of the Internet of Things (IoT) in the cyber-physical system facilitates control and monitoring, however, it also makes the system more vulnerable to cyber-attacks. The first publicly known case in the steel manufacturing system was in December 2014, a German steel mill was accessed by a spear phishing email, which led to cyber attacks on multiple components of the system and eventually caused massive physical damage to the integrated steel mill [2]. Take the rolling mill system as an example. The crackdown of components like the measuring sensors in the system can possibly lead to the failure of thickness reduction of the metal plate. Then, as a cascaded system, the resulting fault signals can be passed to the stages next to the damaged one and cause a series of consequences such as poor manufacturing productivity or even disasters that impact human life. In addition to the manufacturing system,

Manuscript received 28 October 2022; revised 15 April 2023; accepted 14 February 2024. This work was supported in part by U.S. National Science Foundation under Grant ECCS-EPCN 2102032 and Grant NSF-SATC-2019311, and in part by the U.S. Department of the Air Force under Grant FA8571-20-C-0017. Paper no. TII-22-4478. *(Corresponding author: Jin Ye.)*

The authors are with the College of Engineering, University of Georgia, Athens, GA 30605 USA (e-mail: kun.hu@uga.edu; jin.ye@uga.edu; wsong@uga.edu).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TII.2024.3370240.

Digital Object Identifier 10.1109/TII.2024.3370240

growing cyber attack cases are also reported in industrial control systems equipped with IoTs such as power systems, smart buildings, electric vehicles, etc. [3], [4], [5], [6], [7], [8], [9]. Cyber-physical security issues have raised concerns widely in the industry world.

Therefore, there exists a strong motivation for us to do attack prewarning/monitoring, cyber-physical attack detection, and attack-resilient control against cyber-physical attacks. As the first step, we start with the vulnerability assessment of the multistage rolling mill system. The purpose of "vulnerability assessment" is to 1) understand the consequences of cyber-physical attacks, 2) quantify the impact caused by the attack, and 3) provide insights into other security countermeasures such as detection and resilient control.

B. Literature Review

To address the cyber-attacks issues in manufacturing systems, state-of-art research put much effort into cyber-physical attack detection, vulnerability assessment, and resilient control. The threat models in the previous studies are categorized as jamming attacks, replay attacks, Denial-of-service (DoS) attacks, and integrity attacks [10], [11], [12]. The former three attacks usually target the packet transmission in order to disrupt the network in the cyber domain [10], while the integrity attacks target the data transmission of the sensors or the controllers [12], which to some extent are the attacks on the node side in the physical system. As the focus of this article, sensor integrity attacks, also referred to as Man-In-The-Middle (MITM) attacks in [10], are the attacks launched to the measuring sensors with the purpose of modifying the data, which is feasible given the fact the sensors are usually not encrypted. In [3] and [12], the sensor integrity attacks are modeled as scaling attacks, min–max attacks, and additive attacks, which is similar to the fault modeling in the rolling mill system, where the fault is modeled as a multiplicative or an additive number of the actual signal [13], [14], [15], [16].

Although there is extensive literature on fault detection and diagnosis [13], [14], [15], [16], [17], [18], cyber-physical security of the rolling mill system under sensor integrity attacks has not yet been well studied. Relevant literature regarding the vulnerability assessment in the manufacturing system is given as follows.

Hutchins et al. [19] explored the vulnerability assessment for manufacturing systems from the perspective of data risk management in the cyber system. The article establishes a framework to identify generic and manufacturing-specific vulnerabilities by using the data flowing between enterprise nodes in the supply chain. The work targets risks in the cyber domain from the risk management perspective rather than evaluating cyber-physical securities. Therefore, the method cannot be transplanted for vulnerability assessment under sensor integrity attacks as it solely focuses on data flowing between nodes in the cyber domain.

Later, DeSmit et al. [20], [21] provided a systematic vulnerability assessment that uses decision trees to identify cyber-physical vulnerabilities in manufacturing systems. The authors first establish intersection mappings of different entities from both the cyber domain and physical domain, whereas the intersections as they expect are the most vulnerable through the production process. Then five evaluation metrics are proposed to determine the vulnerability impact of each intersectional node. However, the evaluation metrics proposed failed to provide quantitative assessment for other components in the system but solely the intersectional nodes. The proposed evaluation indices are also not sufficient to comprehensively assess a complicated cyber-physical system. Therefore, the proposed assessment framework is not suitable for a rolling mill system.

In addition, Guibing et al. [22], [23] provided quantitative vulnerability assessment in a complex networked manufacturing system by defining the manufacturing system with *node*, *edge*, *local world,* and *growing network*. With the definitions, the article proposes vulnerability indices including structural vulnerability indices and functional vulnerability indices by calculating the *connectivity*, *cohesion degree*, *average path length* in the network (see the definition in the paper). Therefore, the article focus more on data transferring between nodes in the cyber domain. The nodes in the network are greatly simplified in order to assess the connectivity and the proposed indices only focus on the structural vulnerability indices and functional vulnerability. For these two reasons, the vulnerability assessment method in this article is not suitable for the rolling mill system.

In light of the previous vulnerability assessment work on the cyber-physical issues in the manufacturing system, there are some key issues as follows: 1) the assessment methods focus more on the data transferring in the cyber domain; 2) the proposed evaluation indices are not sufficient to provide a comprehensive assessment; 3) the proposed framework is not suitable for a cyber-physical system that requires both device-level and system-level assessment. Most importantly, to our best knowledge, there is no cyber-physical-security assessment framework available for a multistage rolling mill system. A comprehensive vulnerability assessment of the rolling mill system should consider 1) a useful assessment framework to present the manufacturing system, 2) device-level evaluation metrics for each subsystem to understand the consequences of attacks, and 3) an overall system-level metric to provide qualitative and quantitative assessments.

C. Contribution and Article Organization

Inspired by the analysis above, in this article, we present a systematic methodology to assess the vulnerability of the multistage rolling mill system due to sensor data integrity attacks. The main contributions are as follows.

1) A novel vulnerability assessment framework for the multi-stage rolling mill system is proposed.
2) Novel device-level evaluation metrics for the looper and tension control system, the motor drive system, the thickness control system in each stage are proposed.
3) A system-level impact index for the multistage rolling mill system is established.
4) By using innovative evaluation metrics, qualitative and quantitative impact analysis under a series of sensor integrity attacks are presented, revealing the coupling and interactions among stages when the attack happens. The

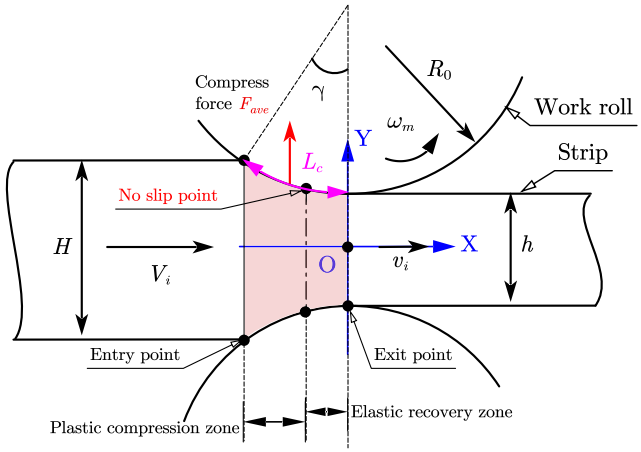

Fig. 2. Deformation process of the ith mill stage.

conclusion can be further used as guidelines for attack detection and mitigation.

The rest of this article is organized as follows. In Section II, the modeling of three physical parts in the each mill stage are described. Then, Sections III and IV provide the attack modeling and evaluation metrics. In Section IV, the simulation and vulnerabilities assessment are presented. Finally, Section V concludes this article.

II. Modeling of Multistage Rolling Mill System

In this article, the vulnerability assessment work is based on a five-stage rolling mill system. Each finishing stage is identical and includes subsystems, such as the hydraulic milling system, motor drive system, and looper tension control system. Therefore, in this section, the modeling of the multistage system is divided into three categories, the deformation process that achieves vertical movement by the thickness control system, the rolling process that realizes the horizontal movement by the induction machine drive system, and the strip tension formation between stages achieved by a looper and tension control system. The following sections will show how each subsystem is conducted and how each stage interacts with each other with modeling details.

A. Modeling of the Deformation Process

The deformation process in each stage realizes the thickness reduction for the metal strip as shown in Fig. 2. In the front view of the roll-bite area in Stage i, the strip is being extruded by the top and bottom work rolls with the thickness plastically reduced from H_i to h_i. The averaged flow stress (engineering stress) σ_c of the roll-bite area is approximated as [24]

$$\sigma_c = K_s \frac{\epsilon^n}{1+n}, \epsilon = \ln \frac{H_i}{h_i} \tag{1}$$

where ϵ is the strain in the roll-bite area; K_s is the coefficient of material strength in MPa; and n is the strain hardening exponent of the material.

With the averaged flow stress, the averaged compressive force can be derived as

$$F_{\text{ave}} = \sigma_c W L_c \tag{2}$$

where W represents the strip width; L_c is the contact length in radians and can be approximated to $\sqrt{R_0(H_i - h_i)}$ as the roll bite angle γ is a small number. Therefore, the load torque exerted on each work roll is approximated by

$$T_{\text{load}} = 0.5 L_c \times F_{\text{ave}}. \tag{3}$$

Consequently, the miling stand and the work rolls are elastically deformed under the compressive force and the following equation holds [25]:

$$h_i = S + F_{\text{ave}}/K \tag{4}$$

where S is the unloaded work roll gap and K is the equivalent mill stand stiffness.

Note that the roll-bite area is a bridge that connects the vertical movement and horizontal movement through the conservation of mass. Assume the width of the plate remains unchanged, the plate entry speed V_i can be obtained as

$$V_i = v_i \frac{h_i}{H_i}. \tag{5}$$

The exit speed v_i is determined by the rotational work rolls with a slip s and is given as

$$v_i = \omega_m R_0 (1+s) \tag{6}$$

where R_0 and ω_m are the radius and the angular speed of the work roll, respectively.

In addition, two delays exist throughout the thickness propagation, i.e., transport delay and measuring delay. The former refers to the time period that takes for a piece of strip to travel between two adjacent exit points, the latter is caused by the distance between the thickness gauge and its corresponding exit point. The transport delay τ_i and measuring delay δ_i can be approximated by

$$\tau_i = \frac{D}{V_i}, \quad \delta_i = \frac{d}{v_i} \tag{7}$$

where D represents the interstage distance and d is the distance that the thickness gauge is away from the exit point. Consider the case that the plate is being transported from Stage 3 to Stage 4 as an example. It takes a measuring delay δ_3 for the thickness sensor being placed in Stage 3 to obtain the actual output thickness of Stage 3 h_3. Thus, the relation of the measured thickness output h_3^{mea} and the actual thickness h_3 is given as $h_3(t) = h_3^{\text{mea}}(t - \delta_3)$. Meanwhile, it takes a transport delay of τ_4 for the plate with thickness h_3 to arrive at Stage 4. Therefore, the input thickness of Stage 4 H_4 is obtained as $h_3(t + \tau_4)$. In this way, with measured thickness output h_i^{mea}, we can derive the actual thickness output h_i of Stage i and the input thickness H_{i+1} of Stage $i+1$.

B. Modeling of the Rolling System

The rolling system plays the role of driving the work roll rotating at a target speed. As shown in Fig. 3, an induction

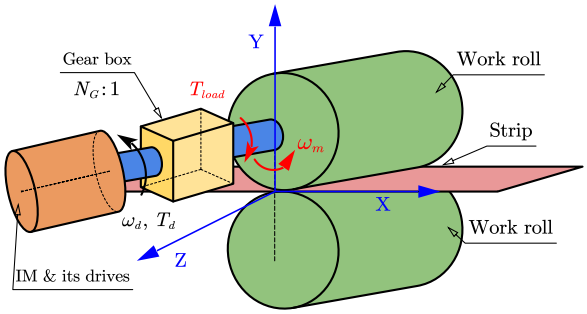

Fig. 3. Rolling system of the ith mill stage.

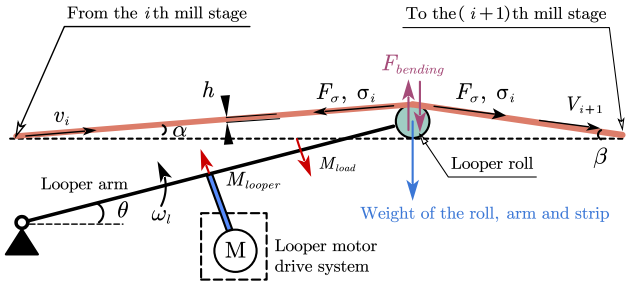

Fig. 4. Looper system between ith and $i+1$th stage.

machine and its drive interact with the work roll through a gearbox and transmission shafts.

The speed dynamic of the machine can be derived as

$$\frac{J_d}{n_p} N_G \frac{\mathrm{d}\omega_m}{\mathrm{d}t} = T_d - \frac{T_{\text{load}}}{N_G}. \tag{8}$$

where n_p and ω_m are the number of pole pairs and the angular speed of the IM, respectively; J_d is the total inertia of the motor and its transmission parts; N_G is the ratio of the gear reducer; and T_d is the electromagnetic torque generated by IM.

The derivation of T_d starts with the three-phase voltage and flux linkage equations shown as follows:

$$\boldsymbol{U} = \boldsymbol{R}\boldsymbol{i} + \frac{\mathrm{d}\boldsymbol{\Phi}}{\mathrm{d}t}, \boldsymbol{\Phi} = \boldsymbol{L}_{\text{in}}\boldsymbol{i} \tag{9}$$

with

$$\boldsymbol{L}_{\text{in}} = \begin{bmatrix} L_{AA} & L_{AB} & L_{AC} & L_{Aa} & L_{Ab} & L_{Ac} \\ L_{BA} & L_{BB} & L_{BC} & L_{Ba} & L_{Bb} & L_{Bc} \\ L_{CA} & L_{CB} & L_{CC} & L_{Ca} & L_{Cb} & L_{Cc} \\ L_{aA} & L_{aB} & L_{aC} & L_{aa} & L_{ab} & L_{ac} \\ L_{bA} & L_{bB} & L_{bC} & L_{ba} & L_{bb} & L_{bc} \\ L_{cA} & L_{cB} & L_{cC} & L_{ca} & L_{cb} & L_{cc} \end{bmatrix}$$

where capital letters in the subscript denote stator variables and small letters for rotor variables; variables $\boldsymbol{U}$, $\boldsymbol{i}$, $\boldsymbol{R}$, $\boldsymbol{\Phi}$ are terminal voltage, phase currents, winding resistance, and fluxlinkage, respectively, and specified as $\boldsymbol{R} = \text{diag}[R_s, R_s, R_s, R_r, R_r, R_r]$; $\boldsymbol{\Phi} = [\Phi_A, \Phi_B, \Phi_C, \Phi_a, \Phi_b, \Phi_c]^T$, $\boldsymbol{U} = [U_A, U_B, U_C, U_a, U_b, U_c]^T$, $\boldsymbol{i} = [i_A, i_B, i_C, i_a, i_b, i_c]^T$; $\boldsymbol{L_{in}}$ is the inductance matrix including self inductance of the stator and rotor, mutual inductance in the stator winding and rotors, and the mutual inductance of the stator and rotor.

To simplify the analysis and facilitate the controller design, the IM model (9) is represented in a static two-phase reference frame using Clarke transformation. With necessary derivation and combing (8), the dynamics of the IM are given as follows:

$$\begin{cases} \frac{\mathrm{d}w_m}{\mathrm{d}t} = \frac{n_p}{J_d N_G}\left(T_d - \frac{T_{\text{load}}}{N_G}\right) \\ \frac{\mathrm{d}\phi_{s\alpha}}{\mathrm{d}t} = -R_s i_{s\alpha} + u_{s\alpha} \\ \frac{\mathrm{d}\phi_{s\beta}}{\mathrm{d}t} = -R_s i_{s\beta} + u_{s\beta} \\ \frac{\mathrm{d}i_{s\alpha}}{\mathrm{d}t} = \frac{\phi_{s_\alpha}}{\sigma L_s T_r} + \frac{\omega\phi_{s\beta}}{\sigma L_r} - R_t i_{s\alpha} - \omega i_{s\beta} + \frac{u_{s\alpha}}{\sigma L_s} \\ \frac{\mathrm{d}i_{s\beta}}{\mathrm{d}t} = \frac{\phi_{s_\beta}}{\sigma L_s T_r} - \frac{\omega\phi_{s\alpha}}{\sigma L_s} - R_t i_{s\beta} + \omega i_{s\alpha} + \frac{u_{s\beta}}{\sigma L_s} \end{cases} \tag{10}$$

where $R_t = \frac{R_s L_r + R_r L_s}{\sigma L_s L_r}$, $\sigma = 1 - L_m^2/(L_s L_r)$, $T_r = L_r/R_r$; $\phi_{s\alpha}$ and $\phi_{s\beta}$, $i_{s\alpha}$ and $i_{s\beta}$, $u_{s\alpha}$ and $u_{s\beta}$ are the stator flux linkage, stage currents, and stator voltage in $\alpha\beta$ reference frame, respectively; L_s, L_r, L_m are the stator inductance, rotor inductance, and mutual inductance in $\alpha\beta$ reference frame, respectively.

Then, the electromagnetic torque can be obtained as

$$T_d = n_p(i_{s\beta}\phi_{s_\alpha} - i_{s\alpha}\phi_{s\beta}) \tag{11}$$

C. Modeling of the Looper System

The looper system between the mill stages aims to form the interstage strip tension by adjusting the looper arm's height. As shown in Fig. 4, the looper system between ith and $(i+1)$th mill stage includes a looper arm, a looper roll, and a mechanism to provide a moment of force on the arm. The dynamics of the looper angular speed is described as

$$J\frac{\mathrm{d}\omega_l}{\mathrm{d}t} = M_{\text{looper}} - M_{\text{load}} \tag{12}$$

where J is the total inertia of the looper mechanism; ω_l represents the angular speed of the looper arm; M_{looper} and M_{looper} are the target moment and the load moment of the looper arm, respectively.

The load moment includes the moment generated by the weight of the looper roll, looper arm, and strip between stages, the bending force of the strip and strip's tension. The derivation of the load moment can be found in [26], which is a nonlinear function of the strip tension and looper angle θ denoted as $f(\theta, \sigma_i)$.

The tensile stress σ_i on the strip can be derived based on Hooke's Law as

$$\sigma_i = E\frac{L - L_0}{L_0}. \tag{13}$$

L_0, known as free strip length, is the total strip length between stages when the looper does not apply a force on the strip. It is only determined by the entry and exit velocity of the strip expressed as

$$\frac{\mathrm{d}L_0}{\mathrm{d}t} = v_i - V_{i+1}. \tag{14}$$

When the looper applies a moment of force on the strip and thus leads to a tensile deformation of the strip. The total length of the stored strip between stages now becomes L. The dynamic

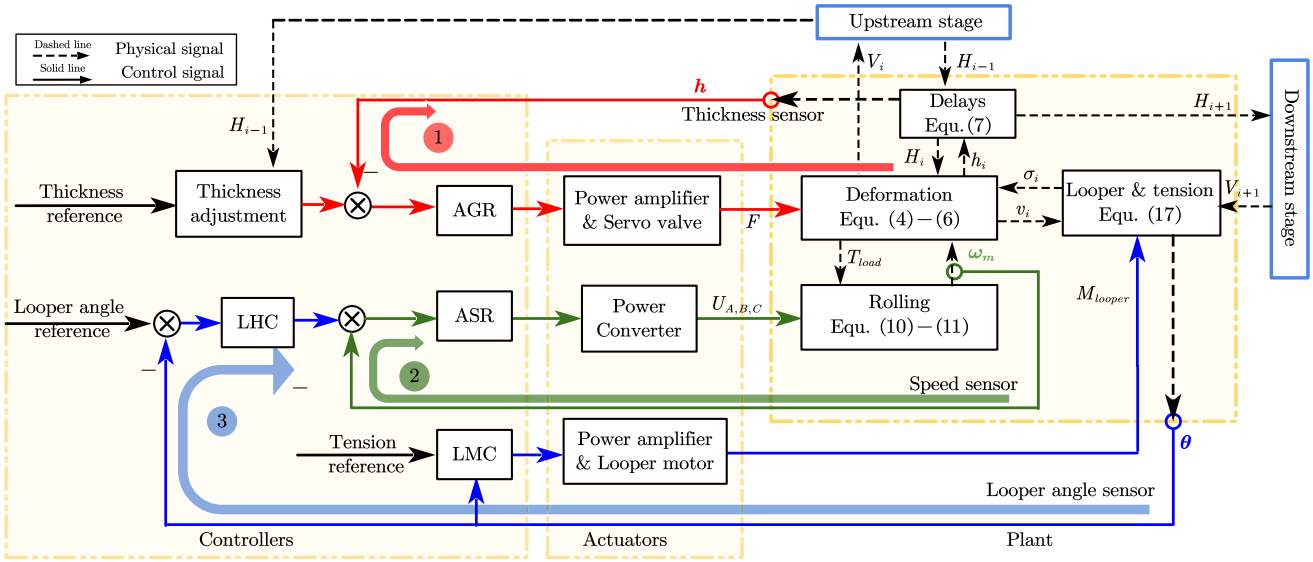

Fig. 5. Control diagram of a single-stage rolling mill system.

of the total length L is derived as

$$\frac{\mathrm{d}L}{\mathrm{d}t} = \frac{\mathrm{d}L}{\mathrm{d}\theta}\frac{\mathrm{d}\theta}{\mathrm{d}t}. \tag{15}$$

Combining (13), (14), and (15), the dynamics of the strip tension can be derived as

$$\frac{\mathrm{d}\sigma_i}{\mathrm{d}t} = E\frac{\mathrm{d}(L/L_0)}{\mathrm{d}t} \approx \frac{E}{L}\left(\frac{\mathrm{d}L}{\mathrm{d}\theta}\frac{\mathrm{d}\theta}{\mathrm{d}t} - v_i + V_{i+1}\right). \tag{16}$$

Therefore, the looper system can be modeled as

$$\begin{cases} \frac{\mathrm{d}\theta}{\mathrm{d}t} = w_l \\ \frac{\mathrm{d}w_l}{\mathrm{d}t} = \frac{1}{J}(M_{\text{looper}} - f(\theta, \sigma_i)) \\ \frac{\mathrm{d}\sigma_i}{\mathrm{d}t} = \frac{E}{L}(\frac{\mathrm{d}L}{\mathrm{d}\theta}\frac{\mathrm{d}\theta}{\mathrm{d}t} - v_i + V_{i+1}). \end{cases} \tag{17}$$

D. Controllers in the Multistage Rolling Mill System

The control diagram of a single-stage rolling mill system is shown in Fig. 5. The thickness control loop marked with red arrows regulates the displacement of the hydraulic valve at the vertical level by the automatic gauge regulator (AGR). The looper and tension control loop marked with blue arrows adjusts the strip tension using the looper height regulator (LHR) and looper moment calculation. The inner speed control loop marked with green arrows realizes the horizontal movement of the strip by the ASR. All the controllers adopt the traditional proportional–integral (PI) controllers. Afterward, a multistage system can be created by applying the transport delays and measuring delays to the exit thickness of each single stage.

III. Attack Modeling

In this article, we analyze the data integrity attacks launched at the speed sensor, looper angle sensor and thickness sensor in a multistage rolling mill system. Based on previous studies on the MITM attack model in [10], integrity attack model in [27], and fault models in [13], [14], [15], [16], [17], [18], the sensor integrity attack models in this article are designed as multiplicative attacks and additive attacks.

As the name suggests, the multiplicative attack in a system is to change the sensor's signal proportionally by

$$y^{\text{atk}}(t) = \begin{cases} \alpha y(t) & t_0 < t < t_0 + T_{\text{atk}} \\ y(t) & \text{else} \end{cases} \tag{18}$$

where y^{atk} and y are the modified sensor signal and actual sensor signal, respectively; t_0 is the attack start time; T_{atk} is the time period under attacks; α is the multiplicative factor. Differentiated by factor α, three types of multiplicative attacks are proposed in this article, they are

1) *Type* I: enlarging the signal with $\alpha > 1$;
2) *Type* II: minifying the signal with $0 < \alpha < 1$;
3) *Type* III: modifying the signal with a time-varying factor $\alpha = 1 + N(0, \sigma^2)$, where $N(0, \sigma^2)$ is a zero-mean normal distribution signal with a standard deviation σ.

The additive attack is designed to change the sensor's feedback by adding an extra signal to it described as

$$y^{\text{atk}}(t) = \begin{cases} y(t) + \beta & t_0 < t < t_0 + T_{\text{atk}} \\ y(t) & \text{else} \end{cases} \tag{19}$$

where β is modeled as an oscillating decaying signal in *Type* IV, and a pulse signal in *Type* V. Specifically, they are

1) *Type* IV: $\beta = Ae^{-t/\tau}\sin(2\pi ft)$, an oscillating decaying signal vibrating at frequency f with an amplitude of A and a decaying constant τ;
2) *Type* V: $\beta = \mathcal{F}(t)$, a pulse signal of a certain frequency f, duty cycle D and amplitude A.

IV. Evaluation Metrics

In this section, the device-level and system-level evaluation metrics are proposed for a multistage rolling mill system. In each stage, we focus on the *milling quality*, *operation safety*, and *milling productivity* by evaluating the transient performance

TABLE I
PART OF THE PARAMETERS IN SIMULATION

Description	Parameter	Value
Nominal thickness	h^{ref}	0.01 m
Stage 1 thickness reference	h_1^{ref}	0.009 m
Stage 2 thickness reference	h_2^{ref}	0.008 m
Stage 3 thickness reference	h_3^{ref}	0.007 m
Stage 4 thickness reference	h_4^{ref}	0.006 m
Stage 5 thickness reference	$h_{\text{exit}}^{\text{ref}}$	0.005 m
Exit plate velocity	$v_{\text{exit}}^{\text{ref}}$	1 m/s
Gear ratio	N_G	20
Nominal looper angle	θ^{ref}	0.5°
Roll slip	s	0.01
Nominal strip tension	σ^{ref}	1.7×10^{10} N/m

using device-level metrics K_1–K_5. Then, we define the index S_{imp}^i to evaluate the vulnerability of the ith stage and S_{overall} to include the impact on all stages caused by the attack. The definition of K_1 to K_5 within a sliding window (denoted as T_{sw}) is given as follows, wherein the lower case letter i represents the stage number and x for the metric number.

A. Manufacturing Quality

Traditionally, the crown and the flatness are two important quality parameters for the metal strip [28]. The crown is defined as the thickness difference between the center and the edge of the strip along the axial direction (*Z*-axis in Fig. 3) [29]. In this article, we simplify the deformation process by treating the thickness of the strip along the axial direction as the same thus the crown is zero. Instead, we focus on the thickness tracking performance of each stage to reflect the manufacturing quality. The thickness tracking metric is defined as

$$K_1^i(t) = (h_i^{ref}(t) - \bar{h}_i(t))/h_i^{\text{ref}}(t) \tag{20}$$

where $\bar{h}_i$ and h_i^{ref} are the averaged exit thickness and target thickness of the ith stage within the sidling windo, respectivelyw.

The flatness refers to the degree to which the strip is planar without being exerted by an external force. Usually, it is represented by the ratio of the wave height and wave pitch on the strip. In the article, we use the ripple of the forward tensile force of the strip to approach the bad flatness [28], [30]. The tensile force is obtained by $F_i = \sigma_i(t)h(t)W$, thus K_2 is given as

$$K_2^i(t) = (F_i^{\max} - F_i^{\min})/F_i^{\text{ave}}. \tag{21}$$

where $F_i^{\max}$, $F_i^{\min}$, and F_i^{ave} are the maximum, minimum, and averaged tensile force of the strip.

B. Operation Safety

The operation safety in the rolling mill system is evaluated by the induction machine's torque ripples and speed ripples in each stage. The metric K_3 for torque ripple and K_4 for speed ripple are defined as

$$K_3^i(t) = (T_i^{\max}(t) - T_i^{\min}(t))/T_i^{avae}(t) \tag{22}$$

$$K_4^i(t) = (\omega_{m-i}^{\max}(t) - \omega_{m-i}^{\min}(t))/\omega_{m-i}^{\text{ave}}(t). \tag{23}$$

where in the sliding window $T_i^{\max}$, $T_i^{\min}$, and T_i^{ave} are the maximum, minimum torque, and averaged torque; $\omega_{m-i}^{\max}$, $\omega_{m-i}^{\min}$ and $\omega_{m-i}^{\text{ave}}$ are the maximum, minimum and averaged speed, respectively.

The reason for choosing the two terms is their bridging of more than two control systems and fast-changing features. Measured in the inner loop of the tension control loop, the metric K_4 has the advantage of indicating possible attacks occurred in both rolling system and looper system. Meanwhile, the metric K_3 can reflect the hydraulic valve's piston displacement in the thickness control system.

C. Milling Productivity

The milling productivity of the multistage rolling mill system is reflected by a Boolean value that describes if the thickness of the strip at the exit stage meets the demand after each sensor integrity attack. The metric is given as

$$K_5 = \begin{cases} 0 & (1-\gamma)h_{\text{exit}}^{\text{ref}} < h_{\text{exit}}(t) < (1+\gamma)h_{\text{exit}}^{\text{ref}} \\ 1 & \text{else} \end{cases} \tag{24}$$

where γ is the thickness tolerance and it is set as 3% in this article.

D. Overall Impact

As presented above, K_1 to K_5 are used to capture the performance of the subsystems in each rolling mill stage. In addition, we propose an index S_{imp}^x to evaluate the overall system performance in Stage i by

$$S_{\text{imp}}^i = a(I_{K_1^i} + I_{K_2^i}) + b(I_{K_3^i} + I_{K_4^i}) + cK_5^i \tag{25}$$

where a, b, and c are the weight factors for the *milling quality*, *operation safety*, and *milling productivity*, respectively; $I_{K_x^i}$ is the summation of impact caused by each integrity attack by

$$I_{K_x^i} = \sum \left(1 - e^{-\left|I_{\text{atk}}^{K_i} + I_{\text{beyond-atk}}^{K_i} - 2I_{\text{normal}}^{K_i}\right|/\Gamma}\right)$$

where

$$I_{\text{atk}}^{K_i} = \sqrt{\frac{1}{T_{\text{sw}}}\int_{t_0}^{t_0+T_{\text{sw}}} (K_x^i(t))^2 \mathrm{d}t}$$

$$I_{\text{beyond-atk}}^{K_i} = \sqrt{\frac{1}{T_{\text{sw}}}\int_{t_0+T_{\text{sw}}}^{t_0+2T_{\text{sw}}} (K_x^i(t))^2 \mathrm{d}t}$$

$$I_{\text{normal}}^{K_i} = \sqrt{\frac{1}{T_{\text{sw}}}\int_{t_0-T_{\text{sw}}}^{t_0} (K_x^i(t))^2 \mathrm{d}t}$$

Γ is set as 0.25/5 for each stage assuming the maximum ripple during attack period is 50%.

The comprehensive impact index S_{comp} for the multistage system then is obtained by summing up the impact in each stage with

$$S_{\text{comp}} = \sum S_{\text{imp}}^i. \tag{26}$$

V. SIMULATION RESULTS AND IMPACT ANALYSIS

To evaluate the system performance and effectiveness of the proposed metrics, we build a five-stage rolling mill system

TABLE II
THICKNESS SENSOR ATTACK MODELING AND CASE DEFINITION

Case	Attack type	Attack strength
F1	Type I	$\alpha = 1.3$
F2	Type II	$\alpha = 0.6$
F3	Type III	$\sigma^2 = 2.5 \times 10^{-3}$, $T_s = 0.1s$
F4	Type IV	$A = 0.2$, $f = 200$, $\tau = 0.1$
F5	Type V	$A = 1 \times 10^{-3}$, $f = 10$, $D = 40\%$

in MATLAB/Simulink. The five-stage rolling mill system is expanded from a three-stage rolling mill benchmark in [31] after adapting the mathematical models, adding disturbance to the thickness, and adding the proposed sensor attacks. The five-stage rolling mill system is designed to realize thickness reduction for the strip from 10 to 5 mm. The first stage, numbered Stage 1 in this article, is the stage that the raw plate is inserted into, while the last stage, numbered Stage 5, is the stage, where the plate is about to be reduced to the thinnest according to the thickness reduction goal. The sampling period is set to 0.001 s. Some key parameters used in the simulation are listed in Table I.

Sections V-A, V-B, and V-C will first present the device-level impact analysis with metrics K_1 to K_5 under single sensor attack. Based on that, the system-level impact analysis is presented in Section V-D to assess the vulnerability of the whole system under a single sensor attack. Then Section V-E explores the vulnerability assessment under combined sensor attacks. Finally, the main achievements and contributions are summarized in Section V-F.

A. Thickness Sensor Attack

To study how the attacked thickness gauge impacts the rolling and milling process as a whole, we simulate a thickness sensor attack that targets the thickness gauge in Stage 3. The attack models and case definitions are specified in Table II. In each case, the time period under thickness sensor attack remains 0.25 s.

Based on the proposed evaluation metrics in Section IV, the device-level and system-level indices for cases F1–F5 are obtained by applying (20)–(26). Fig. 6(a) depicts the system response when the thickness gauge signal in Stage 3 is enlarged by 1.3 times. As described by K_1, the strip thickness in Stage 3 causes an overshoot during the attack period because of the maliciously increased thickness feedback. In response to the enlarged feedback signal, the AGR in Stage 3 decreases the control input. Therefore, an undershoot of actual thickness tracking is observed when the attack ends. The plate with decreased thickness then travels to Stage 4 after a certain interstage transport delay, thus leading to an increased regulated thickness set point for Stage 4. Due to the transport delay τ_4, the thickness tracking in stage 4 first presents an undershoot and then an overshoot as shown in the figure. With another transport delay, the abnormal plate arrives at Stage 5 and repeats similar thickness reduction process as in Stage 4. As for the upstream stages with regard to Stage 3, the thickness reduction process in Stage 1 and Stage 2 are not impacted because of the thickness propagation order.

Based on the thickness performance described by metric K_1, we can predict the compressive force performance, which

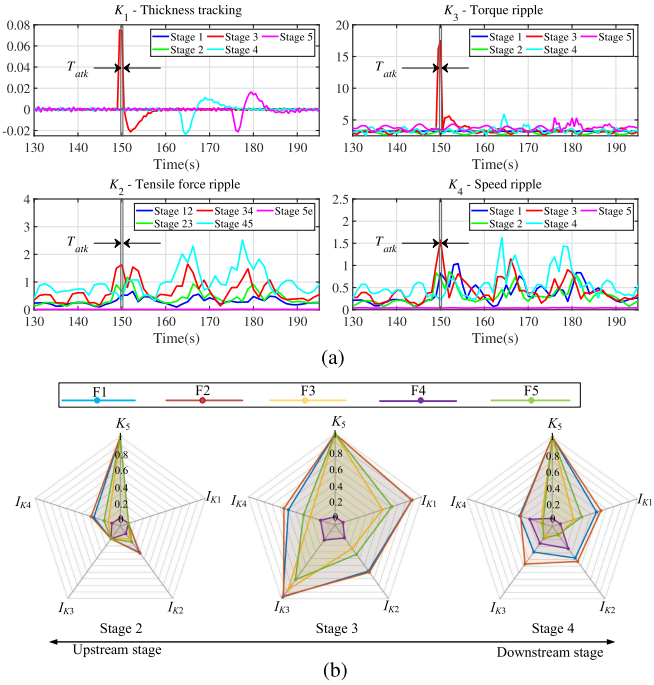

Fig. 6. Evaluation results for the thickness sensor in Stage 3 under integrity attacks. (a) Type I attack, $y_{\text{atk}}(t) = 1.3y(t), t \in [t_0, t_0 + T_{\text{atk}}]$. (b) Radar representation of the proposed indices.

is directly influenced by the valve's piston displacement. The enlarged thickness feedback during the attack period will lead to a higher demand on the compressive force while the decreased thickness feedback gives rise to lower compressive force demands. Therefore, the load torque generated by the compressive force in each stage will be increased or decreased proportionally, which matches the result of metric K_3 where significant torque ripples of the IM in Stage 3 are captured during the attack period and minor torque ripples of the IMs in Stages 4 and 5 appear beyond the attack period.

The thickness performance also directly influences the roll speed through mass conservation stated in Section II. As indicated by the metric K_4 in Fig. 6(a), the thickness-tracking-compromised stage witnesses significant speed ripples in its own stage and also in the rest stages at the same time. This is because the required-entry speed of one stage is also the exit speed of its upstream stage. In this way, speed ripples K_4 in each stage occur synchronously when the thickness tracking performance is compromised. In addition, the tensile force on the strip is impacted by the exit speed and entry speed between stages. Therefore, the metric K_2 for tensile force ripples has a similar pattern as the metric K_4. It should be noted that the speed performance of the last stage and the tensile force between the last stage and the coiler are different from the upstream stages because Stage 5 is bridged to a coiler which is controlled by a constant rotational speed of 1 m/s. This explains why K_2 between Stage 5 and the coiler, and K_4 for the last stage remain unchanged with nearly zero fluctuations.

For the purpose of conciseness, the detailed representation like in Fig. 6(a) for the cases F2–F5 is not provided here. Because

TABLE III
SPEED SENSOR ATTACK MODELING AND CASE DEFINITION

Case	Attack type	Attack strength
F6	Type I	$\alpha = 1.3$
F7	Type II	$\alpha = 0.7$
F8	Type III	$\sigma^2 = 1 \times 10^{-4}$, $T_s = 0.01s$
F9	Type IV	$A = 0.2$, $f = 200$, $\tau = 0.1$
F10	Type V	$A = 200$, $f = 10$, $D = 75\%$

Fig. 6(a) is sufficient as an example to validate the effectiveness of presenting the consequences of thickness sensor attacks and quantifying the impact caused by the thickness sensor attack using metrics K_1 to K_5. Instead, we use the radar plots in Fig. 6(b) to visualize the statistical results of indices under attack scenarios F1–F5. The calculated indices I_{K_1} to I_{K_4} and K_5 range from 0 to 1, with 0 indicating zero impact and 1 for severe impact under single sensor attack. Equivalently, the covered area of the five indices symbolizes the impact intensity caused by the thickness sensor attack. From Fig. 6(b), we can draw the conclusions as follows.

1) Except for the Type IV attack (the oscillating decaying signal), the other four specifically designed types of attacks listed in Table II can cause a failure in thickness reduction while keeping the multistage system stable.
2) The attacked stage is being impacted the most; downstream stages rather than upstream stages with regard to the attacked stage tend to be impacted more; the closer to the attacked stage, the more significant impact in terms of torque ripples, speed ripples, tensile force ripples, and the thickness tracking performance.

B. Speed Sensor Attack

To evaluate the impact of the proposed attacks, we launch integrity attacks on the speed sensor in Stage 3 as defined in Table III. In each case, the time period under speed sensor attack is set as 0.25 s. The evaluation results of cases F6–F10 based on the proposed indices are presented in Fig. 7.

As shown in Fig. 7(a), the multistage system is under the Type II speed sensor attack. The metric K_4 indicates that the IM in Stage 3 achieves significant speed ripples of around 50%, and IMs in the upstream stages, i.e., Stage 2 and Stage 1, have minor speed ripples, while motors of the downstream stages are not impacted when the speed feedback in Stage 3 is minified by 70%. The metric K_2 shows that the strip between Stage 3 and 4 has the greatest tensile force ripples, followed by the strip between Stage 2 and Stage 3, then the strip between Stage 1 and Stage 2. As for the metric K_3, only in Stage 3 are the significant torque ripples observed. The thickness tracking is not impacted under the speed sensor attack by looking at the metric K_1.

The scenario can be explained with the help of the control diagram shown in Fig. 5. When the speed feedback in Stage 3 decreases during the attack period, the control input of the ASR in Stage 3 will be increased correspondingly and then leads to a sudden change in three-phase currents of the IM in Stage 3. Therefore, we observe a surge both in K_4 and K_3 of Stage 3. Followed by the increased exit speed of Stage 3, the strip length

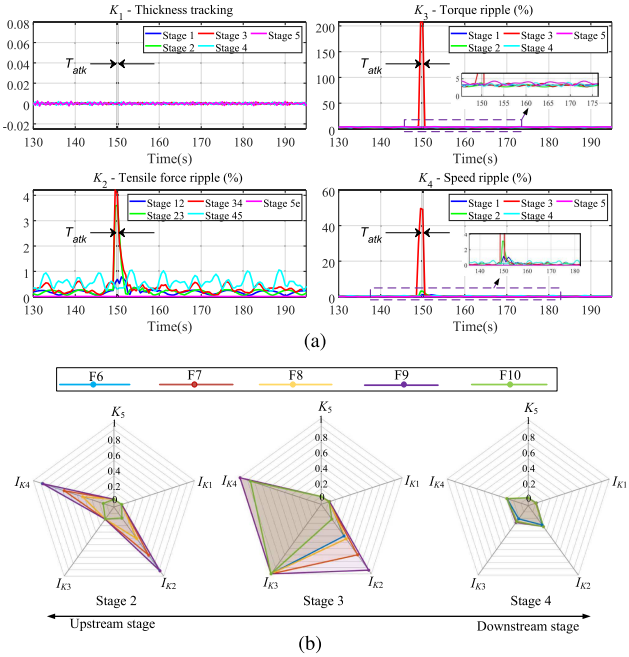

Fig. 7. Evaluation results for the speed sensor in Stage 3 under integrity attacks. (a) Type II attack, $y_{\text{atk}}(t) = 0.7y(t), t \in [t_0, t_0 + T_{\text{atk}}]$. (b) Radar representation of the proposed indices.

accumulated between Stage 3 and 4 is increased and thus the strip tension between the two stages experiences fluctuations, which is reflected by the metric K_2 of Stage 3. Moreover, the speed references for the IMs in the upstream stages are adjusted with the adjusted strip length accumulation based on the mass conservation, therefore, only speed ripples but no torque ripples exist in the upstream stages. While for the downstream stages, the exit speeds are not impacted so that the strip accumulations are not impacted. As a result, there are no adjustments in the ASRs and LHRs of the downstream stages during the steady state and thus no speed ripples or torque ripples. As for the thickness tracking, it is apparent that the thickness of the strip can only be impacted unless the variables at the vertical level, such as the thickness feedback, the compressive force, and the mill stand stiffness are impacted.

Besides the evaluation results presented above, we also adopt the radar charts to visualize the statistical results of the calculated indices I_{K_1} to I_{K_4} and K_5 under speed sensor attack cases F6–F10. Conclusions can be drawn from Fig. 7(b) as follows.

1) The radar representation for indices under speed sensor attack has distinctive features compared to that under thickness sensor attack.
2) The speed sensor attacks do not impact thickness tracking at any stage.
3) The attacked stage is being impacted the most; upstream stages rather than downstream stages with regard to the attack stage are impacted; the closer to the attacked stage from the upstream stage, the more significant impact in terms of torque ripples, speed ripples, and tensile force ripples.

TABLE IV
LOOPER ANGLE SENSOR ATTACK MODELING AND CASE DEFINITION

Case	Attack type	Attack strength
F11	Type I	$\alpha = 1.00025$
F12	Type II	$\alpha = 0.998$
F13	Type III	$\sigma^2 = 1 \times 10^{-8}$, $T_s = 0.1s$
F14	Type IV	$A = 1.25 \times 10^{-4}$, $f = 200$, $\tau = 0.1$
F15	Type V	$A = 5 \times 10^{-5}$, $f = 10$, $D = 75\%$

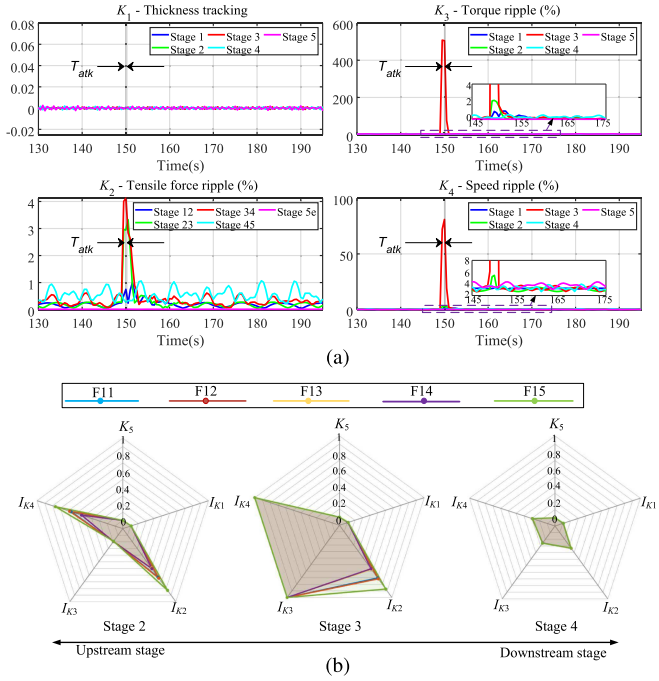

Fig. 8. Evaluation results for the looper angle sensor between stage 3 and stage 4 under integrity attacks. (a) Type I attack, $y_{\text{atk}}(t) = 1.00025y(t), t \in [t_0, t_0 + T_{\text{atk}}]$. (b) Radar representation of the proposed indices.

C. Looper Angle Sensor Attack

Similar to the process of evaluating the impact under thickness sensor attack and speed sensor attack, in this section, we present the evaluation results using proposed indices under looper angle attacks defined in Table IV. The attacked looper angle sensor is in Stage 3 in cases F11–F15. In each case, the time period under the looper angle sensor attack is set as 0.25 s.

By comparing Tables IV to III and Table II, it can be found that the allowed attack strength of the looper angle sensor that causes impacts while keeping the system stable is relatively weak compared to that of the speed sensor and thickness gauge. This is because as the outer loop of the speed control loop, the looper and tension control loop is more sensitive and stringent to the looper angle attacks.

Moreover, the impacted looper angle signal will impact the inner speed control loop, thus generating a similar system response compared to the cases under speed sensor attack. This is why the system response shown in Fig. 8(a) is similar to the results in Fig. 7(a). Therefore, for the sake of conciseness, the illustration of how the indices K_1 - K_5 reflect the impacts is neglected in the section.

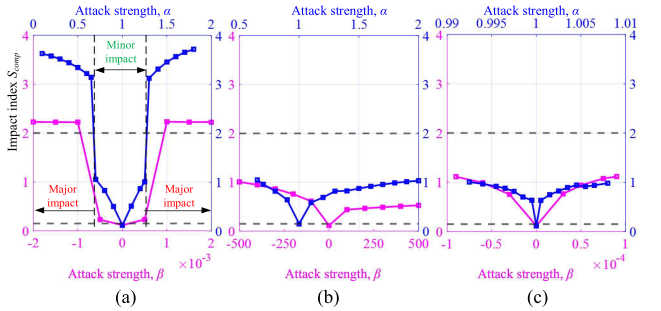

Fig. 9. Vulnerability assessment of one sensor being attacked in stage 3. (a) Thickness sensor attack. (b) Speed sensor attack. (c) Looper angle sensor attack.

The radar chart that presents the calculated indices in attack cases F11–F15 is shown in Fig. 8(b). The conclusions drawn from Fig. 8(b) are almost the same as those under speed sensor attacks except that the torque ripples in all upstream stages with regard to the attacked stage are impacted under looper angle sensor attack.

D. System-Level Assessment Under Single Sensor Attack

In addition to the device-level analysis for sensor integrity attack scenarios in Stage 3 shown above, we also assess the vulnerability of the multistage system under sensor attack from the system-level perspective. In this section, only one sensor in Stage 3 is attacked in each case in order to derive the general conclusion for system-level vulnerability assessment.

In order to value the mill productivity K_5 more and distinguish the thickness sensor attack from the speed sensor and looper angle sensor, the weight factors in (25) are set as $a = 0.15, b = 0.15, c = 0.4$. In this way, the minimum comprehensive impact index S_{comp} exceeds 2 if one thickness tracking failure occurs at the exit stage under thickness sensor attacks, thus the attack is categorized as causing major impacts on the overall system. While for the cases where the thickness tracking at the exit stage meets the demands and S_{comp} exceeds 0.1, we categorize the attacks as causing minor impacts.

Using evaluation metrics proposed in Section IV and designed weights, the quantitative vulnerability assessment results under the multiplicative attack and additive attack of different attack strengths launched in Stage 3 are shown in Fig. 9. From Fig. 9, we observe that 1) only under thickness sensor attacks of relatively strong strength can the attack cause major impacts on the overall system; 2) multiplicative thickness sensor attacks cause more significant impact compared to additive thickness sensor attacks; 3) attacks launched to the speed sensor attack and looper angle have little impact on the milling productivity but more impact on the operation safety and manufacturing quality.

The above observations match the analysis from the perspective of control theory. As known to all, the PI controller in each subsystem has the capability of correcting the tracking error caused by the disturbance from sensor feedback. Within certain boundaries, the system remains stable and is able to recover from deviations caused by the sensor attack. For this reason,

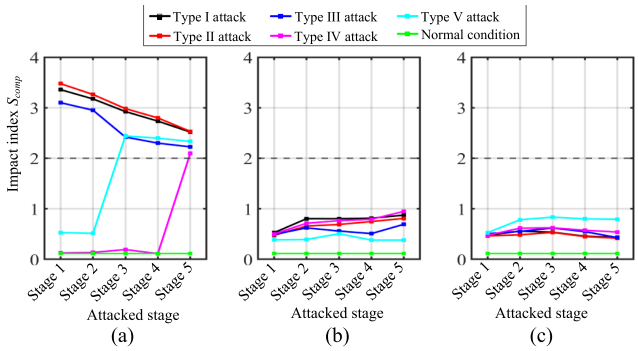

Fig. 10. Overall impact of one sensor being attacked at different stages. (a) Thickness sensor. (b) Speed sensor. (c) Looper angle sensor.

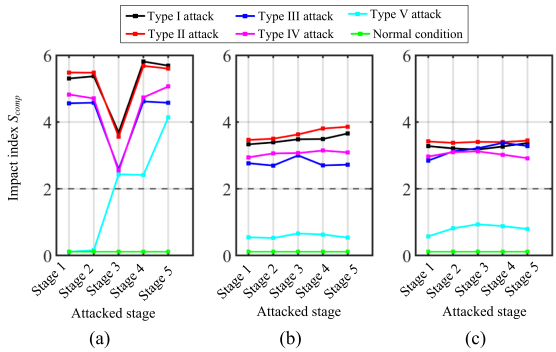

Fig. 11. Overall impact of combined sensor attack with one sensor assigned as the thickness sensor of Stage 3, and the other sensor assigned as (a) thickness sensor, (b) speed sensor, (c) looper angle sensor

observation 1) holds and the conclusion also applies to the speed sensor attack scenarios and looper angle sensor attack scenarios. As for observation 2), this happens because the integral term in the feedforward path of the control loop can eliminate the steady-state error when there is an external disturbance like an additive attack after the PI controller. The steady-state error elimination effect is especially significant when attacking the speed sensor in the rolling mill system with additive attacks as the speed control loop is the inner control loop of the looper angle regulation loop. This is why the maximum attack strength for the speed sensor is much larger than that for the looper angle sensor as shown in Fig. 9. For observation 3), this is true because of the thickness propagation between stages. The attacked thickness control loop not only affects the speed control loop and the looper angle control loop that is coupling within the stage, but also impacts the three subsystems next to it as long as there is thickness propagation. Therefore, the proposed system-level indices are effective in understanding and reflecting the interactions of subsystems in the multistage rolling mill system, and quantifying the impacts caused by each sensor integrity attack.

In addition to the sensor attacks launched in Stage 3, Fig. 10 replenishes the S_{comp} data with the attacks of the same strength launched in other stages for each sensor. The attack strength settings adopt the parameters in Tables II–IV. It can be seen from Fig. 10 that

1) for the thickness sensor suffering from relatively strong attack strength (Type I, II, and III), the further it is away from the exit stage, the more severe the overall impact the attack can cause;
2) for the thickness sensor under Type IV and V attack (additive attacks), it may not lead to milling productivity failure if it is located further enough from the exit stage;
3) for the speed sensor and looper angle sensor in each stage, the integrity attacks do not impact the milling productivity. The two sensors under different attack types have close comprehensive impacts when targeting different stages.

Apparently, the above impact analysis based on the quantitative evaluation results further demonstrates the conclusion drawn from Fig. 9 and shows the effectiveness of the proposed vulnerability assessment framework and metric index.

E. System-Level Assessment Under Combined Sensor Attack

To further validate the proposed assessment method, more complicated scenarios such as the combined sensor integrity attacks are considered in this section. Without losing generosity, two sensors are attacked simultaneously in the five-stage rolling mill. To narrow down the scope of possible combinations, one of the attacked sensors is assigned as the thickness sensor of Stage 3, then the other sensor can be chosen as the thickness sensor, speed sensor, and looper angle sensor from one of the five stages. The integrity attack type for the two sensors in the combined sensor attack case is the same and adopts the parameters listed in Tables II, III, and IV. Weight factors are the same as the settings in Section V-D.

The system-level metrics obtained by the proposed method under the combined sensor integrity attacks are presented in Fig. 11. It is notable that the overall impact S_{comp} exceeds 4 when two thickness sensor attacks (Type I, Type II, Type III, and Type IV attack) are launched at different stages simultaneously as shown in Fig. 11(a). For the sensor integrity attack combination like a thickness sensor combined with a speed sensor or a thickness sensor combined with a looper angle sensor, the overall impact index S_{comp} exceeds 2 under Type I, Type II, Type III, and Type IV integrity attacks because the impact caused by the thickness sensor attack of Stage 3 is dominant compared to that caused by the speed sensor attack and looper angle attack. Therefore, the proposed vulnerability assessment method is still effective for the combined sensor attack cases in terms of distinguishing the thickness sensor attack from the speed sensor attack and the looper angle sensor attack; and indicating if there is more than one thickness sensor attack launched at the system.

F. Main Achievements of the Proposed Methodology

Based on the analysis presented in the previous sections, the effectiveness of the proposed vulnerability assessment method is validated through simulations and calculations. First of all, the vulnerability assessment work focusing on manufacturing quality, operation safety, and milling productivity is verified as a useful framework for manufacturers to monitor and assess the

multistage rolling mill system. Then, the device-level metrics K_1 - K_5, the calculated indices I_{K_1} to I_{K_4} and K_5 serve as great tools for the manufacturers and researchers to understand how each subsystem interacts with each other and responds when sensor integrity attack occurs. Those device-level indices together with the system-level indices S^i_{imp} and S_{comp} provide quantitative impact analysis for the integrated rolling mill system under different attacks.

VI. Conclusion

This article has presented the vulnerability assessment of a multistage on rolling mill system under thickness sensor attacks, speed sensor attacks, and looper angle sensor attacks. The vulnerability assessment in this article, including the multistage system modeling, attack modeling, and innovative evaluation metrics establishment provides general guidance for cyber-attack impact analysis using the device-level indices and system-level indices. The proposed device-level metrics K_1 to K_5 are effective in assessing working conditions in each subsystem in each stage in terms of the manufacturing quality, the operation safety, and the milling productivity; and the system-level index S_{comp} is effective in evaluating the comprehensive impact caused by the sensor attacks. The proposed metrics also distinguish the thickness sensor attack and nonthickness sensor attacks by using well-designed weight factors on the device-level indices. Therefore, the proposed evaluation methods show promise for attack detection and attack-oriented controller design in future work.

References

[1] Q. Bai, B. Jin, Y. Gao, and H. Zhang, "An online fault pre-warning system of the rolling mill screw-down device based on virtual instrument," *Sensors Transducers*, vol. 168, no. 4, pp. 1–7, 2014.

[2] R. M. Lee, M. J. Assante, and T. Conway, "German steel mill cyber attack," *Ind. Control Syst.*, vol. 30, no. 62, pp. 1–15, 2014.

[3] B. Yang, L. Guo, F. Li, J. Ye, and W. Song, "Vulnerability assessments of electric drive systems due to sensor data integrity attacks," *IEEE Trans. Ind. Informat.*, vol. 16, no. 5, pp. 3301–3310, May 2020.

[4] L. Guo, J. Ye, and L. Du, "Cyber-physical security of energy-efficient powertrain system in hybrid electric vehicles against sophisticated cyberattacks," *IEEE Trans. Transp. Electrific.*, vol. 7, no. 2, pp. 636–648, Jun. 2021.

[5] R. McMillan, "Siemens: Stuxnet worm hit industrial systems," Accessed on: Sep. 18, 2022. [Online]. Available: https://www.computerworld.com/article/2515570/siemens--stuxnet-worm-hit-industrial-systems.html

[6] A. Muir and J. Lopatto, "Final report on the august 14, 2003 blackout in the United States and Canada: Causes and recommendations," Apr. 2004. [Online]. Available: https://www.osti.gov/etdeweb/biblio/20461178

[7] I. Zografopoulos, J. Ospina, X. Liu, and C. Konstantinou, "Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies," *IEEE Access*, vol. 9, pp. 29775–29818, 2021.

[8] N. Tuptuk and S. Hailes, "Security of smart manufacturing systems," *J. Manuf. Syst.*, vol. 47, pp. 93–106, 2018.

[9] D. Wu et al., "Cybersecurity for digital manufacturing," *J. Manuf. Syst.*, vol. 48, pp. 3–12, 2018.

[10] M. M. R. Monjur, J. Heacock, R. Sun, and Q. Yu, "An attack analysis framework for Lorawan applied advanced manufacturing," in *Proc. IEEE Int. Symp. Technol. Homeland Secur.*, 2021, pp. 1–7.

[11] I. Kiss, B. Genge, and P. Haller, "A clustering-based approach to detect cyber attacks in process control systems," in *Proc. IEEE 13th Int. Conf. Ind. Informat.*, 2015, pp. 142–148.

[12] Y.-L. Huang, A. A. Cárdenas, S. Amin, Z.-S. Lin, H.-Y. Tsai, and S. Sastry, "Understanding the physical and economic consequences of attacks on control systems," *Int. J. Crit. Infrastructure Protection*, vol. 2, no. 3, pp. 73–83, 2009.

[13] M. Dong, C. Liu, and G. Li, "Robust fault diagnosis based on nonlinear model of hydraulic gauge control system on rolling mill," *IEEE Trans. Control Syst. Technol.*, vol. 18, no. 2, pp. 510–515, Mar. 2010.

[14] D.-W. Gu and F. W. Poon, "A robust fault-detection approach with application in a rolling-mill process," *IEEE Trans. Control Syst. Technol.*, vol. 11, no. 3, pp. 408–414, May 2003.

[15] F. W. Poon, "Observer based robust fault detection: Theory and rolling mill case study," University of Leicester (United Kingdom), 2000. [Online]. Available: https://api.semanticscholar.org/CorpusID:62999917

[16] L. Li and S. X. Ding, "Optimal detection schemes for multiplicative faults in uncertain systems with application to rolling mill processes," *IEEE Trans. Control Syst. Technol.*, vol. 28, no. 6, pp. 2432–2444, Nov. 2020.

[17] Y. Jiang, S. Yin, and O. Kaynak, "Optimized design of parity relation-based residual generator for fault detection: Data-driven approaches," *IEEE Trans. Ind. Informat.*, vol. 17, no. 2, pp. 1449–1458, Feb. 2021.

[18] H. Luo, K. Li, O. Kaynak, S. Yin, M. Huo, and H. Zhao, "A robust data-driven fault detection approach for rolling mills with unknown roll eccentricity," *IEEE Trans. Control Syst. Technol.*, vol. 28, no. 6, pp. 2641–2648, Nov. 2020.

[19] M. J. Hutchins, R. Bhinge, M. K. Micali, S. L. Robinson, J. W. Sutherland, and D. Dornfeld, "Framework for identifying cybersecurity risks in manufacturing," *Procedia Manuf.*, vol. 1, pp. 47–63, 2015.

[20] Z. DeSmit, A. E. Elhabashy, L. J. Wells, and J. A. Camelio, "Cyber-physical vulnerability assessment in manufacturing systems," *Procedia Manuf.*, vol. 5, pp. 1060–1074, 2016.

[21] Z. DeSmit, A. E. Elhabashy, L. J. Wells, and J. Camelio A, "An approach to cyber-physical vulnerability assessment for intelligent manufacturing systems," *J. Manuf. Syst.*, vol. 43, pp. 339–351, 2017.

[22] G. Guibing, Y. Wenhui, O. Wenchu, and T. Hao, "Vulnerability evaluation method applied to manufacturing systems," *Rel. Eng. Syst. Saf.*, vol. 180, pp. 255–265, 2018.

[23] G. Gao, J. Wang, W. Yue, and W. Ou, "Structural-vulnerability assessment of reconfigurable manufacturing system based on universal generating function," *Rel. Eng. Syst. Saf.*, vol. 203, 2020, Art. no. 107101.

[24] M. P. Groover, *Fundamentals of Modern Manufacturing: Materials, Processes, and Systems*. Hoboken, NJ, USA: Wiley, 2020.

[25] W. I. Breesam, K. A. Mohamad, and M. T. Rashid, "Simulation model of cold rolling mill," *Iraqi J. Elect. Electron. Eng.*, vol. 16, no. 1, pp. 1–6, 2020.

[26] S. K. Yildiz et al., "Dynamic modelling and simulation of a hot strip finishing mill," *Appl. Math. Modelling*, vol. 33, no. 7, pp. 3208–3225, 2009.

[27] T. Marcu, B. Köppen-Seliger, and R. Stücher, "Design of fault detection for a hydraulic looper using dynamic neural networks," *Control Eng. Pract.*, vol. 16, no. 2, pp. 192–213, 2008.

[28] D. Raju, A. Iqbal, A. K. Trivedi, and A. Mukhopadhyay, "Prediction of shape defects over length of cold rolled sheet using artificial neural networks," *Ironmaking Steelmaking*, vol. 34, no. 2, pp. 166–176, 2007.

[29] J. Cao, C. Song, L. Wang, J. Xiao, and Q. Zhao, "Transverse thickness profile control of electrical steel in 6-high cold rolling mills based on the GA-PSO hybrid algorithm," *Int. J. Adv. Manuf. Technol.*, vol. 121, pp. 295–308, 2022.

[30] Q.-L. Wang, J. Sun, Y.-M. Liu, P.-F. Wang, and D.-H. Zhang, "Analysis of symmetrical flatness actuator efficiencies for UCM cold rolling mill by 3D elastic–plastic fem," *Int. J. Adv. Manuf. Technol.*, vol. 92, no. 1, pp. 1371–1389, 2017.

[31] Alec Stothert (2022), "Simulink for industrial control of a sheet-metal-rolling application, matlab central file exchange," Accessed on: Sep. 26, 2022. [Online]. Available: https://www.mathworks.com/matlabcentral/fileexchange/13978-simulink-for-industrial-control-of-a-sheet-metal-rolling-application

Kun Hu (Member, IEEE) received the B.S. and M.S. degrees in electrical engineering from the Harbin Institute of Technology, Harbin, China, in 2016 and 2018, respectively, and the Ph.D. degree in electrical engineering from The University of Georgia, Athens, USA, in 2023.

Her current research interests include advanced control for power electronics and electric machines, and cyber-physical security for intelligent electric drives.

Jin Ye (Senior Member, IEEE) received the B.S. and M.S. degrees in electrical engineering from Xi'an Jiaotong University, Xi'an, China, in 2008 and 2011, respectively. And also received the Ph.D. degree in electrical engineering from McMaster University, Hamilton, ON, Canada in 2014.

She is currently an Associate Professor of electrical engineering and the Director of the Intelligent Power Electronics and Electric Machines Laboratory, University of Georgia. Her main research areas include power electronics, electric machines, smart grids, electrified transportation, and cyber-physical security.

Dr. Ye was a recipient of a creative research medal for her significant contributions to power electronics security field and received a best paper award from IEEE Applied Power Electronics Conference. She is a general chair of 2019 IEEE Transportation Electrification Conference and Expo (ITEC). She has served in the organizing committee of IEEE Energy Conversion Congress and Expo (ECCE) since 2019 as a publication chair and \ or woman in engineering (WIE) chair. She is a secretary for IEEE power electronics society (PELS) Technical Committee on Transportation Electrification (TC 4). She is an Associate Editor for IEEE TRANSACTIONS ON POWER ELECTRONICS, IEEE OPEN JOURNAL OF POWER ELECTRONICS, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY AND IEEE TRANSACTIONS ON INDUSTRY APPLICATIONS. She was an Associate Editor for IEEE TRANSACTIONS ON TRANSPORTATION ELECTRIFICATION 2017–2020.

Wenzhan Song (Senior Member, IEEE) received the B.S. and M.S. degrees in computer science from Nanjing University of Science and Technology, Nanjing, China, in 1997 and 1999, respectively, and the Ph.D. degree in computer science from Illinois Institute of Technology, Chicago, IL, USA, in 2005.

He is currently the Chair Professor of Electrical and Computer Engineering with University of Georgia, Athens, GA, USA. His research focuses on sensor data analytics and security, sensor networks and data infrastructures.

Dr. Song's lab invented a series of noninvasive sensing technology for the health and security monitoring of humans, animals, machines and infrastructures, driven by the convergence of AI, data science, and advanced sensing and networking technologies. He is also the founder of Intelligent Dots LLC.